RFP 22-70302

TECHNICAL PROPOSAL

ATTACHMENT F

Instructions: Please supply all requested information in the areas shaded yellow and indicate any attachments that have been included to support your responses.

Please ensure no pricing information is included in this document. All pricing information is to be included in Attachment D – Cost Proposal or the noted supplements.

Contents

1. Background, General Requirements, and Key Definitions

1.1 Please list any additional terms and definitions aside from those listed in RFP Section 1.2 and Scope of Work Section 1.2 used by your company or industry that you would like the State to consider incorporating in the contract. The State will not accept terms and definitions introduced after award during contract finalization and implementation.

If awarded this contract, Onpoint would request that the following terms and definitions be incorporated into any Contract/Agreement resulting from this RFP:

Term	Definition
DQVs	Data quality validations
Onpoint Analytic Environment	Onpoint's secure, cloud-based environment that offers role-based access to APCD data and analytic tools for credentialed users
Onpoint CDM	Onpoint Claims Data Manager (CDM), a proprietary APCD platform that spans data collection, integration, enhancement, and extract services
Onpoint PRP	Onpoint's Performance Reporting Portal (PRP), a proprietary online solution that provides options for provider roster management, performance reporting, and review and reconsideration (R&R)

1.2 Please confirm you have carefully reviewed all requirements listed in RFP Section 1.4. Should your company have any exceptions, substitutions, or conditions for the State's consideration, please list them below. The State will not accept exceptions, substitutions, or conditions introduced after award, during contract finalization and implementation.

Onpoint has reviewed the requirements listed in RFP Section 1.4 and has no exceptions, substitutions, or conditions related to the RFP's stated Scope of Work for the State's consideration.

1.3 Please provide a high-level overview of how you plan to develop a solution that will adequately meet the State's needs.

Onpoint's proposed solution for the Indiana Department of Insurance (IDOI) All Payer Claims Database (APCD) encompasses the technical expertise, proven systems, and responsive service delivery model that will be essential elements of a successful APCD launch for the State. We will leverage the experience and lessons learned over nearly 20 years during our implementation of more than 50% of the established APCDs nationally.

While our planning for Indiana's APCD will benefit from our past experience supporting the successful implementation of other state-sponsored APCDs, Indiana's APCD will be developed to address its specific requirements as reflected in RFP Section 1.4 ("Summary Scope of Work"). Onpoint's proposed solution will be designed to achieve the following program goals:

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

Based on those requirements, we are proposing an end-to-end solution that addresses implementation planning, submitter onboarding, data collection and validation, analytic enhancement (e.g., consolidation, master patient and provider indexes, analytic use flags, groupers, measures), data extraction, data product generations, hosting in a cloud-based Analytic Environment, and the design and launch of public-facing transparency website.

To support IDOI's goals, we have assembled a team of subcontractors that bolster Onpoint's experience and capabilities with on-the-ground Indiana resources and market expertise: Briljent, an Indiana Women Business Enterprise (WBE); Haystack, an Indiana Minority Business Enterprise (MBE); and Vespa Group, an Indiana Veteran Owned Small Business (IVOSB). Together, our team will deliver an APCD solution that meets all of the requirements put forward by IDOI under this procurement, including:

1. **Managing the contract.** Throughout the span of the project, Onpoint and Briljent will provide oversight and active project management support through a team of skilled personnel and a suite of proven tools and approaches that ensure effective communication and close collaboration with IDOI, your data submitters, and other project stakeholders for on-time execution of deliverables. For additional detail, please see our Technical Proposal's Section 2.4.8 ("Project Management").
2. **Registering and onboarding submitters.** As an important part of implementation, Onpoint will conduct orientation and training sessions for data submitters regarding the registration and submission process for Indiana's APCD, including the State's finalized data submission specifications. Training will be supplemented by one-on-one support and online technical resources. Many of the national health plans doing business in Indiana are already familiar with Onpoint's data submission platform, Onpoint CDM, and our onboarding process. For more detail, please see our Technical Proposal's sections 2.4.4 ("Design, Development, & Implementation") and 2.4.6 ("Data Services").
3. **Collecting data, including Medicaid and Medicare FFS.** Using Onpoint CDM's secure data submission portal, IDOI's submitters will transmit their monthly eligibility, claims, and provider files to Onpoint for processing, validation, enhancement, and extraction. Our systems have been designed to flexibly integrate standard submission formats, including the APCD-CDL™. Based on our experience in other states and Indiana's RFP, Onpoint has assumed that we will perform the mapping and submission of Medicare files in the State's prescribed layout. In addition, our proposal assumes that the state's Medicaid program will map to the finalized layouts and submit to the APCD on a monthly basis.

   IDOI staff and data submitters alike will be able to follow each file submission as it moves through the processing queue. Onpoint CDM offers a series of dynamic dashboards that enable end users to monitor submitters' registration status, the status of all files submitted to the APCD, requested and approved variances, and submitters' on-time delivery of files. This reporting is continuously refreshed and available 24/7 to credentialed users. For more detail, please see our Technical Proposal's sections 2.4.4 ("Design, Development, & Implementation") and 2.4.6 ("Data Services").

4. **Integrating data.** Onpoint CDM's data integration systems leverage a robust cloud-based infrastructure that employs a series of complex extract/transform/load (ETL) algorithms to standardize, cleanse, and consolidate the submitted data. Onpoint stores our clients' data in an enterprise system that has been designed to handle large volumes of data and can readily accommodate the approximately five (5) million Hoosier lives anticipated by IDOI. This reporting is continuously refreshed and available 24/7. For more detail, please see our Technical Proposal's sections 2.4.4 ("Design, Development, & Implementation") and 2.4.6 ("Data Services").

5. **Managing data quality, including rigorous validation and ongoing enhancements.** Onpoint will validate and work collaboratively with submitters to improve data quality through all stages of the data processing pipeline, enhancing end users' trust and use of Indiana's APCD.

   Onpoint CDM offers a rigorous suite of iterative, multi-step quality assurance processes, including a library of thousands of data quality validations (DQVs) that assess quality and completeness at the payer, file, and element levels. Our DQVs are reviewed and updated regularly based on scrutiny of incoming data, client input, and evolving analytic uses. For more detail, please see our Technical Proposal's Section 2.4.6 ("Data Services").

6. **Enhancing data.** Onpoint is supporting the largest and most diverse group of APCD users and use cases nationally, which has required us to develop and deliver APCD products with an unmatched, rich suite of data enhancements. These enhancements are not just canned outputs but instead are time-tested, transparent, APCD-specific tools that our clients and their end users rely on daily to make efficient and effective use of their data. For more detail, please see our Technical Proposal's sections 2.4.6 ("Data Services") and 2.4.10 ("Analytics").

7. **Protecting and storing data.** Information security and privacy are critical priorities for Onpoint's business operations and reputation. Since launching our first APCD solution in 2003, Onpoint has securely received and processed more than 50 billion records with zero incidence of accidental disclosure of protected health information (PHI) or personally identifiable information (PII).

   Onpoint's client- and submitter-facing applications, including Onpoint CDM and the Analytic Environment, are hosted in the cloud on infrastructure operated by Amazon Web Services (AWS), with all system resources located inside of the continental United States in data centers that are SOC-2 certified. Onpoint has been vetted and reviewed for privacy and security compliance by all of our state government clients and has successfully achieved HITRUST certification, the gold standard in health data security. For more detail, please see our Technical Proposal's sections 2.4.5 ("Security & Privacy") and 2.4.9 ("Maintenance, Support, & Enhancements").

8. **Creating and providing data extracts.** Onpoint regularly produces a wide range of standard, ad hoc, and customized analytic data sets for our clients, which are delivered either through our Analytic Environment with role-based permissions or via SFTP with PGP encryption. Our proposed solution for IDOI's APCD includes all required data sets, including standard annual data sets, custom ad hoc data extracts, and quarterly database refreshes of the APCD's integrated and enhanced data. Each data set delivery from Onpoint is accompanied by the documentation, release notes, and support necessary for

effective use. For more detail, please see our Technical Proposal's sections 2.4.6 ("Data Services") and 2.4.7 ("Data Production & Consumer Website").

9. **Supporting analysis.** Onpoint offers a secure and highly performant Analytic Environment that features a suite of analytic tools to meet the needs of IDOI and Indiana's end users across varying levels of expertise. These include access to a business intelligence (BI) application developed specifically for APCD users along with leading commercial tools (e.g., Microsoft Office, Tableau Creator, RStudio, DataGrip for SQL queries, Anaconda (Python)). Onpoint's Analytic Environment offers role-based access to APCD data for clients and their approved users via a secure, cloud-based virtual desktop hosted by AWS. For more detail, please see our Technical Proposal's sections 2.4.7 ("Data Production & Consumer Website") and 2.4.10 ("Analytics").
10. **Providing public-facing, interactive website.** Onpoint has provided multiple clients with consumer-facing websites and interactive reporting that provide the public with information regarding the cost, quality, and utilization of healthcare services.

    Our proposed solution for IDOI includes the development of public-facing data visualizations and reports that employ the drill-down and filtering capabilities of Tableau to maximize engagement on a mobile-friendly website, which will be updated annually. For more detail, please see our Technical Proposal's Section 2.4.7 ("Data Production & Consumer Website").

We are excited to offer the State a team and approach that is collaborative, cost effective, and responsive to the State's specific needs.

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 subcontractor.

2.1 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. Please explain how you meet this requirement. Provide client list and examples of work performed.

Onpoint fully meets this requirement independently (without having to factor in our subcontractors). Onpoint has nearly 20 years' experience in large-scale healthcare claims data collection, processing, validation, reporting, and analysis, exceeding the solicitation's requirement of at least five years' experience.

Onpoint has performed a wide array of data management and analytic services for nearly two decades for APCD and multi-payer data initiatives across the country – work that encompasses collection, processing and standardization, validation and quality assurance, and enhancement of eligibility, claims, and provider files across hundreds of payers. Onpoint currently is integrating

data from more than 345 submitters from across the United States and managing 50 billion records covering 80 million lives.

Onpoint CDM (Claims Data Manager), our core data integration platform, has been in production for more than 15 years and has been continuously enhanced to address changes in payment systems, adjudication standards, and evolving use cases. It securely processes and validates a wide range of file types for all payer and plan types and easily handles proprietary layouts and plan-specific elements. Onpoint provides mapping and submission support services to Medicaid and Medicare plans and to any commercial plans requiring technical support. We also are prepared to collect and integrate nonstandard files to support the State's requirements, if necessary, including alternative payment model data, clinical outcomes data, and other supplemental files.

All arriving data are taken through an end-to-end, multi-phase quality assurance (QA) process that includes preliminary integrity checks, initial loading checks, completeness validation, data standardization, data-quality validation, consolidation, and trending analysis, followed by enhancement, additional QA, and extract for data delivery and reporting product generation. The breadth and depth of Onpoint's quality assurance procedures are comprehensive, time-tested, and a differentiator in the APCD market.

A summary of our APCD-related clients is included below in **Table 2.1.A**.

Table 2.1.A. Onpoint's APCD-Related Clients & Metrics

[redacted]

2.2 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. Please explain how you meet this requirement. Provide client list and examples of work performed.

Onpoint fully meets this requirement independently. Onpoint's analytic services are currently being delivered to 10 APCD and multi-payer claims database (MPCD) clients across states and regions nationally and encompass a broad array of analytic products, skills, and capabilities. These services rely on a proven set of analytic methods and tools and include public transparency reporting, population health reporting, provider performance reporting, program evaluation, policy analysis, research collaboratives, and more. Recent client engagements include the following (please see our response to Question #2.1, above, for additional detail):

- **Connecticut Office of Health Strategy (OHS).** Onpoint implemented and continues to serve as data aggregator and analytics contractor for the state's APCD program for more than seven years. For analytic services, we have been responsible for designing a suite of population health and price transparency reporting (for the state's benefits exchange, AccessHealth CT), running race/ethnicity imputation algorithms and generating reporting by geography, and generating a primary care spending analysis.
- **California's Integrated Healthcare Association (IHA).** Onpoint manages the statewide voluntary MPCD in California for IHA, a multi-stakeholder collaborative, and is supporting a number of prominent public reporting and research initiatives, including: A statewide Cost and Quality Atlas initiative that allows the public to compare the quality and cost of care for 20 million people across California; a primary care spending analysis that informed policy decisions by the state's health benefits exchange, Covered California, around primary care investment; an informal PPO network performance analysis that assessed the relative cost and quality of providers within loosely knit provider groups compared to highly integrated systems, also on behalf of Covered California; and an analysis of seriously ill populations and their underlying costs by region.
- **Comagine Health Oregon.** A regional health improvement collaborative, Comagine contracts with Onpoint to manage a statewide voluntary ACPD and generate performance reporting by provider group and region. We generate an array of HEDIS-certified quality measures and numerous cost measures, including HealthPartners' Total Cost of Care, (formerly the Oregon Health Care Quality Corporation) along with performance reporting for multiple initiatives in which they participate, including CMS's Comprehensive Primary Care Plus (CPC+) program.
- **New England States Consortium Systems Organization (NESCSO).** Onpoint was selected by the six-state consortium of New England state health departments to perform a regional primary care spending study using a distributed data model that leveraged APCDs from each of the six states. Onpoint worked with a multi-state advisory group to develop specifications, establish quality assurance procedures, and generate comparative reporting across the region.
- **Maryland Health Care Commission.** Onpoint serves as the state's APCD data management and analytics contractor. Our analytics team is responsible for delivering an annual privately insured market analysis that provides summary statistics and visualizations of the commercial health insurance market in Maryland. The reporting drills into differences and trends in spending and utilization by market segment and across demographic characteristics, service category, service setting, and condition.
- **Vermont Green Mountain Care Board.** Onpoint serves as the state's APCD data management and analytics contractor and, in that role, hosts a cloud-based Analytic Environment that supports analysts across multiple state agencies. We also are responsible, as a subcontractor to Mathematica, for the cost benchmark reporting associated with the state's

CMS-approved All-Payer ACO model. Onpoint produces the mandated reporting against state benchmarks and performs frequent drill-down and cost-driver analyses requested by the state.

- **Vermont Blueprint for Health.** We are responsible for conducting program evaluation and reporting services for the state's Blueprint healthcare transformation initiatives that currently encompass advanced primary care (e.g., chronic disease management, behavioral health integration), women's health, and opioid treatment models. Community and program profiles are generated for each model and include cost and quality measurement with variation, benchmarking, and trending over time. Evaluation services and research publications employ sophisticated statistical modeling.
- **Washington State Health Care Authority.** Onpoint manages the state's APCD and is responsible for generating Washington's Common Measure Set and producing the comparative cost and quality reporting that feeds the state's public-facing consumer website, Washington HealthCareCompare. We also have been contracted to generate a series of studies and reporting, including the reference pricing to support the state's Public Option being offered through the Washington Health Benefit Exchange and, on behalf of the state's Office of the Insurance Commissioner, an analysis to support surprise billing legislation, an analysis of primary care spending, a study of mental health parity, and, most recently, the development of an analysis to support the state's global healthcare cost benchmarking.

Onpoint's Analytic Services team supports a wide range of custom analyses, ad hoc reporting, and standard reporting for clients similar to the recent engagements highlighted above. These initiatives leverage the full range of analytic skills, including advanced statistical analysis and modeling, methods, and tools. Much of our analytic work is grounded in claims data and, increasingly, requires the linkage of claims data with non-claims data sources – an area of considerable experience for Onpoint. Recent data linkage projects have included the linkage of claims with clinical/EHR, public health registry, health improvement program, survey, incarceration, and social determinants of health data.

2.3 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); and

B. Health Information Technology for Economic and Clinical Health Act (HITECH).

Please explain how you meet this requirement. Provide client list and examples of work performed.

Onpoint fully meets this requirement independently. Information security and privacy are critical priorities for our organization, and our team has nearly two decades' experience in understanding, applying, and complying with both state and federal standards.

Following guidance from the U.S. National Institute of Standards and Technology (NIST), Onpoint has developed and maintains a robust information security program that is compliant with both HIPAA and HITECH, ensuring the security and confidentiality of patient-identifiable data.

Our data integration systems have been in steady operation and in service to APCD programs and other clients with zero incidence of accidental disclosure of protected health information (PHI) or

personally identifiable information (PII) across the more than 50 billion records received and processed since Onpoint's first APCD launch in 2003.

Onpoint's information privacy and security program has been vetted and reviewed for compliance by all of our state government clients and has successfully achieved both HITRUST certification, the gold standard in health data security, and CMS Qualified Entity Certification Program (QECP) security compliance, requiring the successful and repeated completion of exacting security accreditation processes. HITRUST is a healthcare-specific common security framework covering the relevant components of security frameworks from the International Organization for Standardization (ISO), the Payment Card Industry (PCI), NIST, HIPAA, and others.

Please see our response to Question #2.1, above, for a list of APCD-related clients and scope of work performed in adherence to HIPAA and HITECH standards.

2.4 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. Include a brief table of key staff members who would be working on this project and clearly detail their experience in the above categories, including timeframes, whether the experience was health care data system/APCD-related, names of data systems/projects, and if work was for data management or analytics or both. Include the qualifications and experience of your Privacy or Compliance Officer.

Onpoint fully meets this requirement independently. With the addition of our Indiana partners, our core project team, detailed below, offers more than 150 years of combined experience in data collection, data management, data enhancement, eligibility/claims reporting, and meeting HIPAA/HITECH mandates. The following table identifies the key staff members who will support Indiana's APCD as well as details regarding their experience.

Table 2.4.A, below, details our team's key staff members' experience. All key staff members are supported by a deep bench of staff with APCD expertise and bring valuable, relevant experience to IDOI's APCD implementation and operations. Key staff members are listed in the table below in the same order as listed in other staffing-related sections (e.g., our Technical Proposal's Section 8 ("Project Management"), our completed RFP Attachment J1 ("Resource Usage Template")).

Table 2.4.A. Key Staff Experience Summary

Project Role: Account Management Lead	**Name:** Monique Cote, PMP (Onpoint)	**Total Years of Experience:** 11
Experience Category	Data Management	
Timeframe	4/2011 – 4/2022	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Rhode Island Health Information Exchange – project management	☒ Data Management ☐ Analytics
	• Rhode Island Regional Extension Center – project management	☒ Data Management ☐ Analytics
	• Integrated Healthcare Association – implementation and project management	☒ Data Management ☒ Analytics
	• Washington HealthCareCompare website – implementation and project management	☒ Data Management ☒ Analytics

	• Clarify Health – implementation and project management • California Department of Health Care Access and Information – account management	☒ Data Management ☐ Analytics ☒ Data Management ☒ Analytics
Experience Category	Meeting HIPAA/HITECH mandates	
Timeframe	4/2011 – 4/2022	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Rhode Island Health Information Exchange – project management • Rhode Island Regional Extension Center – project management • Integrated Healthcare Association – implementation and project management • Washington HealthCareCompare website – implementation and project management • Clarify Health – implementation and project management • California Department of Health Care Access and Information – account management • Massachusetts CHIA Statistical De-identification Analysis – project management	☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☒ Analytics ☐ Data Management ☒ Analytics
Experience Category	Reporting services using health care claims	
Timeframe	7/2017 – 4/2022	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Integrated Healthcare Association custom reporting, ad hoc analytic services – project management • Washington APCD custom data extracts and reporting, ad hoc analytic services – project management • California Department of Health Care Access and Information – account management	☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics
Project Role: Health IT Project Manager	**Name:** Grace Chandler (Briljent)	**Total Years of Experience:** 14
Experience Category	Encounters for a large data system	
Timeframe	7/2008 – present	
Was the experience health care data system / APCD related?	☐ Yes ☒ No	
Project/Data System Names & Work Type	• Patient Centered Medical Homes, State of Idaho, Department of Health and Welfare – project management • Medicaid Electronic Health Record Incentive Program Contract, CMS and Urban Institute – project management • Affordable Care Act Training Contract, Indiana Family and Social Services Administration and Indiana Department of Insurance – project management • Supporting State Medicaid Agencies and Health Information Technology coordinators in implementing their Medicaid Electronic Health Records Incentive Programs • Indiana Department of Insurance (IDOI) – Director for the Indiana State Health Insurance Assistance Program	☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics

	• Medicare Supplement Insurance Committee of the National Association of Insurance Commissioners – program lead	☒ Data Management ☒ Analytics
Project Role: Health IT Consultant	**Name:** Susan Clark (Briljent)	**Total Years of Experience:** 25
Experience Category	Encounters for a large data system	
Timeframe	1/1997 – present	
Was the experience health care data system / APCD related?	☐ Yes ☒ No	
Project/Data System Names & Work Type	• Indiana FSSA Health Information Exchange (HIE) – strategic project planning and management	☒ Data Management ☒ Analytics
	• Missouri HIE – strategic project planning and market assessment	☒ Data Management ☒ Analytics
	• Nebraska Health Information Initiative (NeHII) – strategic project advising	☒ Data Management ☒ Analytics
	• Indiana FSSA regarding 21st Century Cures Interoperability Rules, telehealth, and data systems optimization to advance Health Homes – strategic advising and management of long-term services and supports for the Division of Mental Health and Addiction Data Modernization, and All Payer Claims Database (APCD)	☒ Data Management ☒ Analytics
	• AHIMA Advocacy and Policy Council Chair	☒ Data Management ☒ Analytics
	• IHIMA president (past)	☒ Data Management ☐ Analytics
Experience Category	Meeting HIPAA/HITECH mandates	
Timeframe	1/1997 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• 20+ years in managed care, clinical operations, revenue cycle, HIPAA, process/quality improvement, business process re-engineering, strategic planning, project management, system implementation, practice transformation consulting, and business development	☒ Data Management ☒ Analytics
Project Role: Health IT Consultant	**Name:** Shaun Wilhelm (Briljent)	**Total Years of Experience:** 19
Experience Category	Data Collection	
Timeframe	7/2013 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Washington Health Care Authority, State Health Information Technology Coordinator – HIT Section Manager	☒ Data Management ☒ Analytics
	• Oversaw the design and development of IT systems used for data acquisition and data management, including policy and infrastructure development of the Washington APCD	☒ Data Management ☒ Analytics
Experience Category	Data Management	
Timeframe	7/2013 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	

Project/Data System Names & Work Type	• Washington Health Care Authority, State Health Information Technology Coordinator – HIT Section Manager • Oversaw the design and development of IT systems used for data acquisition and data management, including policy and infrastructure development of the Washington APCD	☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics
Experience Category	Reporting services using health care claims	
Timeframe	7/2013 – present	
Was the experience health care data system / APCD related?	☐ Yes ☒ No	
Project/Data System Names & Work Type	• Division of Behavioral Health (DBH), Wyoming Department of Health, Lead Statistician, Policy and Research Analyst • Division of Behavioral Health, Alaska Department of Health and Social Services, Chief of Risk and Research Management	☒ Data Management ☒ Analytic ☒ Data Management ☒ Analytics
Project Role: Privacy Officer	**Name:** Anna Dawkins (Onpoint)	**Total Years of Experience:** 13
Experience Category	Meeting HIPAA/HITECH mandates	
Timeframe	1/2009 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Maintain Onpoint's robust privacy program by ensuring compliance with HIPAA/HITECH, assorted state agencies, and other privacy regulations and standards • Oversee annual HIPAA training for Onpoint staff • Oversee HITRUST certification process	☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics
Experience Category	Data Collection	
Timeframe	1/2009 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Maintain compliance with assorted state and client data collection requirements/standards	☒ Data Management ☐ Analytics
Project Role: Data Operations Lead	**Name:** Gina Robertson (Onpoint)	Total Years of Experience: 4
Experience Category	Data Management	
Timeframe	4/2018 – 3/2022	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Data Operations management for WA APCD, VT APCD, RI APCD, MN APCD, MD APCD, CT APCD, Comagine APCD (Oregon) • Data Operations management for Medicare FFS datasets in WA, VT, RI, PA, OR, CT • Implementation management for MD APCD • Data analytics for WA APCD, RI APCD, VT APCD, MN APCD, Comagine APCD	☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics
Experience Category	Data Collection	
Timeframe	11/2019 – 3/2022	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	

Project/Data System Names & Work Type	• Data Operations Analyst and Data Submitter Liaison for RI APCD, MD APCD, CA APCD	☒ Data Management ☒ Analytics
Project Role: Health Analytics Lead	**Name:** Amy Kinner, MS (Onpoint)	**Total Years of Experience:** 20
Experience Category	Reporting services using health care claims	
Timeframe	7/2012 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Implemented a public reporting website in Washington State to provide price transparency and quality measures • Subject matter expert on HEDIS measures and reporting at the practice, payer, and geographical levels • Worked collaboratively with clients to develop creative reporting solutions for program evaluation and new analytic products • Expertise in Tableau, SQL, SAS, and risk adjustment	☐ Data Management ☒ Analytics ☐ Data Management ☒ Analytics ☐ Data Management ☒ Analytics ☐ Data Management ☒ Analytics
Experience Category	Meeting HIPAA/HITECH mandates	
Timeframe	7/2009– present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Responsible for ensuring Analytics Team follows HIPAA/HITECH compliance • Responsibility for QA of analytic reports to ensure HIPAA compliance and best practices regarding blinding of small numbers	☐ Data Management ☒ Analytics ☐ Data Management ☒ Analytics
Experience Category	Encounters for a large data system	
Timeframe	7/2009 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Led projects with the Integrated Healthcare Association in California that used encounter data for analytics and HEDIS measures • Implemented linkage between encounter data and claims data in Vermont to measure health systems performance	☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics
Project Role: Technical Infrastructure Engineer	**Name:** Corey Ramsey, CISSP (Onpoint)	**Total Years of Experience:** 7
Experience Category	Meeting HIPAA/HITECH mandates	
Timeframe	10/2021– 3/2022	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Policies/procedures review to ensure compliance • Evidence collection • HITRUST certification • Build out of Analytic Environment for Maryland client • Ensuring all data and platforms are secure and compliant. • Ensuring all database access is role based using least-privilege model	☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics
Experience Category	Data Management	
Timeframe	6/2015 – present	

Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Ensuring systems meet security requirements for housing data • Ensuring all databases meet security standards • Ensuring all database access is role based using least privilege model	☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics
Project Role: Systems Development Engineer	**Name:** Jeff Cain (Onpoint)	**Total Years of Experience:** 11
Experience Category	Data Management	
Timeframe	1/2011 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Data management SME across Onpoint clients, including for California's MPCD, Connecticut's APCD, and Minnesota's APCD • Manage processing of more than 9,000 files quarterly across Onpoint's client base • Implemented ETL for taking data submission to conformed data set in warehouse for both RI and VT clients • Generate data structures to support data processing and apply business rules to transform data into standard formats	☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics
Experience Category	Reporting services using health care claims	
Timeframe	3/2020 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Mapping healthcare claims data to HEDIS and other measure specifications, including advanced analysis, design, development, and implementation of software solutions • Advised on data intake structure and process for supporting PROMS depression measurement and reporting for California's MPCD	☒ Data Management ☒ Analytics ☒ Data Management ☒ Analytics
Experience Category	Meeting HIPAA/HITECH mandates	
Timeframe	1/2011 – present	
Was the experience health care data system / APCD related?	☒ Yes ☐ No	
Project/Data System Names & Work Type	• Responsible for annual HIPAA security training • Responsible for ensuring Systems Development Team follows HIPAA/HITECH compliance	☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics
Project Role: Systems Development Engineer	**Name:** Quinton Chester (Haystack)	**Total Years of Experience:** 11
Experience Category	Data Management	
Timeframe	8/2021 – present	
Was the experience health care data system / APCD related?	☐ Yes ☒ No	
Project/Data System Names & Work Type	• Created and developed eye-catching, engaging user experiences for the Central Indiana Community Foundation • Architected, designed, and developed applications for client websites, including Sold By You and Nodit	☒ Data Management ☐ Analytics ☒ Data Management ☐ Analytics

Experience Category	Data Collection	
Timeframe	3/2020 – 7/2021	
Was the experience health care data system / APCD related?	☐ Yes ☒ No	
Project/Data System Names & Work Type	• Developed, communicated, and tracked pertinent team measurements, timelines, and performance targets	☒ Data Management ☐ Analytics
	• Created easy-to-use, innovative applications for high-profile clientele looking for mobile solutions, including VenuEats	☒ Data Management ☐ Analytics
Project Role: Data Architect	**Name:** Rajesh Govindarajan (Vespa Group)	**Total Years of Experience:** 23
Experience Category	Data Management	
Timeframe	12/1999 – present	
Was the experience health care data system / APCD related?	☐ Yes ☒ No	
Project/Data System Names & Work Type	• COID-19 contact tracing data integration	☒ Data Management ☐ Analytics
	• Developed and managed Azure Data Factory pipelines and Power Apps data flow to integrate data between the National Electronic Disease Surveillance System Base System (NBS) and ISDH contract tracing portal based on Dynamics 365	☒ Data Management ☐ Analytics
	• Designed and managed a contact tracing SQL Azure database to consolidate data from NBS and ISDH call center into one centralized database to generate Power BI reports for decision-makers at ISDH	☒ Data Management ☐ Analytics
	• Developed and managed Power Automate flows to monitor and notify end users about critical system issues	☒ Data Management ☐ Analytics

Anna Dawkins has served as Onpoint's Privacy Officer for 13 years. Ms. Dawkins has been responsible for overseeing Onpoint's robust privacy program by ensuring compliance with HIPAA, HITECH, the requirements of a variety of state agencies, and other privacy regulations and standards.

Please see our response to Question #2.1, above, for a list of APCD-related clients and scope of work.

2.5 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. Please submit proof of this requirement. 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. If you are not currently a CMS approved Custodian, outline your plan to obtain approval.

Onpoint fully meets this requirement independently. For all but one of our APCD clients, Onpoint currently serves as the designated Custodian for Medicare submissions from the U.S. Centers for Medicare & Medicaid Services (CMS). Proof of our certification for Comagine Health, our APCD client in Oregon, is included as an example via the following attachment: "Onpoint - IN RFP 22-70302 - Technical Exhibit 2.4.2.5.A - QECP Certification Proof (Oregon Example).pdf". (Please

note that the CMS certification letter cites the client's name as "Oregon Health Care Quality Corporation (Q Corp)," which was later rebranded to "Comagine Health," which is the name referenced elsewhere in this proposal.)

2.6 Respondent must currently be or agree to become CMS Qualified Entity (QE) (https://www.qemedicaredata.org/). Please submit proof of this requirement. If you are not currently a QE, outline your plan to obtain approval.

Onpoint has served as the designated Data Custodian for multiple Qualified Entities in the past and, as such, has fulfilled the rigorous data security review process required to obtain Qualified Entity Certification Program (QECP) approval. Onpoint's clients typically have served as the Qualified Entity, not Onpoint, because it has been their role to sponsor their respective measurement and public reporting initiatives, including the convening of stakeholders, and our clients would like their access to Medicare data to transcend a single vendor. We have supported several of our clients throughout the QECP application process and are very familiar with the steps required to become a Qualified Entity. Onpoint has reviewed the QECP Program Guide and is qualified and capable of meeting all QECP requirements. We are willing to take on this role if that is the preference of IDOI. Onpoint is prepared to immediately register with CMS and request the application to become a Qualified Entity if awarded the contract by IDOI and will work with our assigned CMS Program Manager to diligently complete the three-phase application process.

If IDOI wishes to consider other options, it may be of interest that Onpoint's other state APCD clients have evaluated the merits of the various approval tracks available to them for receiving Medicare claims data and, most often, have chosen the State Agency track available through the Research Data Assistance Center (ResDAC). This track gives states the flexibility and data access they require without the level of CMS compliance oversight, reporting requirements, and recertification embedded in the QECP.

It may also be worth noting that the QECP requires that a corrections and appeals process be put in place if IDOI decides to publicly report on the performance of individual providers, which can be resource intensive, costly, and politically sensitive. Onpoint supports this process for other QEs through our Performance Reporting Portal (PRP), which Onpoint has not included as part of the scope for this proposal but could readily include if requested by the State. Among its many features, Onpoint's PRP provides secure access to patient-level measure results, allows for provider roster management, and offers practices an automated corrections and appeals process. The patient-level measure results would be updated with each reporting cycle, on a quarterly basis, and we would recommend that the corrections and appeals process be undertaken twice per year.

2.7 Provide a copy of your most recent SOC 2 report as an attachment OR provide proof that you currently are HITRUST CSF Validated and have a valid HITRUST CSF Certification.

Onpoint is HITRUST CSF certified and has included our HITRUST certification letter as the following exhibit: "Onpoint - IN RFP 22-70302 - Technical Exhibit 2.4.2.7.A - HITRUST Letter.pdf".

3. High-Level Solution and Administrator Requirements

3.1 Please outline how you will meet each of the Administrator Duties and Responsibilities listed in Section 3.1 of the Scope of Work.

Onpoint's proposed solution to implement and operate Indiana's All Payer Claims Database (APCD) in support of the Indiana Department of Insurance (IDOI) encompasses the technical expertise, proven systems, and track record of successful APCD implementations necessary to ensure success in Indiana.

Onpoint's data integration platform brings together the latest in big data technology, end-to-end data quality validation procedures, HITRUST-certified information security, a cloud-based Analytic Environment, and a team of analysts and software engineers with the skill to design an innovative web-based public reporting solution tailored to meet IDOI's vision.

To expand our resources and market expertise and to address the State's diversity goals in this procurement, Onpoint is partnering with three Indiana-certified contractors that bring distinct skills and capabilities: Briljent (WBE) will deliver project management and APCD consulting services, Haystack (MBE) will provide web development services, and the Vespa Group (IVOSB) will provide infrastructure support services. Together with these subcontractors, Onpoint is prepared to meet all duties and responsibilities of the APCD Administrator as reflected in the Statement of Work (RFP Attachment K) and described in detail below.

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.** Information security and privacy are critical priorities for Onpoint's business operations and reputation. Since launching our first APCD in 2003, Onpoint has securely received and processed more than 50 billion records with zero incidence of accidental disclosure of protected health information (PHI) or personally identifiable information (PII). Onpoint's client- and submitter-facing applications, including Onpoint CDM and our Analytic Environment, are hosted in the cloud on infrastructure operated by Amazon Web Services (AWS), with all system resources located inside of the continental United States in data centers that are SOC-2 certified. Onpoint's information security program has been vetted for compliance with all relevant data security frameworks and standards by all of our state government clients. We have successfully achieved HITRUST certification, the gold standard in health data security.

2. **Defining infrastructure needs and developing a sustainability plan.** Onpoint will work with the State to understand and document your business requirements. Next, needs will be assessed and defined for each of the key APCD infrastructure components, including data collection and integration, the Analytic Environment, and the web-based public reporting solution. Requirements will encompass technical business processes, performance and service-level agreements, and data security standards. [redacted] This scalable architecture ensures that the underlying infrastructure can be adjusted easily over time as program demands for data processing and storage change.

   For sustainability planning, Onpoint will leverage our experience supporting other state-mandated APCDs and help the State develop similar sustainability strategies. From building marketable data products and seeking inter-agency financial support to seeking

CMS Implementation Advanced Planning Document (IAPD) approval of federal matching funds, Onpoint can support the State's efforts to ensure adequate ongoing funding. We will leverage Briljent's specific expertise in this area, with members of their team bringing experience as state government officials and consultants supporting efforts to plan for and secure future APCD program funding.

3. **Drafting a data submission guide.** Onpoint will work collaboratively with the IDOI Program Manager and Advisory Board to develop a data submission guide (DSG) that will serve the data needs of the state of Indiana. We will bring forward templates from our work supporting other state APCDs and offer the key technical expertise to draft a DSG that ensures that comprehensive, timely, and reliable data are collected. The DSG should provide important technical guidance around file-naming conventions, file-structure specifications, data element definitions, and submission formats, for example. DSGs typically outline the threshold percentages that payers will be expected to achieve – not only for each element's completeness, but for each element's completeness with *valid* data. All program documentation, including the DSG, will be easily accessible via Onpoint CDM's secure online portal.

4. **Collecting, managing, analyzing and hosting an online data submission portal or a proposed equivalent.** Onpoint's data integration services are delivered through a Software as a Service (SaaS) model, which enables cost-effective access by clients and data submitters to a market-leading data integration solution called Onpoint CDM (Claims Data Manager). The SaaS model encompasses the technology, training, support tools, and expert staff required to efficiently support an all-payer claims database (APCD) system.

   Onpoint CDM, which includes a secure submission portal, provides proven tools for data collection, cleansing and standardizing, rigorous quality assurance, and the consolidation and enhancement of the data for analytics. Most important, Onpoint CDM is a proven APCD platform with a record of successfully collecting and integrating billions of insurance claims and enrollment records from more than 345 submitters on a monthly or quarterly basis. The platform has been continuously enhanced to address changes in billing standards and payment models and to meet the evolving analytic use cases that a contemporary APCD must support. Onpoint CDM leverages the Amazon Web Services (AWS) cloud and guarantees 99.9% uptime. Throughout, the system is overseen by dedicated quality assurance analysts and IT experts to make sure that our clients' data is securely managed, efficiently processed, and reliably delivered.

5. **Collecting, storing, managing, and hosting all data collected by the APCD in an Administrator-developed centralized data warehouse or proposed equivalent.** All APCD data collection and integration functions are performed within Onpoint CDM's proven platform. This robust, cloud-based infrastructure performs a series of complex and configurable extract/transform/load (ETL) processes that standardize, cleanse, and consolidate submitted data. Onpoint CDM is architected to flexibly handle claims submissions and supplemental files using any layout – from the APCD-CDL™ (Common Data Layout), CMS standard file structures, and state- and payer-specific layouts. The ETL process dynamically ingests and transforms arriving data into standard elements within Onpoint CDM's common data model. Every incoming data element is transformed based on rules configurable at the element, submitter, and client levels while also maintaining the as-submitted value in the data warehouse. Onpoint stores our clients' data in an enterprise system designed for handling large volumes of data and can scale easily to accommodate Indiana's anticipated data volume of 5 million lives. The state's

comprehensive data warehouse will be hosted in a cloud-based Analytic Environment, architected for analytic use, and refreshed on a quarterly basis.

6. **Securing and streamlining data collection and aggregation.** Onpoint's data collection and integration platform, Onpoint CDM features a secure, online data submission portal that will enable IDOI staff and data submitters alike to follow each submission as it moves through the processing queue, accessing comprehensive real-time reporting about submission status and quality. End users are supported by dedicated data operations staff and transparent documentation on business processes and rules. National health plans doing business in Indiana already would be familiar with Onpoint CDM's file submission and data-status reporting tools as they likely are submitting data to Onpoint in other states. Our systems have been designed to easily scale and flexibly integrate both claims and non-claims data sources on behalf of state APCD programs.

7. **Performing claims editing and business processing.** Onpoint's data integration platform, Onpoint CDM, relies on a wide array of data quality validation checks along with data standardization and transformation processes to ensure the completeness and validity of APCD submissions. More than 2,000 validation checks are enforced at the payer, file, and element levels. These validation checks (or "edits") will be configured within Onpoint CDM to support Indiana's data submission specifications, including your acceptance thresholds.

   Other business processes encompassed within our APCD platform include a suite of data enhancements that support the usability of the data sets that we deliver. These enhancements are differentiated from those of other APCD vendors in that they are not just the canned output from a third-party product but instead are time-tested, transparent, APCD-specific value-adds that our clients rely on daily to make efficient and effective use of their data.

8. **Performing data analytics and providing analytical tools and access to the end users.** Onpoint proposes to deploy a secure, highly performant Analytic Environment that features a suite of analytic tools to meet the needs of IDOI and Agency users with varying levels of expertise. All users will have access to a business intelligence (BI) solution designed for APCD data that provides a suite of dashboards and data marts organized around specific health analytic domains. The dashboards will leverage Tableau's intuitive user interface with flexible filtering and visualizations and are built for self-service reporting. Other analytic tools available to the required ten (10) users include Microsoft Office, Tableau Creator, RStudio (R), Anaconda (Python), and DataGrip (SQL).

   Onpoint's Analytic Environment offers secure, role-based access to APCD data by approved users through a virtual desktop in a virtual private cloud hosted by AWS. IDOI's instance of the Analytic Environment will accommodate all of the State's historical data and will be refreshed quarterly with new data, allowing users to conduct analysis across payers, providers, conditions, geography, and other dimensions over time.

9. **Providing datasets and reports.** Onpoint regularly produces a wide range of standard, ad hoc, and customized analytic data sets for our clients, which are delivered either through our Analytic Environment with role-based permissions or via SFTP with PGP encryption. Our proposed solution for IDOI's APCD includes all required data sets, which will be derived from the quarterly data refresh cycle: (a) a comprehensive, unfiltered quarterly extract; (b) a set of commonly requested analytic data sets, refreshed quarterly; (c) five (5) custom ad hoc data extracts, refreshed annually; and (d) a public use file data set,

refreshed annually. Each data set delivery from Onpoint will be accompanied by the documentation and support necessary for effective use.

10. **Furnishing data access for State-approved users.** Onpoint's Analytic Environment is the primary vehicle for provisioning secure, role-based access to APCD data for state-approved users. Through a dedicated AWS-hosted environment, data users will have access to a suite of analytic tools, training, and technical support.

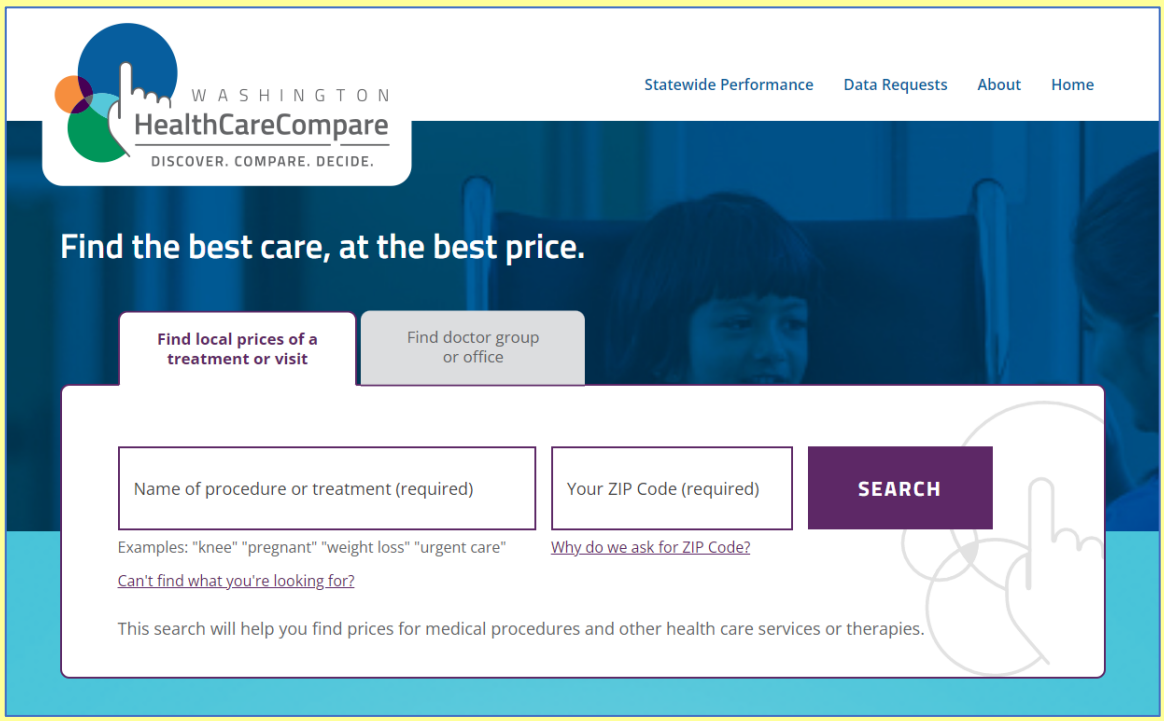
    To ensure secure access, [redacted]

    Additionally, the Analytic Environment provides users with access to only their authorized data sets (e.g., comprehensive data set, standard data product, custom data sets), which can be adjusted at any time based on client requests and requirements. State APCD programs typically adopt specific release rules and guidelines that will inform the data release process (e.g., minimum necessary rules, sensitive data restrictions, data use restrictions). Most often, states convene an advisory committee to support data governance activities – similar to what is envisioned for IDOI's Advisory Board. Onpoint can provide sample tools and templates to support standard data governance processes, including the data release process.

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.** Onpoint proposes to develop a custom consumer transparency website that contains a suite of comparative price/cost and quality reporting with drill-down and filtering capabilities and easy navigation among reporting dimensions that include geography and provider/facility. The dashboards will leverage the rich and dynamic features of Tableau technology to maximize engagement. The site will be refreshed annually and enabled for mobile-friendly viewing.

    In designing IDOI's consumer site, Onpoint will leverage our extensive experience developing public reporting solutions for other APCD clients. To illustrate, we developed a similar site for the state of Washington, which was recognized by the National Association of Health Data Organizations with its "Innovation in Data Dissemination Award" in 2018. This site, Washington HealthCareCompare, was designed to achieve goals similar to those of IDOI, including the price transparency reporting component highlighted in **Figure 3.1.A**, below.

Figure 3.1.A. Washington HealthCareCompare Consumer Website



12. **Presenting data to allow for comparisons of geographic, demographic, and economic factors and institutional size.** Onpoint will provide IDOI with public-facing reporting using a suite of dynamic, Tableau-based dashboards focused on key interest areas for easy integration into a mobile-friendly website for the State. During requirements gathering and report design sessions, Onpoint will draw upon our many years of experience using APCDs to analyze cost, utilization, access, quality, equity, and member demographics to deliver meaningful, intuitive public-facing reports and websites. Each of the public reporting initiatives that we have supported is distinct and tailored to our client's specific audience, requirements (content, legal, and other), communication strategy, and budget, and we will follow that same approach in support of IDOI.

    Onpoint will lead initial planning sessions to address any open questions around the vision, purpose, and topic areas of interest and then shift to content and design questions. We will work with IDOI to identify key measures of interest, desired geographical and other stratifications, and demographic breakouts, for example.

13. **Presenting data in a consumer-friendly manner in accordance with the Assistive Technology Policy (Section 508).** Onpoint follows industry-best practices in the design of our online solutions, including compliance with the Americans with Disabilities Act. Design features include the use of alternative image text, following color-contrast guidelines, and allowing for keyboard navigation. Onpoint performs regular Section 508 compliance testing to ensure the accessibility of the pages within our online solutions and will perform this testing before release of IDOI's public website and public-facing Tableau dashboards. Indiana's website also will undergo this testing before any major release as well as annually if no major release occurs in a given year. If any pages are

found to be out of compliance, changes will be made to remediate the identified accessibility issues.

Onpoint, with input from the IDOI Program Manager and the Advisory Board is also prepared to address the following additional scope of work to ensure the successful implementation of the Indiana APCD, including:

1. **Ensuring the security of the data.** Data security is of utmost importance to Onpoint and our clients. Onpoint's data security policies and standards have been developed to ensure that PHI and PII are protected from unauthorized access. Our Information Security Program (ISP) is HITRUST certified, a gold standard in health data security. The ISP is continuously updated to address new environmental risks and ensure that best practices are followed and contemporary safeguards are employed.

   All data sets delivered on behalf of our clients adhere to data use agreements approved by clients that govern security standards that must be followed and guidelines for appropriate data use, public reporting, and data destruction, for example. No public-facing reporting produced by Onpoint will contain PHI or PII. Additionally, summary-level public reporting will adhere to standards for blinding and cell suppression from CMS and to IDOI-specific standards if more stringent. Onpoint also will ensure compliance with any privacy and security safeguards established by the IDOI Program Manager and the Advisory Board.

2. **Protecting the privacy of the data in compliance with State of Indiana and federal law.** Information privacy and security are critical priorities to Onpoint's business operations and reputation. Onpoint has been vetted and reviewed for privacy and security compliance by all of our state government clients and has successfully achieved both HITRUST certification and CMS Qualified Entity Certification Program (QECP) security compliance, requiring the successful and repeated completion of exacting security accreditation processes. HITRUST is a healthcare-specific common security framework covering the relevant components of security frameworks from the U.S. Health Insurance Portability and Accountability Act (HIPAA), the International Organization for Standardization (ISO), the Payment Card Industry (PCI), the U.S. National Institute of Standards and Technology (NIST), and others.

   Onpoint has developed and maintains a robust Information Security Program to ensure our compliance with state and federal privacy and security laws and regulations. Onpoint's security team is familiar with several of Indiana's privacy and security statutes, including the Cyber Incident Reporting Law (HEA 1169), data breach notification statutes (IC 4-1-11, 24-4.9), Social Security number release statute (IC 4-1-10), insurance data security statute (IC 27-2-27), and data disposal regulations (IC 24-4-14). If awarded the APCD Administrator contract, Onpoint will work with the Indiana Office of Technology's cybersecurity team to ensure compliance with Indiana law and any applicable standards set out in the State's Information Security Framework.

3. **Incorporating and utilizing 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.** Onpoint has in-depth experience integrating non-claims data with APCD data, most often through person-, geographic-, or provider-level linkage, enriching and expanding the possibilities for reporting. For our APCD clients, Onpoint currently integrates a range of non-claims data sources, including laboratory results and other clinical data, vital records

(e.g., birth, death, cancer), U.S. Census, social determinants and survey data (e.g., Behavioral Risk Factor Surveillance System (BRFSS)), Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) patient experience, socioeconomic data, incarceration, chronic disease management program, and more. When linking non-claims data at a provider or member level, Onpoint will work with the IDOI team to ensure that the necessary patient and provider identifiers are included to allow for the best match to members and providers in the APCD. This process starts with providing process documentation and working closely with the State and those providing the non-claims data to ensure a smooth and efficient process with the highest possible match rate.

4. **Ensuring uniform data collection and determining 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.** Onpoint will work with the State to develop a data submission guide (DSG) that will become the basis for standardization in both the content and format of data submissions. Our data integration platform, Onpoint CDM, will be configured to enforce compliance with the submission specifications contained in the DSG, including acceptance thresholds at the element level. Data submissions to the Indiana APCD will be required to pass a broad array of data quality validations (DQVs) that are imposed at the payer, file, and element level at progressive stages of processing. Files will not move to the next stage of processing without meeting the State's thresholds for acceptability. DQVs and acceptance thresholds are reviewed and updated regularly based on scrutiny of incoming data, client input, and evolving analytic uses.

   After submissions have successfully passed all automated quality assurance checks, a wholistic battery of quality assurance reporting will be undertaken by a dedicated analyst specializing in Indiana's APCD data. This reporting will compare the most recently consolidated data against national, Indiana, and payer-specific benchmarks and trending over time. Any data anomalies will be investigated, documented, and communicated to IDOI prior to release and to the State's end users in thorough documentation that accompanies each data set.

5. **Auditing the accuracy of all data submitted and providing audit results in a report format agreed upon by the State of Indiana**. To audit arriving data – including fee-for-service (FFS) and capitated claims and other file types – Onpoint CDM employs a library of more than 2,000 automated data quality validations (DQVs) along with element-specific acceptance thresholds. DQVs are applied against data submissions at the payer, file, and element levels. Onpoint CDM is configured to ensure that submissions meet the specifications established in the state's DSG. We will collaborate with the IDOI team to assess the need for market-specific quality assurance procedures. The State may have unique insurance products, benefits design, and coverage rules that may require the collection of new elements in the APCD. If so, Onpoint will install new DQVs and acceptance thresholds to ensure complete and reliable data submissions for those new elements.

   To audit post-processed data, Onpoint produces a set of standard quality assurance reporting and investigates any anomalies. [redacted]

[redacted] This summary reporting will be shared with the State, including findings associated with any data investigations.

Onpoint also regularly conducts an annual independent audit process with submitters, which we will use to support Indiana's APCD with input and approval by IDOI. This attestation process provides data submitters with the opportunity to validate that Onpoint has received and processed their data accurately. Each data submitter will receive an audit report that summarizes key metrics for their data spanning the most recent 12-month period, including total record count, total dollars, distinct claim counts, and distinct member counts. This independent assessment is often reassuring to clients, end users, and other stakeholders.

6. **Collecting, aggregating, distributing, and publicly reporting performance data on cost, utilization, and pricing in a manner accessible for consumers, public and private purchasers, health care providers, and policymakers.** The opportunities to leverage Indiana's APCD for public reporting are nearly limitless. It will be important early on to clearly establish the IDOI's vision, audience, and goals for your public reporting initiative. Onpoint will work with IDOI and your stakeholders to translate those goals into a set of reporting options for prioritization. We plan to engage our partner, Briljent, in this facilitation process given their skill and experience in this arena.

   In bringing options forward for the State's consideration, Onpoint will leverage experience designing public-facing reporting solutions as well as lessons learned from other successful consumer-focused reporting tools. We will inventory the major APCD-based consumer sites – those designed by Onpoint and those developed by others – and summarize our findings and recommendations for IDOI. The requirements-building process will be collaborative in nature and employ Agile principles in order to deliver a product that effectively addresses the State's vision and does so in a timely fashion. Indiana's consumer-facing website will be designed to address all RFP requirements.

7. **Sharing data nationally and/or helping to develop a multistate effort if recommended by the Advisory Board.** Onpoint was recognized with a 2021 "Innovation in Data Dissemination Award" by the National Association of Health Data Organizations for our multi-state data sharing initiative across six New England APCD programs. The focus was a common policy interest among the states: Primary care spending. The initiative was led by the New England States Consortium Systems Organization (NESCSO) and employed a distributed data model. This approach required Onpoint to develop detailed specifications, SQL code, and quality assurance procedures so that each state could independently yet consistently run the analysis. The approach was collaborative with much shared learning and results that allowed each state to benchmark against comparable results from other states individual and collectively. Onpoint supported a similar initiative led by the Dartmouth Institute, which was comprised of a Total Cost of Care model demonstration across Michigan, Texas, and the northern New England states.

   If recommended by the Advisory Board, Onpoint is prepared to work similarly with IDOI on a national or multi-state data sharing and/or analytic initiative. Whether a distributed or centralized model is used, the keys to success, in our experience, are collaborative and committed participants and agreement around key process and technical issues.

8. **Sharing data for research and publication purposes if approved by the Advisory Board.** Onpoint has proposed to stand up a secure, cloud-based Analytic Environment as the primary vehicle for providing end users with access to appropriate data and analytic tools (e.g., Tableau, querying tools for Python, R, and SQL) to support approved research publication interests. The Analytic Environment will be tailored to the needs of the State and your user community. Approved data users can query and interact with the APCD data and other data sources using a virtual desktop in a virtual private cloud hosted by Amazon Web Services (AWS). The Analytic Environment is ideal for collaboration among analysts, providing access to the most current data, contemporary tools and technology, expert training, and technical support.

The following proposal provides additional detail regarding the solution components outlined above, the relevant experience and qualifications of Onpoint and our subcontractors, and our proposed approach to ensuring the successful launch of Indiana's APCD.

3.2 Please detail your experience with and approach to providing technical assistance and expertise on projects of similar size and scope.

Onpoint takes an active, hands-on approach to technical assistance – for clients, data submitters, and data users. Our team offers unmatched expertise in all aspects of APCD implementation and operations. On the front end of the data collection process, we rely on certified provider billing and coding experts with expertise in payer adjudication processes and standard transaction sets in order to support states in the development of data collection regulations and submission specifications. Our expertise will be essential to building out a data submission guide tailored to Indiana's policy interests and the planned uses of the APCD.

An experienced, dedicated data operations analyst will support Indiana's APCD submitter onboarding, providing day-to-day, hands-on support throughout the testing and submission process. Onpoint's operations analyst will offer expert support regarding the secure submission options and how to meet quality and completeness standards at each stage of submission validation. Data submitters will be thoroughly trained in how to monitor the status of submissions, request variances, access relevant documentation, and review up-to-date quality and variance reporting at any time. Submitters will be scheduled for one-on-one support calls as needed to ensure timely and smooth onboarding.

In support of researchers and analysts making effective use of the APCD data, Onpoint will assign a dedicated, experienced analyst to support the IDOI user community. Our analyst will provide training and support around efficient and accurate use of the APCD data, including leveraging the array of data enhancements delivered in each extract. Onpoint's data enhancements are tailored to APCD use and are unmatched in their breadth and usability. These enhancements span the application of consolidation logic and member and provider indexes as well as the generation of a wide array of other data enhancements, including:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

Analysts approved by IDOI for use of the Analytic Environment will be provisioned with data access and tools consistent with the State's guidance. Onpoint's infrastructure support team will provide training and will be available for one-on-one end user support as needed. Users will be able to easily request support from the infrastructure team and will be able to track any requests or issues through Onpoint's Jira-based help-desk ticketing system.

By leveraging AWS security services, including AWS Identity and Access Management (IAM), AWS Microsoft Active Directory, and AWS Security Groups, roles and groups are created to enforce consistent role-based access to the Analytic Environment and consistent network traffic control. Onpoint will help IDOI identify the appropriate user groups to properly manage IDOI's user base and will create corresponding groups within the data access layer. As new users are identified, Onpoint will provision them with new workspaces and the agreed-upon tools consistent with our proposed solution.

Onpoint will enhance the ability of end users to understand and use the data sets that we deliver through documentation, transparency into technical processes and methodology, and a comprehensive training and support model. We will ensure effective ongoing support to IDOI and authorized data users by providing:

- Dedicated analyst resources who have a detailed understanding of Indiana data – its content, data enhancements, any known limitations, and nuances
- A help-desk service and ticketing system for triaging support questions and requests
- Individualized support and end-user webinars to troubleshoot questions and support use of the data sets and tools within the Analytic Environment
- Useful, up-to-date documentation to support efficient use of the State's analytic data sets
- Training in the use of Onpoint's Analytic Environment and data schemas

Onpoint also organizes user group sessions for all of our clients and their authorized data users to build a knowledge base that helps them use APCD data most efficiently and effectively. Recent user group topics have included an exploration of alternative payment models (APMs) and their importance to APCDs, an overview of Onpoint's quality assurance processes, a review of our enhanced medical claim service-line flags and how to use them appropriately, and a review of how COVID-related claims are impacting trends in APCD reporting.

3.3 Please detail your experience with and approach to prioritizing security and protection of personal identifiable information ("PII") and protected health information ("PHI") data.

Onpoint has nearly 20 years of experience in deploying and operating APCDs in full compliance with state and federal privacy and data security laws as well as national security frameworks. Our systems have been in steady operation in service to APCDs and other clients, with zero incidence of accidental disclosure of PHI or PII with more than 50 billion records received and processed since Onpoint's first APCD launched in 2003.

Information security and privacy are critical priorities to Onpoint's business operations and reputation. Onpoint has developed and maintains a robust Information Security Program (ISP) that complies with all of our state and federal government clients and has successfully achieved both HITRUST certification, the gold standard in health data security, and CMS Qualified Entity Certification Program (QECP) security compliance, requiring the successful and repeated completion of exacting security accreditation processes. HITRUST is a healthcare-specific common security framework covering the relevant components of security frameworks from the International Organization for Standardization (ISO), the U.S. National Institute of Standards and Technology (NIST), the U.S. Health Insurance Portability and Accountability Act (HIPAA), and others

The scope of Onpoint's ISP includes all functional areas within Onpoint and the activities of our employees, consultants, and contractors. Our ISP establishes Onpoint's compliance goals and information security policies, designates an individual responsible for information security, outlines information security documentation requirements, and governs our ongoing security awareness training program. Aspects of Onpoint's ISP include the following:

- **Data storage.** All data are stored using secure storage, including physical media, laptops, and digital databases. [redacted] All electronic PHI is stored in encrypted format, and redaction is performed on database access points based on client requirements.
- **Data encryption (at rest and in transit).** All data is encrypted in motion and at rest using, [redacted] Data submissions are required to be PGP encrypted prior to transmission and must be transmitted over SFTP or HTTPS protocols. Data stored within Amazon Simple Storage Service (S3) leverages Amazon Sever Side Encryption.
- **Access to applications and client data.** Onpoint employs the HIPAA principle of "minimum necessary" for internal and external users who have access to data. Multi-factor authentication (MFA) is enforced on all external endpoints that serve PHI data, including the AWS Console and the Analytic Environment.
- **User rights.** User rights and privileges are tightly controlled at the network, application, and database layers. Here, too, "minimum necessary" remains the governing principle.
- **Portal security requirements.** All externally facing applications are tested by third-party security firms prior to being released to production. Encryption and password policies, including complexity and automatic expiration/renewal requirements, are implemented in the portals. MFA is enforced in all portals providing access to PHI data.

All components of Onpoint's infrastructure dedicated to hosting the IDOI's APCD are located within the continental United States in data centers that are SOC-2 certified and FedRAMP-compliant. A SOC-2 Type II audit report will be provided annually to IDOI along with the findings from our HITRUST audit and certification upon request, documenting how our infrastructure and company practices meet the five Trust Services Criteria of security, availability, confidentiality, privacy, and processing integrity. Onpoint's Information Security Committee (ISC) meets monthly to review the effectiveness of and compliance with our policies and standards.

In addition to adhering to strict physical and system security protocols, Onpoint uses a standard multi-tiered approach to secure data submissions and storage. This approach includes: (1) the transfer of files using only SFTP or Hypertext Transfer Protocol Secure (HTTPS) to ensure an

encrypted transmission tunnel; (2) file-level encryption prior to transmission using the OpenPGP standard and signed by a sender registered with Onpoint; (3) field-level masking/encryption to protect all PHI and PII elements; and (4) media encryption to ensure that all physical disks and tapes, including regular back-ups, are encrypted when data is at rest.

3.4 What funding sources would you seek to offset costs to implement and maintain the database?

Foundational to generating the financial support necessary to cover the up-front and ongoing costs of Indiana's APCD program will be raising its visibility, demonstrating its value, and, in the process, garnering political support. Our experience in other states points to the need for a multi-pronged financial sustainability model since no one funding source is likely to cover the full costs of the program. Potential funding sources include the following:

- **General support through an appropriation by the Indiana General Assembly.** It is typical for an APCD program to receive a portion of its funding through general budget appropriations. Key to securing this funding will be to identify a champion of the APCD within the sponsoring agency and Assembly, in our experience. Leveraging the APCD for high-profile health policy analysis is useful in maintaining program visibility and ongoing funding.
- **Interagency support by other state agencies.** Multiple states with APCDs have negotiated support from other state agencies that see value in the database. One way of engaging other agencies is to invite their participation in some type of joint governance, oversight, or advisory committee.
- **"Medicaid match" dollars from the federal government through IAPD.** Under federal Social Security Law (Title XIX, "Grants to States for Medical Assistance Programs"; Sec. 1903, "Payment to States"), state Medicaid programs participating in certain healthcare initiatives and infrastructure improvements can apply to have their dollars matched by the federal government through Federal Financial Participation. For programs not already participating in this matching initiative, funds can be accessed by submitting an application using Implementation Advance Planning Documents (IAPDs). There are two avenues, both of which are currently being leveraged by APCDs: The first provides a 50% federal match, while the second provides a 90% federal match to the state Medicaid program's 10% contribution for the design, development, and implementation of the system (shifting to a 75%/25% match for ongoing maintenance and operations).
- **Federal and foundation grants.** In developing a long-term funding strategy for Indiana's APCD, the State may want to consider foundation and government-sponsored grant opportunities. These opportunities could include:
  - Federal funding of APCD development at $2.5M will become available as part of the U.S. Health and Human Services Department's Consolidated Appropriations Act, which could offset start-up costs.
  - Alternative payment models (APMs) supported through the Center for Medicare & Medicaid Innovation (CMMI) or other programs at the U.S. Centers for Medicare & Medicaid Services (CMS) are a potential source of funding that could reasonably support the development of Indiana's APCD. There continue to be models that require multi-payer participation, data aggregation, and reporting, which could rely on the Indiana APCD as its data source.

  - Indiana's health plan-affiliated foundations (e.g., the Health Foundation of Greater Indianapolis, the Indiana Health Care Foundation, the PHP Foundation at the Physicians Health Plan (PHP) of Northern Indiana) may support APCD-based public transparency reporting, for example.
  - National foundations that invest in payment reform, performance transparency, and targeted research regarding health policy issues or interventions (e.g., the Arnold Foundation, the Robert Wood Johnson Foundation, West Health, the Peterson Foundation) are another funding source that is worth exploring.
- **Data and product sales.** Once in production and generating data products – and assuming that Indiana's APCD release regulations will permit broad accessibility – APCD revenues can be generated from a variety of deliverables, including:
  - Subscriptions to the Analytic Environment (i.e., role-based access to approved data sets accompanied by a suite of analytic tools)
  - Sales of data products, including public use files, limited use files, Safe Harbor files, and custom extracts
  - Additional fees associated with access to a business intelligence (BI) reporting tool or data enhancements (e.g., quality measures, groupers)

Typical customers include researchers, commercial entities, advocacy organizations (e.g., hospital and medical associations), health systems, health plans, and Accountable Care Organizations.

3.5 Please describe your approach to and experience with data sharing across multiple states and/or the nation. What is your approach to handling non-Indiana data sets?

Onpoint has experience with data sharing both nationally and across multiple states, which offers Indiana crucial advantages and opportunities, including:

- Leveraging lessons learned through our work standardizing data across multiple states and regions in both distributed and centralized data models that involved standardized collection specifications, quality assurance procedures, and analysis and reporting plans. These initiatives primarily focused on common health policy or research interests (e.g., primary care spending, total cost of care, pediatric quality of care).
- Engaging with other APCD clients to meet, collaborate, and share information with Indiana regarding both standard operating models (e.g., submission compliance and enforcement, emerging payment models, expanded data collection, quality assurance standards) and opportunities for collaboration and learning (e.g., benchmarking, performance measurement, policy-oriented studies, standards).

Recent examples of Onpoint's data sharing initiatives, including an overview of the approaches taken, include:

- **New England States Consortium Systems Organization (NESCSO).** Onpoint was selected by the six-state consortium of New England state health departments to perform a regional primary care spending study using a distributed data model that leveraged the APCDs in each of the participating states. Onpoint worked iteratively over a six-month period with a multi-state advisory group to develop specifications, establish quality assurance procedures, and oversee comparative reporting across the region. Onpoint's

integration of data from all six New England states' APCDs was used to assess the percentage of overall healthcare spending being invested in primary care services based on claims data for 7.2 million commercial, Medicaid, and Medicare members. The initiative received the 2021 "Innovator in Data Dissemination Award" from the National Association of Health Data Organizations.

- **CMS Comprehensive Primary Care Plus (CPC+) model.** Onpoint's most complex multi-vendor IT initiatives have been part of our role as a contractor to the federal government. As a subcontractor on the CMS Data Feedback and Reporting Tool contract, Onpoint worked collaboratively with multiple other technology and services vendors to stand up a national reporting platform for one of CMS's largest alternative payment models, CPC+, which reached 5,500 practices in 18 regions nationally. Our role began with developing quality, utilization, and cost measures and refreshing the reporting platform on a quarterly basis with updated measure results. We worked with the Chronic Care Data Warehouse vendor, GDIT, to gain access to Medicare data and to build and disseminate measures. We built a formal data exchange process with RTI, which was responsible for creating provider attribution files needed for measurement and reporting, and with the prime contractor, Deloitte and then NewWave Technologies, automating the report refresh cycle within the business intelligence platform.
- **Comagine Health's participation in national demonstration projects.** A regional health improvement collaborative, Comagine Health contracts with Onpoint to manage its Oregon Data Collaborative, which involves management of a statewide voluntary APCD and generation of performance reporting by provider group and region. We have supported Comagine's participation in two national demonstrations that involved multiple other states and regions. First was the CMS Comprehensive Primary Care initiative in which Comagine participated as one of 18 regions, following a consistent primary care payment model with measurement and incentives around a standard set of performance measures. Second was Onpoint's support of Comagine's participation in a national demonstration of HealthPartners' Total Cost of Care model in which multiple regions across the country followed a standard approach to implementing a set of measures approved by the National Quality Forum.

Onpoint's approach to the integration of non-Indiana data sets to support broader analysis than possible with the APCD alone would start with a profile of the new data source, including its content, structure, and limitations. Non-claims data sources would require linkage to the APCD using member, provider, geography, or some other common element(s), depending on the data source. Onpoint has extensive experience successfully linking APCD data with other sources – from public health registry and Census data to clinical and program data, for example.

3.6 Will the proposed solution conform to the Assistive Technology Policy (Section 508) and the State's architectural standards? If not, is there a plan to migrate the application to conform to the Assistive Technology Policy (Section 508) and / or the State's architectural standards, and what is the timeline? Will your company maintain the solution to conform to the Assistive Technology Policy (Section 508) and the State's architectural standards?

Onpoint's proposed solution will conform to the Assistive Technology Policy (Section 508) and the State's architectural standards. Onpoint follows industry-best practices in the design of our online solutions, including compliance with the Americans with Disabilities Act. Design features encompass the use of alternative image text, following color-contrast guidelines, and allowing for

keyboard navigation. To ensure that we maintain our solution's conformance to these standards, Onpoint will regularly perform Section 508 compliance testing, as noted in our response to Question #3.1, above.

3.7 Describe any additional value-added services not otherwise mentioned in your proposal.

Onpoint's proposed solution is designed to meet all of the State's requirements without any additional services not already included in our proposal. Depending on the State's interests, there may be opportunities to expand the scope of services provided in the following areas at IDOI's direction:

- **Sustainability planning.** The State may wish to engage Onpoint or our subcontractors in the pursuit of federal funding under an IAPD process, for example, or to engage potential data users in the planning for marketable data products.
- **Regulatory development.** Onpoint or our subcontractors could support the development of detailed data collection and release regulations or data governance policies and guidelines to support Indiana's APCD program operations.
- **Analytic enhancements.** Depending on the analytic use cases that emerge in Indiana for the APCD, Onpoint is prepared to deliver additional data enhancements. These could include a more expansive set of NCQA-certified HEDIS measures, additional groupers beyond those included in this proposal, provider directory services (if the State wants to roll up individual providers to groups or systems), or an application to support a review and reconsideration process to the extent required prior to public reporting, for example.
- **Policy and program analysis.** In Onpoint's work with insurance regulators and agencies in other states, our analytics team has supported numerous policy and program analyses. Recent work has included analysis, modeling, and evaluation services associated with Washington State's price transparency reporting, surprise billing legislation, mental health parity legislation, primary care spending legislation, global expenditure target legislation, and public option legislation; Covered California's primary care spending analysis, PPO provider network performance analysis, and seriously ill population analysis; Maryland's privately insured market analysis; Rhode Island's Comprehensive Primary Care program; and Vermont's all-payer CMS waiver, price transparency program, and Hub & Spoke opioid treatment program.

4. Design, Development, and Implementation

4.1 Please describe your approach to design, develop, and implement the APCD to align with the State's expectations. Include detailed steps and key milestones.

Overview

Onpoint anticipates using a hybrid Waterfall/Agile approach to design, develop, and implement the Indiana APCD project. For the standard elements of the project – project milestones, tasks, deliverables documentation, and progress reporting, for example – we plan to employ a traditional Waterfall approach.

For the elements that require software development, we will rely on an Agile approach in which two-week sprints are organized, priorities are set, resources are assigned, progress is reported, and adjustments are made as each sprint is completed. Onpoint follows the Agile and Scrum software development life cycle (SDLC), using an iterative approach to ensure that our user interfaces are intuitive, adhere to best practices, and allow for the deployment of frequent, incremental releases. New development and software bugs are tracked through the Jira ticketing system to ensure rapid resolution. All critical system errors will be documented and resolved through Onpoint's Agile SDLC process prior to launch. Onpoint will review any known issues with IDOI throughout the implementation process to align on the priority of individual issues. All non-critical issues will be documented and assigned expected resolution timelines for IDOI's review and feedback and will have interim mitigation strategies in place.

Deliverable Approach

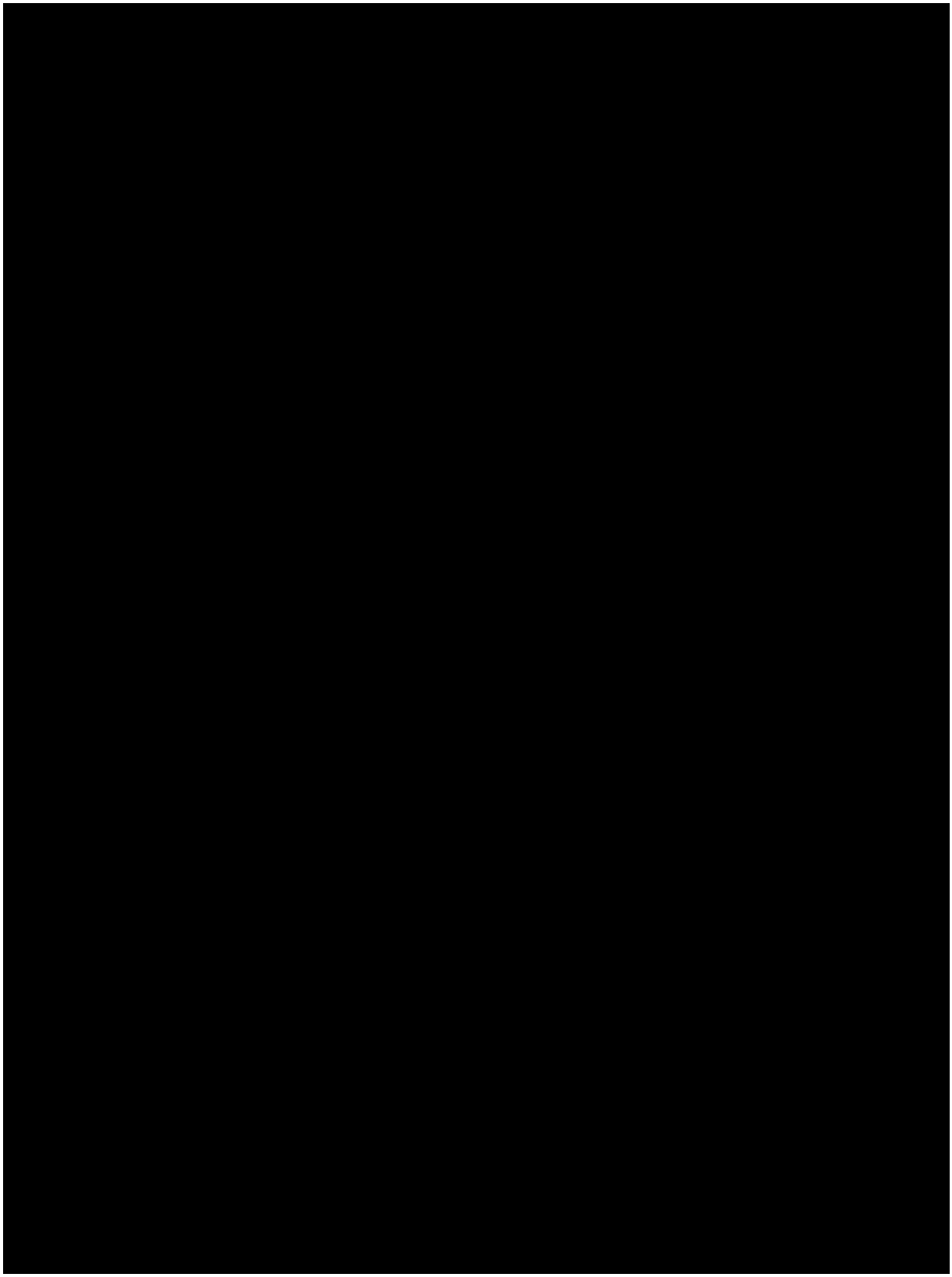
During the planning process, we will work collaboratively with IDOI, providing technical assistance and lending our expertise to address the following key components:

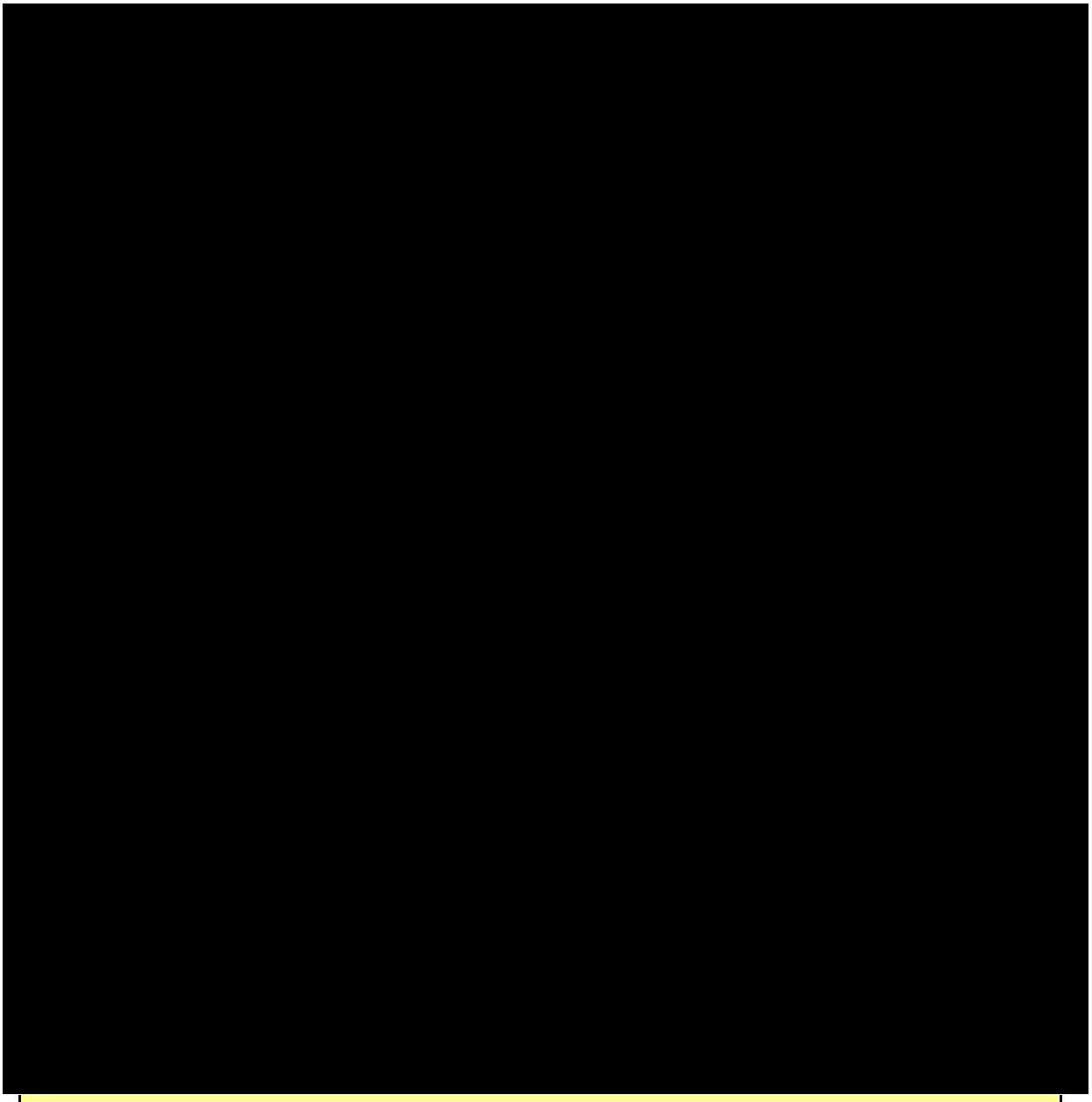
- **Project objectives.** For project success, it will be critical to spend the necessary time up front to gather requirements, defining, reviewing, and confirming IDOI's project objectives and documenting them in specific, measurable tasks and subtasks with clear due dates.
- **Statement of work and deliverables.** The Agreement between Onpoint and IDOI will include a detailed statement of work (SOW) and a list of deliverables, high-level timeline, and assumptions.
- **Schedule.** A work breakdown structure will be used to determine what needs to be delivered and when.
- **Milestones.** Key project milestones and deadlines will be established with input from IDOI and incorporated into the project schedule.

The Work Plan will be guided by IDOI's goals and deliverable schedule (see **Table 4.1.A** below) and will be updated regularly to continue to align with the priorities of the IDOI. This table also is included in Section 8 ("Project Management") to ensure a comprehensive response in case the sections are reviewed by different evaluation team members.

Table 4.1.A. Work Plan

REVISED 2.15.2022





After all deliverables and planning documents have been approved by IDOI, Onpoint will begin executing all steps required to deploy the database in the agreed-upon timeline. Key to each successful APCD implementation is transparency into the processes, enhancements, and data quality steps taken at each critical step and stage. To this end, Onpoint will ensure that IDOI staff have ample opportunities throughout implementation to undertake thorough user acceptance testing (UAT) according to our Test Plan, which Onpoint will prepare for the state for all key APCD functions.

Onpoint will adhere to the State's requirements and will complete all following activities prior to the APCD system launch:

- Provide access to nonproduction environments to the State team for User acceptance testing (UAT)

- 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

4.2 Describe your network and database model. Provide an architectural diagram of your proposed solution, including all hardware / infrastructure required for the application to operate, including backup and disaster recovery.

Network & Database Model Overview

Onpoint's proposed solution is delivered in a Software-as-a-Service (SaaS) model using an Application Programming Interface (API), which removes the burden of managing technology infrastructure and software for our clients. [redacted]

[redacted] **Figure 4.2.A**, below, provides a visual overview of the current Onpoint CDM technology stack.

Figure 4.2.A. Onpoint's Technology Stack (Overview)

Additional system-design details are provided below and in **Figure 4.2.B**:

- **Data integration solution front end.** Our data integration solution's front end has been designed using [redacted] All Onpoint web applications are thoroughly tested by Onpoint technical staff, external users (including submitters and clients to ensure a user-friendly experience), and third-party security experts to ensure adherence to secure coding practices.
- **Back-end databases.** The database technologies utilized by the system are [redacted]
- **Restful API.** An API provides a communication interface between the front-end and back-end databases as well as between the processing pipeline and the back-end databases. Employing an API has several advantages, including interoperability between systems, the ability to evolve and change front-end and back-end systems while keeping

the business logic intact, and its ability to function as a single source of truth for business logic.

- **Data processing pipeline.** Onpoint's data processing system utilizes the [redacted]

Figure 4.2.B. Data Storage Hosting Diagram

[redacted]

Back-up & Disaster Recovery

Onpoint's Business Continuity Plan and Disaster Recovery Plan are critical components of our business operations and Information Security Program. These plans are updated on an annual basis and as needed in the event of major system changes. The plans serve as guides for the recovery of normal operations following any disaster that affects the delivery of information technology services in accordance with our performance standards and contractual obligations.

The plans cover the recovery of all supporting systems, applications, and data. All client-facing and mission-critical systems are backed up at least daily with a retention policy of at least two weeks. All other systems are backed up daily to weekly, depending on the criticality of the system.

Architecting our systems in the Amazon Web Services (AWS) cloud gives Onpoint the flexibility and resources to achieve a short Recovery Point Objective (RPO) and a rapid Recovery Time Objective (RTO). By utilizing AWS to provide the infrastructure for our systems and solutions, any failure of a critical system would be exceptionally rare, with recovery often imperceptible to end users. All Onpoint systems are architected with a 99.9% uptime service-level commitment.

Onpoint follows NIST 800-88 guidelines for sanitizing devices at end of life to ensure secure data disposal. Hard drives, which contain only encrypted data per standard policy, are overwritten and then shredded. Copies of Onpoint's Business Continuity Plan and Disaster Recovery Plan will be made available for IDOI's review.

4.3 Describe the host architecture and the secure means that will be used by State employees to access the data warehouse remotely.

Onpoint has developed, implemented, and operated role-based data access and reporting systems for nearly 20 years. Onpoint maintains rigorous access control and oversight of the data in our systems. Both of the client-facing solutions that are foundational to our secure, end-to-end APCD Platform solution – Onpoint CDM for data intake/integration and the Analytic Environment for data access and analytics – employ role-based data access protocols for all credentialed users.

Onpoint requires all data submitters to register, be approved, and receive role-based credentials via secure email prior to submission or gaining access to Onpoint CDM's secure online portal. Onpoint CDM provides all credentialed users with access to real-time reporting regarding the stage and status of submitted files. This role-based functionality allows data submitters to view the progress of all of their (and only their) submitted files across all reporting periods. Onpoint and client staff are assigned a different role and thus have a broader view: The ability to look across all data submitters and all reporting periods at any time to fully monitor the status of all submissions to the APCD. Onpoint works closely with our clients and their data submitters throughout the project to regularly identify and confirm their users and assign role-based permissions with the appropriate level of access.

The Analytic Environment also employs role-based access control for our clients' analysts and data users. Through the use of Amazon Web Services (AWS) security tools, including AWS Identity and Access Management (IAM), AWS Microsoft Active Directory, and AWS Security Groups, roles and groups are created to enforce consistent role-based access and consistent network traffic control across services. Users are assigned to groups (e.g., data analysts, data users) based on client requirements. [redacted] dditionally, the Analytic Environment provides users with access to only their authorized data sets (e.g., comprehensive extracts, custom data sets, limited/researcher data sets), which can be adjusted at any time based on client requests and requirements.

As an additional safeguard, Onpoint approaches all data access using a "minimum necessary" standard, including both internally and externally facing systems. Within Onpoint CDM, access to sensitive data is provisioned at the client and data element levels, requiring additional approval on a case-by-case basis for access to protected health information (PHI), which is otherwise redacted. Onpoint leverage AWS Lake Formation to manage this access. All externally facing applications

are tested by third-party security firms prior to being released to production. Encryption and password policies, including complexity and automatic expiration/renewal requirements, are implemented in the portals. MFA is enforced in all portals providing access to PHI data using the DUO two-factor authentication solution.

4.4 Describe the storage technology and an estimate of storage type and size required to sustain the State's data warehouse.

Onpoint's proposed solution for IDOI's APCD will provide scalable, secure storage that is segregated from our other clients' data. Based on the numbers provided in the State's RFP, we estimate that Indiana's APCD will require [redacted]

Scalable. Our data storage solution leverages several AWS services, [redacted]

Secure. All data received, processed, and stored by Onpoint is encrypted in motion and at rest using, [redacted] npoint employs the HIPAA principle of "minimum necessary" for both internal and external users requiring access to data. Access to applications and data must be approved and go through a formal change-control process prior to being granted. Multi-factor authentication (MFA) is enforced on all external endpoints that serve potentially sensitive data, including the AWS Console and the Analytic Environment.

Segregated. All data stored for IDOI's APCD functions will be stored separately from other clients' data. This includes additionally segregated storage for the State's Medicare data and Medicaid Managed Care programs to comply with their applicable security and storage requirements. This segregated storage will be provided using AWS's highly scalable and secure cloud solutions as described above.

4.5 Describe your data management approach, including data definitions and organization, data standards that you intend to adhere to within the warehouse, and how you intend to enforce data consistency standards across the warehouse.

Onpoint's data management approach is based on delivering APCD services through a Software as a Service (SaaS) model that includes our market-leading data integration solution, Onpoint CDM (Claims Data Manager).

Onpoint CDM. Onpoint CDM's SaaS model encompasses the technology, training, support tools, and expert staff required to efficiently support an all-payer claims database (APCD) system. Onpoint CDM provides tools for secure submission, cleanses and standardizes incoming data,

performs rigorous quality review, and then aggregates, consolidates, and enhances the data to support analytics. Most importantly, Onpoint CDM is a proven APCD platform with a record of successfully collecting billions of insurance claims and enrollment records from more than 345 payers on a monthly or quarterly basis. The platform has been continuously enhanced over time to address changes in billing standards and payment models and to meet the evolving analytic use cases that a contemporary APCD must support. Onpoint CDM leverages the AWS cloud and guarantees 99.9% uptime. Throughout, the system is overseen by dedicated quality assurance analysts and IT experts to make sure that our clients' data is securely stored, efficiently processed, and reliably delivered.

Data definitions. Onpoint will provide submitters with a comprehensive data submission guide (DSG) that details data submission standards, including file-naming conventions, file-structure specifications, and data element definitions and formats. These data definitions provide clear guidance to submitters on the reporting expectations for each data element, including listing valid values for each data element and mapping to national standards (e.g., CMS-1500, UB-04, X12) to ensure consistent reporting across all payers.

The DSG also will outline the threshold percentages that payers will be expected to achieve – not only for each element's completeness, but also for each element's completeness with *valid* data. All program documentation, including the DSG, will be easily accessible for download at any time via Onpoint CDM's online portal.

Data organization. Onpoint CDM is architected to flexibly handle submissions using any format – traditional APCD, APCD-CDL™, CMS standard layouts, state or payer specific, etc. – with all submitted fields mapped to data elements within our comprehensive data warehouse. Onpoint stores our clients' data in an enterprise system that has been designed to handle large volumes of data, leveraging a data model that is organized so that data can be easily queried, consistently processed, and systematically delivered to clients.

For each of our APCD clients, Onpoint retains both the originally submitted data files as well as the historically submitted "raw" data values from submitters in our operational datastore. We leverage AWS's Simple Storage Solution (S3), which offers a secure, reliable, and scalable storage solution in the cloud. We also leverage various types of Elastic Block Storage in the AWS cloud. All client data is virtually segregated from other client data.

Data standards. Onpoint CDM's data integration systems leverage a robust cloud-based infrastructure that employs a series of complex extract/transform/load (ETL) algorithms to standardize, cleanse, and consolidate the submitted data.

During annual review sessions, Onpoint works with key stakeholders to examine new billing standards and codes, evaluate changes to existing thresholds/acceptance criteria in light of improved data quality, create new validations based on any issues that have surfaced and evolving

analytic use cases, and review current and proposed focus areas to target enhancement efforts for maximum support of data users.

Onpoint's standard approach to data quality involves trending analysis and comparisons to quality benchmarks and includes reporting for submitters to review for accuracy. Data trending includes evaluations of the number of members enrolled, claim volumes, total dollars paid and charged, PMPM statistics, percent of claims supported by enrolled members, and other profile statistics. Trending analysis is performed both before and after the data is transformed, allowing QA analysts to investigate data anomalies that are highlighted by the aggregation process. Final quality validation is done post-aggregation across the complete data set and prior to release to end users to ensure that all files included in each data extract are accurate, complete, have referential integrity, and align with expectations and national benchmarks. These post-aggregation analyses and validation checks are part of a formal and rigorous process by which Onpoint flags outliers and finalizes documentation of any data anomalies, their impact on analytics, and any remediation efforts that have been or will be performed.

Reference data. Onpoint CDM includes more than 200 reference tables that cover a large range of code sets to support validation on arriving data and look-ups across delivered data sets. Licensed reference tables include:

- ICD-10 diagnosis and procedure codes
- Procedure codes
- Current Procedural Terminology (CPT)
- Healthcare Common Procedure Coding System (HCPCS)
- Code on Dental Procedures and Nomenclature (CDT, also known as Current Dental Terminology)
- Health Insurance Prospective Payment System (HIPPS) procedure codes
- Standard claim billing codes (e.g., UB-04, CMS-1500, X12 HIPAA)
- National Plan and Provider Enumeration System (NPPES)
- RED BOOK® prescription drug information containing a crosswalk with National Drug Codes (NDCs) to enable linkage to drug names, generic names, therapeutic class, Drug Enforcement Agency (DEA) classifications, and other NDC-related attributes

Additional reference tables for claims and eligibility include detail around enrollment code sets (e.g., coverage type codes, market category codes, HIOS exchange product codes) and other national standard reference tables (e.g., taxonomy specialty codes, race, ethnicity, Federal Information Processing Standards (FIPS) county codes).

4.6 How flexible is your system architecture?

Onpoint CDM has been securely managing submissions of a wide range of file types (e.g., eligibility, encounter, medical claims, pharmacy claims, dental claims, members, providers, cost, lab) and layouts (e.g., APCD-CDL™, CCW, T-MSIS, and custom) for nearly 20 years across multiple states. Onpoint's systems are flexible and agnostic to file structure or layout. Our approach is always to adapt to the file structures and layouts that will meet the needs of our clients and their submitters most effectively. We have successfully onboarded a wide range of plans with varying abilities and experience in the data submission process, including commercial and workers' compensation, Medicaid FFS and managed care plans, and Medicare FFS and managed care plans.

As noted above, Onpoint CDM's integration systems leverage a robust, cloud-based infrastructure to perform a series of complex yet flexible data transformation processes that standardize, cleanse, and consolidate the received data. Onpoint CDM is architected to flexibly handle submissions using any format – state or payer specific, traditional APCD, APCD-CDL™, CMS standard layouts, etc. – with all submitted fields mapped to data elements within our comprehensive data warehouse. Onpoint CDM also is easily adaptable to intake data from certain payers (e.g., Medicaid) that include unique services and supplemental file types.

Onpoint CDM's processing engine is hosted in the cloud by Amazon Web Services, offering our clients a solution that can scale rapidly and automatically. On a regular basis, Onpoint CDM processes files from more than 345 submitters covering nearly 80 million covered lives. This includes the submission of multiple file types per source – eligibility, medical claims, pharmacy claims, dental claims, provider, alternative payments, clinical, and more – as well as any resubmission and replacement files.

Onpoint CDM currently processes and validates 35 million records per hour and is scalable both vertically by adding more server power and horizontally by adding more compute nodes without interruption to the end user. This scalability allows our systems to process large file volumes efficiently, with Onpoint CDM's data quality validations and operations and analytic staff reviewing the data to ensure ongoing accuracy and data quality to meet our clients' established extract schedules on time.

Our solution additionally offers a flexible suite of standard data enhancements that can be configured to meet IDOI's needs. These enhancements are time-tested, transparent, APCD-specific tools that our clients rely on every day to make efficient and effective use of their delivered data sets. Standard data enhancements include:

- [redacted]

[redacted]

4.7 Explain how unstructured data elements (e.g., emails, imaged documents, forms, reports, etc.) are managed.

AWS provides readily available analytics tools such as [redacted]

4.8 Can the proposed product or solution integrate with Access Indiana (https://www.in.gov/inwp/access-indiana/)?

The public-facing transparency website hosted by Onpoint can integrate with Access Indiana, and Onpoint will work with IDOI to identify valuable use cases for including this integration. Onpoint's other products are not designed for use by the general public, and Onpoint CDM is designed for submitters to leverage for data collection initiatives across multiple states and therefore uses initiative-agnostic credentials.

4.9 Outline any issues your solution would encounter with utilizing Access Indiana, if any.

Onpoint's Analytic Environment leverages technologies such as AWS Directory Service to provide a seamless and secure experience across multiple third-party tools hosted within user workspaces. In its current implementation, this requires authentication within Onpoint's environment.

Onpoint CDM is designed such that data submitters can have one access point for many data collection initiatives (i.e., all states in which they do business). This benefit requires that user authentication be consistent across initiatives, which is why Onpoint hosts this authentication process. Onpoint would need to separate users into multiple accounts in order to support Access Indiana, potentially negating this benefit for Indiana submitters.

4.10 If the proposed solution cannot currently accommodate Access Indiana, what actions and their accompanying timelines would need to be completed for utilization?

Onpoint proposes leveraging Access Indiana for the public-facing transparency website, which would facilitate access for all Indiana citizens. The other pieces of our solution have a narrower user group and would maintain standard Onpoint authentication mechanisms. If integration is required for these products, Onpoint can redesign aspects of our authentication process, which will require significant development and testing time as well as comprehensive security reviews to ensure that Onpoint's system maintains compliance with HITRUST security guidelines. This design and development would add as many as six months to the implementation timeline.

4.11 Can the proposed product or solution leverage existing State Data Exchange platforms (GoAnywhere for flat file movement, Mulesoft for integration and API development)?

Onpoint CDM is a SaaS solution, complete with AWS-hosted SFTP and direct Amazon S3 delivery options for external data exchange, which do not directly leverage the tools identified. MuleSoft provides Amazon S3 connectors, which IDOI may be able to leverage when interacting with S3 buckets hosted by Onpoint.

4.12 Are your company's servers shared among multiple customers or dedicated to one customer?

Onpoint's solution leverages Amazon Web Services (AWS) cloud-based services for all data storage and processing. AWS uses a multi-pronged approach – leveraging identity management, network security, serverless and container services, host and instance features, logging, and encryption – to build logical security mechanisms that ensure the separation of data and security information between different customers that are physically located in the same data center.

Within the AWS infrastructure that we employ, Onpoint segregates client data in different locations and uses different sever instances to process data. Each client's Analytic Environment is built in a separate Virtual Private Cloud (VPC) with isolated networking, databases, and servers.

4.13 How is load balancing performed for all of your customers within each data center, as well as between the primary and secondary data center, if applicable?

Onpoint's systems are built in the AWS cloud with redundancy across multiple data centers. Should one server or data center fail, the application will failover to another server or data center. Elastic load balancers are utilized to manage high-availability services and distribute network traffic.

4.14 Identify the tools that will be used to develop and / or maintain the solution; include software, development tools, database management system, testing tools, data conversion tools, training tools, etc. Include licensing, and other requirements and ensure fees are included in the Other Costs tab of Attachment D – Cost Proposal. Please ensure that no pricing information is included in this answer.

As part of our proposed solution, Onpoint will be using the tools outlined below in **Table 4.14.A** for software development, database management, testing, data conversion, service delivery, support and issue tracking, and training.

Table 4.14.A. Tools Used in Onpoint's Proposed Solution

[redacted]

4.15 Provide details of minimum client and server hardware and software (including operating systems, plug-ins, libraries, etc.) required to access and use the application. Also, provide details of the recommended client and server hardware and software (including operating systems, plug-ins, libraries, etc.) for optimal application performance.

Onpoint's solution does not require the Indiana to install, purchase, or maintain any special hardware or software. The Onpoint CDM portal can be accessed through any standard web browser. The Analytic Environment is a virtual Windows desktop that can be accessed through the free AWS WorkSpaces client, which is available on Android, iOS, Fire, Mac, Windows, Chromebook, and Linux devices.

4.16 What coding language(s) do you recommend for this application and why?

Onpoint CDM leverages various coding languages for different use cases. [redacted]

Onpoint's core data processing engine leverages Java and Apache Spark to ensure that data is processed in an efficient and scalable manner.

Users within the Analytic Environment have their choice of various languages to interact with the data. Onpoint's solution includes tools that support the use of SQL (DataGrip), R (RStudio), and Python (Anaconda) for analytic querying.

4.17 Describe your coding strategy / standards used to develop applications.

Onpoint's standard approach to systems development follows the Agile and Scrum systems' development life cycle (SDLC) methodology, which extends from requirements discovery through analysis, design, development, testing, and deployment. On a daily basis, our team participates in Scrum sessions that support an iterative, rapid-cycle development process. Key aspects of our approach are detailed in the following section.

Product roadmap and prioritization. Onpoint's product team is responsible for defining and prioritizing Onpoint's product roadmap. Product owners conduct regular and ad hoc client interviews to gather feedback on our existing products and collect enhancement and major feature requests so that we can prioritize based on client impact, applicability to other clients, and industry trends. These enhancements are continuously rolled out to all of our APCD clients as part of our SaaS model.

Sprints ensure ongoing enhancements. Product releases usually occur at the end of a team "sprint," which typically lasts two weeks and provides for the rapid and continuous enhancement of Onpoint's products and our clients' deliverables. Using this approach, Onpoint's products are continuously iterated with minor releases occurring on a frequent basis. Major releases occur when a new product is released or when a major system component is changed substantially.

Our product owners work with both internal and external stakeholders, including clients, coordinating with our client account managers to capture development requests and prioritize them in the product backlog, which is continuously groomed to ensure that the most important features and user stories rise to the top for the next sprint. Client account managers facilitate client scoping sessions for major feature requests as needed.

Sprints begin with planning sessions during which development requests are reviewed to determine requirements, the high-level design approach, and the feasibility for incorporating into the product. During these planning sessions, product owners review the backlog with the team and facilitate the group's discussion to determine the full scope of the next sprint.

Software and systems testing. Onpoint performs testing throughout the various stages of our system development lifecycle. We use Jira to track all development tasks whether they are enhancements or bug fixes. As part of any Jira development task, a quality assurance analyst develops a test plan to ensure that the development task meets its expected objectives. Developers working on the task write unit tests in conformance with the test plan. These tests are then executed and must be passed before code is incorporated into the main code branch. Onpoint uses Jenkins to run automated unit and regression tests using the following steps:

1. The developer commits code to the source code repository using a source control tool (e.g., Bitbucket).

2. Jenkins creates a new build with the new code commit incorporated into the latest successful build.
3. The build runs through automated unit and regression tests.
4. If all testing passes successfully, the build is approved for release at the next scheduled deployment. If the build breaks, the development team is notified that fixes are required.

When applicable, load testing of applications is performed in a staging environment prior to release to the production environment. Load testing is performed on client-facing systems. In addition to software testing, Onpoint's QA analysts run automated and manual tests on data outputs to ensure that the data meet QA acceptance standards and will be sufficient for downstream analyses and reporting. All development and testing are performed on representative test data. No client PHI/PII is used in any development or testing environment.

4.18 Describe secure coding methods used.

Onpoint follows Open Web Application Security Project® (OWASP) best practices in secure coding, and all developers undergo yearly secure coding training as part of Onpoint's HITRUST certification process. These methodologies include but are not limited to best practices in authentication and password management, input validation, access control, logging, communication cryptology, and database security.

Application networking is limited wherever possible to ensure appropriate traffic, and all software is scanned and reviewed by third-party organizations to ensure application security. Any identified issues are prioritized and addressed within Onpoint's standard development process. Onpoint follows strict maintenance schedules to ensure that any vulnerability due to third-party tools is addressed, including patches for critical vulnerabilities as needed.

4.19 Do you have peer review for coding changes? Describe the peer review process.

Yes, Onpoint's development team performs regular code review of newly developed features. Peer reviewers are identified at the start of each sprint for given tasks and pull requests must be completed before code can be deployed to the test environment. Onpoint conducts technical review sessions each week during which critical new work is discussed with key technical staff and architectural and implementation details are approved. Each sprint also ends with a sprint review that includes demonstrations of all new software to the entire product development team and other key stakeholders.

4.20 Describe your application / code versioning strategy and processes. How will code / configuration be promoted?

Onpoint uses a four-tier environment – development → test → stage → production – for product development. All system development occurs in the development environment and is migrated to the test environment only after development is complete and all unit tests have passed for the sprint tasks. Once a release passes the testing phase, which includes thorough regression and system testing, it is deployed to stage where internal users, clients, and other external users can

perform user acceptance testing. While in stage, performance and load testing are conducted to ensure that the new release meets performance expectations. The stage environment is used only in instances where load testing is necessary or access is needed for individuals outside of the product development team. This step may be skipped if product updates do not require this type of testing. Once this phase is approved, the release is deployed to production.

All development requests – whether standard maintenance, a bug fix, or an enhancement – are entered and prioritized in the product backlog. Any serious software flaw is addressed as a hot fix and deployed as soon as possible. Hardware and other application upgrades and patching follow a similar lifecycle, with all application and hardware changes first deployed to a test environment for thorough evaluation prior to being deployed to production.

The Analytic Environment is designed for querying production data using third-party analytic tools and, accordingly, has only a production environment as all software updates are production releases from these third-party organizations.

This systematic yet flexible approach is strengthened by Onpoint's use of Atlassian, an industry-leading project management and collaboration platform that includes Jira and Confluence. Onpoint uses Jira for tracking all planned and unplanned software application and infrastructure tasks. Confluence is used for documentation of product requirements, technical designs, and technical operating procedures. Bitbucket is used for software code version control.

4.21 Explain how you will provide the State's team with access to nonproduction environments during implementation?

Key to each successful APCD implementation is transparency into the processes, enhancements, and data quality steps taken at each critical step and stage. To this end, Onpoint will use our systems and previous APCD experience to quickly begin data collection and system testing to ensure that IDOI staff have ample opportunities throughout implementation to undertake thorough user acceptance testing (UAT) of all key APCD platform functions prior to release. These include the following:

- **Onpoint CDM.** Onpoint will be configured to provide access to a non-production instance of Onpoint CDM for IDOI user acceptance testing. Onpoint will provide training to State users in Onpoint CDM, the data submission, data quality, variance, and approval processes. If elected to do so, State users will be able to perform user acceptance testing of the implementation of the IN APCD, including the configuration of the file layouts, application of the data quality validations, and the associated thresholds by submitting files to Onpoint CDM and following the files' progression as they are processed by the system.
- **Submitter testing.** All submitters have the ability to submit test files via Onpoint's CDM portal at any time. These test files often are used during onboarding to verify accurate coding of submitters' data files and also are helpful to test updates related to DSG changes or whenever submitters undertake system changes. Although test files can contain true "test" data, Onpoint CDM is engineered with the same security controls for all files and allows submitters to instead use actual production data, if desired, from their systems to verify that their data is being pulled correctly. This approach improves Onpoint's ability to validate submitters' actual data and helps submitters' shift to production submissions more seamlessly.

File submissions to Onpoint CDM can be flagged as either "test" or "production" to prevent any test files that contain sample/fake data from entering the system. Regardless of this flag, all file submissions interact with Onpoint CDM using the same workflow and validation processes, allowing credentialed users to access a real-time view of their files' workflow, including updates on file statuses, data completeness, and variances. Each test file undergoes the same formatting, data completeness, and data quality validations as a production file. Submitters are able to view detailed data quality feedback within Onpoint CDM, and submitters receive a series of automated emails that summarize each file's data quality status upon file submission and each stage of file processing. Onpoint's dedicated Operations analysts will review the data quality results of the submitted test files, follow up with submitters on the status of their test files, and work with submitters to remediate any issues that need to be addressed to enter the production phase successfully.

- **Analytic Environment.** During implementation, Onpoint will collaborate with IDOI in creating the business and technical specifications to meet the needs of IDOI and your end users. We will gather all requirements from IDOI through a series of working sessions. Onpoint can share our experience on best practices and provide recommendations on user-friendly and analytic-enriched extracts based on feedback from other end users. Once extracts have been created and delivered, a user acceptance period will be provided for testing and final sign-off by IDOI.

  Following completion of each quarterly extract, Onpoint will provide IDOI with a release notes package. The release notes will detail any changes in data structure and field assignments since the preceding extract, identify which submitters' data is included in the extract, detail the completeness of the data using triangulation reporting, indicate any data issues that have been identified and retained in the data, and offer information about enhancements or data findings relevant to data research and analysis. To ensure that integrated and enhanced quarterly extracts meet IDOI's acceptance criteria, IDOI will have a user acceptance testing (UAT) window to review the data delivery prior to release to all users.

- **Public-facing consumer website.** During implementation, Onpoint's team will develop a public-facing website as directed by IDOI through an iterative process. A test environment will be used for developing and will host the UAT. IDOI staff will be able to view and approve all changes within this environment. Upon completion of the UAT period, the updates will be promoted to the production environment during a scheduled maintenance window. Any accessibility or functionality issue identified with the website will be logged and tracked through Onpoint's Jira-based ticketing system and addressed in a timely manner.

  Each subsequent website refresh will include a UAT period, during which IDOI staff will have the opportunity to provide feedback regarding recent updates and desired changes. Users will have access to a limited-access test environment in which the updated website will be made available. Users will have two weeks to review the website changes and provide feedback. Onpoint will document any feedback and work with IDOI to identify a prioritized list of all issues that must be addressed before release to production. Onpoint will update the website based on this feedback and reopen the website for a second round of UAT. Any remaining issues will be addressed during this period before the website is released to the general public.

  Before each UAT period, Onpoint's designated Project Manager will work with IDOI to identify all changes required for the latest refresh. These tasks will be outlined for

Onpoint's web development team at least a month prior to the UAT period, allowing for sufficient time to make required changes.

4.22 Describe the process that will ensure the most recent version of the application / code will be placed in escrow and made available to the State if needed.

[redacted]

4.23 What mechanism would you propose to provide a flexible methodology and tool to allow the IDOI quickly and easily to identify the physical locations in Indiana where a health care provider currently practices and similarly find specialized providers near a given physical location in Indiana?

a. This provider locator tool must contemplate and incorporate solutions for providers that practice at multiple work locations (hospitals, clinics, offices, etc.).
b. Describe the functionality of the provider locator methodology, including a description of how business rules are incorporated and can be adjusted as needed.
c. Provide a supplement to the Cost Proposal Template (as a separate attachment; not as part of this Technical Proposal response) to reflect any added expense/income associated with this enhancement.

Onpoint regularly creates a master provider index to identify unique healthcare providers, facilities, and other healthcare providers across payers and time using best practices. We have been developing master provider indexes for more than a decade. Onpoint's provider clustering process involves a complex series of algorithms, internal and external reference files, and automated and manual-review linkage steps. Our provider clustering solution assigns persistent unique IDs to providers no matter their role (e.g., PCP, rendering, prescribing, billing, attending) and no matter their type (e.g., individuals, facilities, pharmacies) to enhance linkage results.

Our clustering process also incorporates national reference files, including a monthly subscription file from CMS's National Plan and Provider Enumeration System (NPPES). This information is integrated into our Provider Master table, enabling us to regularly update provider information. This data is utilized to enhance our provider linkage process and serve as an independent "source of truth" for provider identity resolution, improving the assignment of unique provider IDs. Similar to NPPES, Onpoint creates only one master record per unique National Provider Identifier (NPI).

The development of a provider locator tool would begin with the generation of the master provider index and utilize the provider information reported to the APCD. This would require geographical information indicating where services have been provided, which usually is included in the claims submissions with detailed address-level information. Additional provider location information may be reported in a separate provider file.

Depending on the reliability of the information reported by submitters, supplemental provider files can be integrated into the APCD, including provider-to-practice rosters and provider registries.

To facilitate this process, Onpoint has received provider registry data from external sources, integrating and clustering the external provider data with the APCD. The format of this data exchange can be tailored to the needs of IDOI. Onpoint CDM's data intake and extraction process can be leveraged to exchange provider information on a regular basis via SFTP, allowing for clustered data to be sent to IDOI and third-party vendors as needed. An API interface also can be provided to allow for requests of the provider data as needed. In this event, Onpoint would work with IDOI to define the access needs and format requirements of this interface.

A supplement to the Cost Proposal Template can be found as a separate attachment included in our response and has not been included as part of this Technical Proposal response. For details, please see Onpoint's Cost Proposal supplement: "Onpoint - IN RFP 22-70302 - 2.5.4 - Cost Proposal Supplement (2022-04-04).pdf".

5. Security and Privacy

5.1 Provide all applicable security and privacy policies that your organization maintains.

Onpoint CDM and Onpoint staff have been handling secure file submissions – eligibility, medical claims, pharmacy claims, dental claims, provider, alternative payments, clinical results, and more – for nearly two decades across multiple states and from more than 345 submitters across the commercial and government markets.

Using guidance from the U.S. National Institute of Standards and Technology (NIST), Onpoint has developed and maintains a robust information security program with policies that are compliant with both the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, ensuring the security and confidentiality of patient-identifiable data. Onpoint is HIPAA compliant and HITRUST certified. (HITRUST is the gold standard in health data security, and its common security framework encompasses all relevant and appropriate HIPAA and NIST security requirements.)

Onpoint maintains an up-to-date Security Plan that covers our daily operations across all applications, platforms, and clients and which is attached to this proposal as the following confidential exhibit: "Onpoint - IN RFP 22-70302 - Technical Exhibit 2.4.5.1.A - Security Plan (Confidential).pdf". If selected for contract award, Onpoint can work with IDOI to provide additional policies and plans from our information security plan that are of interest.

5.2 Review the State's Information Security Framework and either confirm that your company conforms to the policy or provide explanation to the areas for which your company does not conform.

Onpoint can conform to Indiana's Information Security Framework. Onpoint has nearly two decades' experience in understanding, applying, and complying with both state and national safeguards as well as our clients' program-specific rules. Our systems have been in steady operation in service to APCDs and other clients since 2003, with more than 50 billion records

received and processed with zero incidence of accidental disclosure of protected health information (PHI) or personally identifiable information (PII).

5.3 Describe your logical security measures (e.g., software safeguards for your organization's systems, including user identification and password access, authentication, access rights and authority levels) in place.

Information security and privacy are critical priorities to Onpoint's business operations and reputation. Highlights of logical security measures include:

- Infrastructure design and security best practices are followed to meet HITRUST and other third-party audits
- All systems are located in a Virtual Private Cloud (VPC)
- Except for front-end applications, production systems cannot be directly logged into by users
- [redacted]
- [redacted]
- All systems are built for high availability and failover across Amazon Web Services (AWS) availability zones with 99% or greater uptime
- Each client's data is always encrypted and segmented from other clients' data
- Systems employ 24/7 real-time system monitoring and alerting
- Systems are managed and monitored by cloud-certified engineers
- All system access is logged and monitored
- All networks and systems are tested by third-party security professionals
- Real-time firewall and log analysis are performed by event management systems and personnel at a third-party security partner
- Several risk assessments are performed annually

5.4 What physical security measures do you have in place (e.g., key cards for caged areas, maintenance and support areas, etc.)? Are surveillance cameras at the entrance to your facility?

[redacted]

All sensitive data is stored in AWS data centers in the continental United States. AWS employs a variety of physical security measures including:

- **CCTV.** Physical access points to server rooms are recorded by closed-circuit television (CCTV) cameras. Images are retained according to legal and compliance requirements.
- **Data center entry points.** Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized AWS staff utilize multi-factor authentication (MFA) mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.
- **Intrusion detection.** Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate AWS personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide MFA before granting entry or exit. As noted above, these devices will sound alarms if the door is forced open or held open. Door-alarming devices also are configured to detect instances in which an individual exits or enters a data layer without providing MFA. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

5.5 Are security guards on duty at all times? If not, what is the current security guard schedule?

[redacted]

5.6 Are locked cages, cabinets, and racks required to be used?

As noted in our responses to questions #5.4 and #5.5 above, all AWS data centers are thoroughly locked down, and access is tightly controlled and monitored. For additional detail regarding AWS data center security controls, please see: https://aws.amazon.com/compliance/data-center/controls.

5.7 Are non-employees allowed entry to the data center floor or development areas?

When approved individuals are on site at AWS data centers, they are given a badge that requires multi-factor authentication and limits access to pre-approved areas. Even AWS employees who routinely need access to a data center are given permissions to only relevant areas of the facility based on job function. AWS employee access is regularly scrutinized as well. Access lists are routinely reviewed by area access managers to ensure that each AWS employee's authorization is still necessary. If an AWS employee does not have an ongoing business need to be at a data center, they are required to go through the visitor process.

5.8 Are firewalls shared across several customers or does each customer have its own firewall?

[redacted]

5.9 How is one customer prevented from accessing another customer's data? What is your company's client data isolation scheme?

All data stored for each of our APCD clients is stored separately from other clients' data, both during the data enhancement process as well as within the Analytic Environment. This separated storage is provided using AWS's highly scalable and secure cloud solutions. Additionally, each client's Analytic Environment is hosted within their own AWS Virtual Private Cloud (VPC), so users querying the data are in a different network with no connection to other clients' storage locations.

5.10 What application and infrastructure intrusion detection programs are in place? What mechanisms are in place to provide real-time alerts for intrusion detection?

[redacted]

5.11 What mechanisms are in place to protect against service attacks?

[redacted]

5.12 Has anyone ever compromised the integrity of your network? If so, what happened and what was the response?

Since launching our first APCD solution in 2003, Onpoint has securely received and processed more than 50 billion records with zero incidence of network compromise or accidental disclosure of PHI or PII. Onpoint has successfully achieved both HITRUST certification, the gold standard in health data security, and CMS Qualified Entity Certification Program (QECP) security compliance, requiring the successful and repeated completion of exacting security accreditation processes. Onpoint also has met the security requirements of every state Medicaid agency with which we have worked.

5.13 Are the data centers audited and / or certified? Provide details of Server Scans details, etc.

Third-party testing of AWS data centers ensures that AWS has appropriately implemented security measures aligned to the established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing

of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment. AWS supports more security standards and compliance certifications than any other cloud provider, including PCI-DSS, HIPAA/HITECH, SOC, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.

5.14 Where do you propose to store the data within the continental US? Where is the data housed (e.g., mainframe, client server, local, data center, cloud)?

a. If a cloud solution is proposed that is not SaaS, could it be hosted in the State cloud tenants?
b. If a data center is proposed, is the data center owned and operated by your company or do you subcontract out this functionality? If subcontracted, identify the subcontractor(s).
c. Describe the security measures in place at that facility.
d. Is redundant power supplied to the cabinets / facility?
e. Describe all major power failures you have experienced. Are power failures tested? How often?
f. Do you provide remote operations for your data center(s)?
g. Describe the backup and recovery procedures you have in place.
h. Describe your planned outage windows. Does the State have any authority to delay / postpone an outage if that outage would cause issues with critical business processes during that outage?
i. Describe your strategy and process for hardware, software, operating system patching / upgrades / updates.

If a cloud solution is proposed that is not SaaS, could it be hosted in the State cloud tenants?

Onpoint's proposed cloud solution is a SaaS solution.

If a data center is proposed, is the data center owned and operated by your company or do you subcontract out this functionality? If subcontracted, identify the subcontractor(s).

All of Onpoint's systems are hosted in the cloud on infrastructure operated by Amazon Web Services (AWS), with all system resources located inside of the continental United States in data centers that are SOC-2 certified and FedRAMP-compliant.

Describe the security measures in place at that facility.

Please see our responses to questions #5.4 through #5.7, above, which describe the security measures in place at AWS data centers.

Is redundant power supplied to the cabinets / facility?

AWS data centers' electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures that their data centers are equipped with back-up power supply to ensure that power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Describe all major power failures you have experienced. Are power failures tested? How often?

Onpoint has never experienced any issues due to power failures at the AWS data centers that we use. It is the responsibility of AWS to test for power failures.

Do you provide remote operations for your data center(s)?

This is not applicable; AWS is responsible for managing and operating the data centers that we use.

Describe the back-up and recovery procedures you have in place.

Onpoint's solution leverages AWS cloud-based services for all data storage and includes flexible and automated back-up and recovery configuration. [redacted]

[redacted]

Onpoint regularly performs disaster recovery testing, restoring prior versions of databases to ensure efficient recovery in the event of an incident, and will perform this function annually. In the event of an issue requiring restoration of a back-up, Onpoint will provide on-demand support to resolve the issue within 24 hours of the occurrence.

Describe your planned outage windows. Does the State have any authority to delay / postpone an outage if that outage would cause issues with critical business processes during that outage?

Onpoint performs regularly scheduled maintenance on a monthly basis. Regular maintenance periods are conducted Friday during off-peak periods, with email notifications provided to end users that may be impacted (e.g., submitters, credentialed users of the Analytic Environment). Onpoint will notify the State if critical updates or patches need to be made outside of this regularly scheduled period. Onpoint will work with the State if there is a need to delay or postpone an outage that would impact critical business processes.

Describe your strategy and process for hardware, software, operating system patching / upgrades / updates.

Onpoint performs regularly scheduled patching and maintenance on a monthly basis as noted above.

5.15 What type of application scans does your company provide and at what frequency?

[redacted]

5.16 Describe your organization's policies and procedures related to background checks for personnel that are assigned to develop applications.

All employees undergo a background check before employment.

5.17 How would you ensure the following?

a. That data is submitted and released in a machine-readable format;
b. That the data from the database is used in an ethical manner; and
c. That the data is not personally identifiable and is properly secured and maintained, and that the Respondent complies with federal and State health care privacy law?

Onpoint would ensure Indiana's concerns in the following manner:

a. That data is submitted and released in a machine readable format

In each of our APCD engagements, data is submitted to Onpoint for the APCD as delimited text files that can be produced universally by any payer and are machine readable. In working with hundreds of data suppliers across the country, we have found this to be a reliable approach for payers. Beyond simply making data machine readable, Onpoint has extensive experience working with many states to establish a standard format for data submissions so that data is standardized and of the highest quality. Payers are provided with a detailed data submission guide prior to programming their data submissions and are offered ongoing opportunities for training and support to ensure that they are able to submit data in a uniform manner.

For data release, Onpoint sends files as delimited text [redacted] which are universally machine readable by industry-standard data integration software.

b. That the data from the data base is used in an ethical manner

An APCD can be an incredibly valuable data resource for states to measure healthcare outcomes, utilization, and cost and to answer critical questions regarding public health, provider performance, and the impact of policy interventions. However, it is important that there is a transparent process in place to ensure that the APCD data is used in an appropriate and ethical manner. For our APCD clients, Onpoint often has supported the client in establishing a data request application and review process to ensure adequate review and has built appropriate data products for release following extensive design review. Many APCDs establish a data release committee that convenes to review and approve data request applications and ensures that the proposed data uses are compliant with state and federal laws and any program-specific guidance. A strong example is Washington State's APCD, which offers an online page detailing data requests and available products: https://www.wahealthcarecompare.com/wa-apcd-data-requests.

c. That the data is not personally identifiable and is properly secured and maintained, and that the person complies with federal and state health care privacy laws

Onpoint has employed a variety of methods to ensure that released data is not personally identifiable and is properly secured and maintained. Onpoint has experience creating de-identified Safe Harbor data sets (in which all identifiers are removed) as well as data sets that have been de-identified in accordance with HIPAA's "Expert Determination" method using statistical techniques. We also create limited-use data sets (in which most identifiers are removed) and analytic-use data sets in which the data is aggregated and enriched so that it can support many use cases without being personally identifiable.

The data release process, detailed above, should include a review of recipients' data management procedures to ensure that the data will be appropriately secured and maintained. For the most sensitive data sets, Onpoint typically offers data access via our role-based secure Analytic Environment. Data users must use multi-factor authentication to log in to the Analytic Environment, after which they can interact with their approved data in a familiar Windows-like environment with their choice of analytic tools. Permissions and connections to the Analytic Environment are tightly controlled, providing our clients with important reassurance that the data is secured even when being accessed by approved users outside of state government.

When Onpoint staff are required to access a client's data – most often to support analytics or provide quality assurance – the state's data is used only for purposes approved by the state. Access to sensitive data by Onpoint's analysts is approved only by management on an as-needed basis. Data is encrypted at all times, and all users are authenticated using multi-factor authentication.

5.18 How will you keep Medicare data isolated as needed or required to ensure proper handling and for purposes of data release or analysis?

The Medicare data stored on behalf of each of our clients is stored separately to comply with CMS's applicable security and storage requirements. This segregated storage is provided using AWS's highly scalable and secure cloud solutions.

5.19 How do you ensure the confidentiality and security of health plan member information, medical records, and data?

Onpoint's Information Security team is led by our Security Officer and backed by a full team of dedicated information services and information technology professionals. Onpoint has successfully achieved both HITRUST certification, a gold standard in health data security, and CMS Qualified Entity Certification Program (QECP) security compliance, requiring the successful and repeated completion of exacting security accreditation processes. Additionally, the AWS infrastructure that we utilize operates data centers in alignment with the Uptime Institute's Tier III+ guideline, has been granted FedRAMP Provisional Authority-To-Operate (JAB P-ATO), and has been granted Defense Information Systems Agency (DISA) provisional authorization for Impact Level 2.

All components of Onpoint's infrastructure dedicated to hosting our clients' APCDs are located within the continental United States in data centers that are SOC-2 certified and FedRAMP-compliant. Onpoint's Information Security Committee (ISC) meets monthly to review the effectiveness of and compliance with our policies and standards.

In addition to adhering to strict physical and system security protocols, Onpoint uses a standard multi-tiered approach to secure data submissions and storage. This approach includes: (1) the transfer of files using only SFTP or Hypertext Transfer Protocol Secure (HTTPS) to ensure an encrypted transmission tunnel; (2) file-level encryption prior to transmission using the OpenPGP standard and signed by a sender registered with Onpoint; (3) field-level masking/encryption to protect all PHI and PII elements; and (4) media encryption to ensure that all physical disks and tapes, including regular back-ups, are encrypted when data is at rest.

Once within Onpoint's systems, data remains protected from unnecessary access. Onpoint employs the HIPAA principle of "minimum necessary" for both internal and external users who have access to data. Access to applications and data must be approved through a formal change-control process completed prior to being granted. For proper safeguarding of PHI received from Medicare, originally submitted data is stored separately and protected with two-way encryption technology per individual client DUAs with CMS.

5.20 What are your processes for ensuring the privacy and security of data transmitted to or from and stored in your system? Describe your data encryption. How will you provide encryption services for data at rest? How will you provide encryption services for data in transit? Is sensitive data cryptographically hashed?

Onpoint's Information Security Program (ISP) includes the following safeguards related to data transmission and storage:

- **Data storage.** All data are stored using secure storage, including physical media, laptops, and digital databases. [redacted]
- **Data encryption (at rest and in transit).** All data is encrypted in motion and at rest [redacted]
- **Access to applications and client data.** Onpoint employs the HIPAA principle of "minimum necessary" for internal and external users who have access to data. Multi-factor authentication (MFA) is enforced on all external endpoints that serve PHI data, including the AWS Console and the Analytic Environment.
- **User rights.** User rights and privileges are tightly controlled at the network, application, and database layers. Here, too, "minimum necessary" remains the governing principle.
- **Portal security requirements.** All externally facing applications are tested by third-party security firms prior to being released to production. Encryption and password policies, including complexity and automatic expiration/renewal requirements, are implemented in the portals. MFA is enforced in all portals providing access to PHI data.

5.21 What is your protocol for handling a data breach? What safeguards are in place to protect the data from breaches?

Following guidance from NIST, Onpoint's Information Security Program (ISP) meets or exceeds breach notification as required by section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act as well as federal and our state clients' security breach notification laws. Onpoint also conducts data breach exercises on an annual basis using table-top scenario walkthroughs, escalation procedures, and training for all staff.

Since launching our first APCD solution in 2003, Onpoint has securely received and processed more than 50 billion records with zero incidence of network compromise or accidental disclosure of PHI or PII. Our responses the questions throughout this section detail many of the safeguards that we have in place to protect our clients' data from breaches.

5.22 What are your plans to mitigate technology risks, whether from failures or external threats?

Onpoint's solution is cloud-based and leverages Amazon Web Services (AWS). As such, data is stored redundantly within Amazon's facilities, data center sites are selected for environmental stability, and data centers are secured with best-in-class physical security protocols.

Additionally, various monitoring tools are employed within Onpoint's infrastructure, including support for the Analytic Environment. Utilizing AWS monitoring tools [redacted]

Onpoint employs an external cybersecurity firm to monitor all access to our environments, with reports reviewed on a daily and monthly basis by Onpoint's security team. Onpoint adheres to strict security policies and processes and monitors and tracks all access/change control requests to all data, systems, and environments.

Onpoint uses the tools described above as well as [redacted]

5.23 What are your current practices regarding auditing and reporting on the effectiveness of your controls for security, availability, processing integrity, confidentiality, and privacy? Provide any relevant information related to audits describing the effectiveness of your nonfinancial controls.

Onpoint is HITRUST certified. As part of that annual certification process, the effectiveness of our controls for security, availability, processing integrity, confidentiality, and privacy are rigorously audited and tested. Please see the following exhibit: "Onpoint - IN RFP 22-70302 - Technical Exhibit 2.4.2.7.A - HITRUST Letter.pdf".

5.24 Confirm that your organization is compliant with all HITRUST CSF requirements. Is your organization HITRUST CSF Validated? Does your organization currently have a valid HITRUST CSF Certification?

We confirm that we are HITRUST CSF certified and validated. Please see the following exhibit: "Onpoint - IN RFP 22-70302 - Technical Exhibit 2.4.2.7.A - HITRUST Letter.pdf".

5.25 What is your experience with National Center for Health Statistics (NCHS) processes and documentation? Identify any other national or industry standards that you have adopted and implemented and indicate whether your security controls are currently in compliance with those standards. Provide a detailed explanation, including number of years.

We have not been asked before to work with any National Center for Health Statistics (NCHS) processes or documentation. For more than six years, Onpoint has successfully achieved both HITRUST certification, the gold standard in health data security, and CMS Qualified Entity Certification Program (QECP) security compliance, requiring the successful and repeated completion of exacting security accreditation processes. Onpoint also has met the security requirements of every state Medicaid agency with which we have worked. Additionally, we have demonstrated compliance with HIPAA and adherence to National Institute of Standards and Technology (NIST) guidance for our Information Security Program's standards, policies, and procedures. There tend to be significant overlap in the security controls required by these standards, making it likely that Onpoint could meet any standards from the National Center for Health Statistics (NCHS) that are critical for Indiana.

5.26 What type of security protection training do you conduct for your employees?

Workforce security, access management, and user awareness training are important components of Onpoint's Information Security Program. Onpoint requires a series of annual trainings for all staff that cover important topics such as HIPAA statutes and additional security and privacy standards, regulations, and policies. Additionally, we provide regular security bulletins to employees and have a standing security agenda item at our weekly all-staff meetings. As part of security awareness training, we regularly conduct mock social engineering exercises to train our employees to ensure vigilance against phishing attacks and other threats.

5.27 Do you employ two-factor authentication before personnel can access sensitive records?

Yes, multi-factor authentication (MFA) is enforced on all external endpoints that serve PHI data. [redacted]

5.28 Who will have access to the data collected by the APCD (and specifically access to sensitive health care and financial data) in your organization? Will those individuals in your organization who have access to the data collected by the APCD be assigned role-based security access? Will they be able to view details at the individual claim level?

Onpoint maintains rigorous access control and oversight of the data in our systems. Both of the client-facing solutions that are foundational to our secure, end-to-end APCD Platform solution –

Onpoint CDM for data intake/integration and the Analytic Environment for data access and analytics – employ role-based data access protocols for all credentialed users.

Additional security measures include role-based access rights and HIPAA-compliant audit trails that include the logging of all key management operations. Onpoint employs the HIPAA principle of "minimum necessary" for internal and external users who have access to data. Data access to sensitive data is approved by management on a case-by-case, as-needed basis and at a minimum-needed standard.

When specific Onpoint staff are required to access a client's data – most often to support analytics or provide quality assurance – the state's data is used only for purposes approved by the state. In such cases, claim-level detail is available for the minimum duration necessary. Access to sensitive data by Onpoint's analysts must be approved by management on an as-needed basis. Data is encrypted at all times, and all users are authenticated using multi-factor authentication.

5.29 Will subcontractors be used to perform services related to data collected by the APCD? If so, in what capacity? How long has/have the subcontractor(s) been providing services related to this RFP (if applicable)? How long, and in what capacity, have you been working with each of the proposed subcontractors (if applicable)?

Onpoint has carefully selected three Indiana-based subcontractors to complement our team with Indiana-based subject matter expertise and supplemental support:

- Briljent is an Indiana-accredited women business enterprise (WBE) that will be providing project management support
- Haystack is an Indiana-accredited minority business enterprise (MBE) that will support the development and deployment of the State's public-facing website
- Vespa is an Indiana-accredited, veteran-owned small business (IVOSB) that will support our team's data architecture optimization and security

While Onpoint has not yet worked with these Indiana-based partners, we have been meeting regularly with each of them over the past months to review scope requirements, explore approaches, understand the distribution of work, and build relationships so that we are ready to hit the ground running in support of the State's APCD.

Briljent, Haystack, and Vespa will not have access to PHI in this project.

5.30 How will you monitor and audit access to the data warehouse as well as detect and manage unauthorized access?

Security measures include role-based access rights and HIPAA-compliant audit trails that include the logging of all key management operations and data access. As noted above, Onpoint employs the HIPAA principle of "minimum necessary" for internal and external users who have access to data. Data access to sensitive data is approved by management on a strictly as-needed basis and at a minimum-needed standard. By default, Onpoint employee access to sensitive data is redacted.

Additionally, all access to data in Onpoint's Analytic Environment is monitored and logged, enabling access to audit trails, including the flagging of any queries accessing PHI.

5.31 How will you protect the data warehouse from malware and malicious attempts like phishing attacks and ransomware?

[redacted]

5.32 Describe the proposed security architecture and how it will secure communications between the data warehouse and any transactional databases.

[redacted]

5.33 What is your strategy for operating security and middleware security updates and maintenance?

Any middleware that is utilized in Onpoint's SaaS solutions is patched and maintained by the respective provider. All such patching and maintenance are reviewed and vetted by Onpoint's security team, which conducts both daily and monthly reviews.

5.34 How will you ensure the physical security to the data center and any corresponding facilities?

The physical security of the data center is handled by AWS and is detailed above in our responses to questions #5.4 through #5.7.

5.35 Describe the backup process and frequency of backup.

[redacted]

[redacted]

Onpoint regularly performs disaster recovery testing, restoring prior versions of databases to ensure efficient recovery in the event of an incident, and will perform this function annually. In the event of an issue requiring restoration of a back-up, Onpoint will provide on-demand support to resolve the issue within 24 hours of the occurrence.

5.36 Identify and describe your level of NIST compliance, including but not limited to NIST 800-53.

Following guidance from NIST, Onpoint has developed and maintains a robust Information Security Program (ISP) that meets or exceeds:

- Health Insurance Portability and Accountability Act (HIPAA) requirements
- Breach notification as required by section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act
- Requirements put forth for all qualified entities (QEs) for CMS
- State and federal security breach notification laws
- Onpoint is HITRUST certified and implements NIST 800-53 security requirements, including password complexity and encryption at rest and in transmission.

5.37 Please describe how your system complies with each subcategory of the NIST Cybersecurity framework (see https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf for more information). Please be sure your answer addresses each subcategory individually, with the exception of ID.RA-2 and RC.CO-1, which are optional subcategories.

Onpoint maintains an up-to-date Security Plan, which covers our daily operations across all applications, platforms, and clients and which is attached to this proposal as the following confidential exhibit: "Onpoint - IN RFP 22-70302 - Technical Exhibit 2.4.5.1.A - Security Plan (Confidential).pdf". Onpoint's Security Plan lists the relevant NIST controls and subcategories along with details related to Onpoint's implementation of those controls. Onpoint can provide additional supporting detail upon request by IDOI.

6. Data Services

6.1 How would you propose to collect all relevant claims data for the database from a health payer in a manner that would minimize technical barriers for a health payer to submit a claim?

Minimizing barriers for health payers to submit claims to the APCD is critical to ensuring that data is received on a timely basis and is of the highest quality. Following are some of the key considerations:

- Submission portal. One of the largest barriers to effective use of APCDs are data submission delays. Our APCD solution, Onpoint CDM (Claims Data Manager), was created through collaboration with payers across the country, resulting in a user-friendly interface that reduces lag time for data submissions through a payer-optimized workflow. Onpoint CDM is an industry-leading tool that facilitates secure submission uploads, cleanses, and standardizes incoming data, performs rigorous quality review, and then aggregates, consolidates, and enhances the data to support analytics.
- Dedicated support. Accompanying Onpoint CDM's intuitive interface is the support from Onpoint's staff. Onpoint's Data Operations team supports payers by removing submission barriers, working diligently to promote collaborative and results-oriented relationships with payers. Examples of the value of having a dedicated Data Operations team is highlighted in the onboarding process, which can be especially intensive during start-up. Our Operations team helps ensure that payers feel supported, informed, and invested by providing regular all-payer calls and webinars, email updates with helpful tips, notices detailing any upcoming system or rule changes that may impact payers, one-on-one solutioning sessions, and open office hours. Our dedicated Operations staff is also available to address emails, phone calls, and questions anytime they arise.
- Data layouts. Data layouts are always a consideration when working to minimize technical challenges for payers. The use of standard data layouts and standard definitions of data elements enables payers to program their data extract processes more quickly and efficiently. This fosters consistent reporting across payers and improves the quality and volume of data that can be made available for follow-on analytics.
- Documentation. We have found that one of the most important considerations when implementing an APCD's layouts is providing the critical support for payers via accessible staff and detailed documentation (e.g., a data submission guide) that contains clear definitions, mappings, and expectations for each file being provided to the APCD. Onpoint's data submission guides (DSGs) are available 24/7 within Onpoint CDM and are accompanied by FAQs, user guides, and other documentation necessary for payer support.
- Secure submission. Providing industry-standard tools and different options for data submissions is also helpful to minimizing the barriers of submitting data to the APCD. Onpoint supports data submissions via SFTP with PGP encryption as well as an easy, drag-and-drop approach using Onpoint CDM's user-friendly interface. We have found that most payers prefer to submit data using SFTP since this allows for the automation of data submissions, streamlining the process for more timely submissions.
- Claim adjustments. Supporting the multiple ways in which payers store and report claims adjustments to APCDs is another critical consideration. Based on the variation in payers' approaches that our team has encountered across the country, our data integration solution, Onpoint CDM, currently includes nearly 30 consolidation methodologies that reconcile and resolve original claims and their subsequent adjustments to report and deliver a final claim to end users. Included in our library of methodologies are standard versioning and aggregation methodologies as well as customized, payer-specific methodologies. This enables payers to easily report claim adjustments as stored in their warehouse rather than shoehorn adjustments into a one-size-fits-all solution that may not accurately reflect their claims.

- Data quality. All data received by Onpoint are taken through a systematic, multi-phase quality assurance process that includes preliminary integrity checks, initial loading checks, completeness validation, data standardization, consolidation, and trending analysis.

  As data submitters send data to Onpoint, they receive automated emails updating them on the status of their submissions. Credentialed users can log in to Onpoint CDM for on-demand reports and dashboards with up-to-date file quality and status reporting, including a continuous history of all submissions and related statistics on completeness and data quality. If data submitters have questions about their submissions beyond the detailed status reporting available at Onpoint CDM, our Data Operations staff are always available to provide answers, identify further examples of failing records, and assist in investigating any need for a variance.

  Once a submission passes all data quality checks, it is promoted to an approved status (Validation/Pass), the data payer is notified automatically, and the data begins the transformation and loading process into our operational data store for further processing, enhancement, and use in reporting and extracts.

- Transparency. Onpoint CDM's secure portal provides up-to-date information regarding submission compliance and status as well as information on submission quality (e.g., comparison to benchmarks, completeness of fields, validity of codes). Using the secure portal, state staff and their data submitters alike can follow each submission as it moves through the processing queue, accessing comprehensive reporting about submission quality as well as detailed and transparent information about quality validations, identified file errors, and more as show in **Figure 6.1.A**.

Figure 6.1.A. Onpoint CDM Submission Status Dashboard (Demonstration Client)

6.2 How would you work with other states and relevant stakeholders to either use a data language that is already available or facilitate the establishment of a common data language to be used by states for the data? Would you recommend the use of the Common Data Layout (CDL) for All-Payer Claims Databases (APCD-CDL™)?

Onpoint has been at the forefront of data language standardization for APCDs since the market's inception. Working with stakeholders, our approach has been used to implement more than half of the country's functioning APCDs. The greatest lesson that we have learned is that while all states have needs specific to their populations and missions, roughly 90% of all APCDs have common analytic needs. Onpoint's data integration and enhancement platform, Onpoint CDM, supports standardization across states and payers while also allowing for the flexibility required to meet individual client's goals.

The importance of standard submission layouts is twofold. First, for payers that support numerous APCD submission efforts, consistency across multiple states improves timely and consistent data submissions. Second, standard layouts within an APCD create clear expectations, definitions, and consistency that are the foundation for the follow-on analytics that drive change.

Onpoint defines standards and expectations through a comprehensive data submission guide (DSG) that is customized to each client's data collection requirements. The DSG is updated any time collection requirements change and is reviewed regularly with submitters and key stakeholders. The DSG provides submitters with detailed data specifications, including each field's required completeness threshold and denominator as well as mappings to applicable national standards.

Onpoint authored the original APCD standard file layouts that are used nationwide and continues to stay on the cutting edge of data-collection standards. Our team offers unmatched knowledge of APCD data and was an active participant on the steering committee that designed the initial APCD Council's Common Data Layout (APCD-CDL™) and continue to provide input into updates. Onpoint CDM is architected to flexibly handle submissions in the numerous and varying formats specified by APCDs across the country, including the APCD-CDL™ format.

Onpoint has implemented the APCD-CDL™ and all related data quality validations. We would note that while the APCD-CDL™ captures most fields traditionally collected for APCDs, it lacks the inclusion of certain Medicaid fields and allows for limited customization to collect data that may be of specific interest to the State. We would recommend its use in an adaptive format, allowing for the collection of add-on fields (e.g., alternative payment model data) and fields specific to Medicaid programs (e.g., dual eligibility, third-party liability, federal poverty levels) to ensure that Indiana is able to optimize the collected data.

6.3 How would you promote and encourage self-funded plans to voluntarily submit claims data for inclusion in the database? How would you propose self-funded plans opt-in to submit claims data?

Onpoint has been implementing and operating APCDs since 2003 and currently takes in regular submissions from more than 345 health plans on behalf of our clients. Until 2016, following the U.S. Supreme Court's March 2016 ruling in *Gobeille v. Liberty Mutual Insurance Company,* these submissions uniformly included self-funded commercial data. The loss in covered lives has varied by state, depending on the proportion of larger, self-funded employers in the market.

Onpoint's recommendations based on our team's specific experience in overcoming the challenges to the reporting of self-funded data include:

- Helping our clients construct outreach and communication plans to encourage voluntary participation by self-funded plans

- Including self-funded plans in stakeholder meetings – during implementation and operations alike – to foster a sense of inclusion and highlight the benefits of participation
- Working with leading APCD advocacy organizations such as the National Association of Health Data Organizations (NAHDO) and the APCD Council to put in place a national reporting solution for self-funded plans with the U.S. Department of Labor (DOL) – an option noted in the *Gobeille* ruling. This includes serving on the committee that created the APCD-Common Data Layout (APCD-CDL™), an effort focused on reporting standards for payers to reduce administrative burden, as well as providing input and testimony to the DOL's State All Payer Claims Databases Advisory Committee (SAPCDAC).

Our experience also suggests additional approaches that Indiana could take to foster greater participation by its self-funded plans. Among them:

- Collect state and other public employer self-funded data, as mentioned above, which is not governed by ERISA
- Consider adhering to the APCD-CDL™ data collection standard proactively to facilitate compliance and buy-in from voluntary submitters
- Engage the state's business coalitions and health plan advocacy organizations to highlight the value proposition of an APCD, including emphasizing the fact that it is the only comprehensive data source for comparative cost analysis. We have found that self-funded groups are some of the strongest proponents of APCDs given their vested interest in containing costs and maintaining the health of their own employees and the public at large.

These strategies and careful planning can help engage self-funded plans regarding the importance of a comprehensive database in supporting health improvement and cost-containment goals. Employers understand the importance of data completeness when undertaking performance measurement, benchmarking, trend analysis, program evaluation, reporting, and supporting analytic use cases.

Our broad APCD client base has given Onpoint a unique vantage point in both understanding and monitoring how the *Gobeille* ruling has impacted our clients' data collection efforts, including the provision of regular support documentation and data status updates that help our clients understand changes in their APCDs associated with self-funded plans.

6.4 What threshold should be set for health payers to submit data for the database?

Thresholds that set a clear benchmark for required submissions to an APCD are a key and helpful step in clarifying whether health plans must participate. A key lesson learned from the various approaches that our clients have taken is that the threshold's definition should be specific and clear from the start to avoid confusion and decreased participation. Among the considerations:

- **Number of covered lives.** The state should review the volume of lives covered by health plans licensed to do business in Indiana and set a threshold to capture a meaningful percentage of insured Hoosiers. Some APCDs set the threshold very low (e.g., 200 covered lives in Vermont) while others set the threshold higher (e.g., 3,000 covered lives in Rhode Island).

Our recommended minimum adheres to the "80/20" rule, which would set the covered-lives threshold at a volume that will capture a critical mass of at least 80% of insured individuals in the state. A higher percentage would be even better for broad population analysis but pushback from smaller plans may discourage raising the bar to a "90/10" level, for example.

- **Definition of covered lives.** The state also will want to provide clarity regarding which members are included in the count of covered lives. For example, when working with payers that have several plans and submitters (e.g., UnitedHealthcare, UnitedHealthcare Medicare Advantage, etc.), removing the ambiguity regarding whether the threshold applies to each individual plan or instead to the full book of business or parent organization is recommended.
- **Geography.** Another consideration in establishing the APCD's mandatory-participation threshold would be whether the residence of the member or the situs of the plan is used to determine who is required to be submitted. Using members who live in a given state (e.g., Indiana) is typically a straightforward definition for payers to align submissions. By broadening the definition to the situs of the plan, the collection rule would expand to require the reporting of claims for individuals insured by all policies written in Indiana regardless of the insured member's residence location.

6.5 How would you determine the requirements for data collection and the data formats for each file type and platform?

Onpoint has extensive experience advising state-sponsored APCDs regarding the data collection specifications and layouts that will support the intended uses of the data resource. We recommend the following steps when Indiana is determining the requirements for data collection and data formats:

- **Convening stakeholders for a business-needs analysis.** Paramount to planning an effective approach to data collection is understanding the intended use cases for the APCD data. It has been our experience that convening stakeholders to identify and explore their vision for how the APCD could address their information needs is a vital first step. Onpoint's staff have participated in a wide range of stakeholder design sessions prior to drafting initial data collection regulations. Our team is prepared to make recommendations and provide technical assistance regarding the identification of data elements to be collected, addressing privacy concerns regarding PHI and other sensitive elements, preparing responses to stakeholder questions, and participating in public forums with stakeholders to answer questions and solicit feedback.

  To enhance payers' buy-in and support for an APCD, we recommend including payers early in the process. Doing so allows the State to understand any potential limitations in payers' reporting capabilities from the outset. This knowledge is crucial to developing both the list of elements that can be collected and the expected acceptance thresholds for those elements.

  Important topics to explore with state agencies and other stakeholders include which types of less common data will be collected (e.g., dental, clinical, non-claims payments, etc.) and how the data will be used for analytics that potentially impact public policy and healthcare operations such as provider performance measurement, population health analytics, policy analysis, program evaluation, and other areas of interest.

- **Assessment of Medicaid and other public program requirements.** We also recommend collaborating with Indiana's Medicaid program early in the APCD planning process. Medicaid's services and data differ significantly from those of commercial payers and other payers. Anticipating both the distinct data elements that would be crucial to include in the APCD (e.g., dual eligibility, aid categories) as well as any specific analytic needs of the program will be important to consider from the outset.

  Beyond the state Medicaid program, there also may be other state-specific areas of interest that should be considered when evaluating which data elements to collect. Indiana may wish to keep in mind that these data elements must still be part of the member enrollment and claims adjudication process to ensure that they are available for reporting to the APCD. Examples of elements included in the collection efforts of other states are the Public Employees Benefit Board program flag in the state of Washington and an ACO Participation Indicator in the state of Vermont.

- **Developing effective data layouts.** Information identified during the stakeholder engagement process should be used to identify health plans' reporting limitations and the optimal list of fields for Indiana's data collection. As part of the APCD implementation process, two or three years of historical data usually is collected. It is crucial to develop comprehensive file layouts so that essential data is collected at the outset to prevent the need to request later resubmissions for missing data.

  Indiana also may want to consider the benefits of implementing the APCD-CDL™. This emerging national standard includes many of the data elements that are collected in the widely used APCD layouts but uses a different format. Although the APCD-CDL™ is a relatively new layout, national payers participated in its development and are familiar with its structure. Implementing the APCD-CDL™ could position Indiana to potentially capture self-funded ERISA plan data if the federal government eventually adopts the standard as well.

- **Ease in payer implementation.** Payers have been participating in APCD collection efforts for nearly 20 years. Many have extensive experience with the current APCD standard used by many states, which, if implemented by Indiana instead of the APCD-CDL™, may allow for a quicker implementation and less burden to payers.

  It will be important to recognize that there are a finite number of data elements that are routinely and consistently coded and captured by health plans, pharmacy benefit managers, third-party administrators, Medicaid, and Medicare. These data elements must be weighed against the proposed uses of the database, taking into consideration potentially sensitive information associated with patient confidentiality, identified provider activity, contracting relationships, and proprietary financial information.

- **Providing initial and ongoing support.** To help health plans become familiar with state collection regulations, Onpoint always provides a data submission guide (DSG) that includes links to relevant laws and regulations regarding data collection, data specifications, and mappings to applicable standards (e.g., UB-04, HCFA 1500, HIPAA ASC X12, NCPDP guidelines, ADA dental claim form). DSGs also feature detailed information about the data submission process, registration and submission timelines, details regarding data security and encryption, and specifications related to the required data elements (e.g., field definitions, layouts, and acceptance thresholds).

  Clear direction in the data submission guide helps guarantee an accurate understanding of the required data elements, accelerating the onboarding process and enhancing the quality and consistency of data across payers. DSGs should be reviewed with payers and other

stakeholders at least annually and should be updated whenever collection requirements change.

6.6 How would you integrate new file feeds if requested by the State? Explicitly define any related fees within a supplement to the Cost Proposal Template (as a separate attachment; not as part of this Technical Proposal response).

Onpoint regularly onboards new submitters for our APCD clients. This typically happens when a client expands their data collection efforts to include a new claim type (e.g., dental) or when a new high-volume payer enters the market. Regardless of the circumstance, Onpoint's approach remains consistent: We provide all new submitters with webinars, one-on-one meetings, and documentation to facilitate their understanding of the collection requirements and onboarding process.

For details related to fees for onboarding additional file feeds, please see Onpoint's Cost Proposal Supplement: "Onpoint - IN RFP 22-70302 - 2.5.4 - Cost Proposal Supplement (2022-04-04).pdf".

6.7 How would you crosswalk (i.e., mapping fields from one layout to another layout) Medicaid and Medicare data to the APCD format?

Onpoint has been a leader in the mapping and integration of file formats from CMS and state Medicaid programs. Our staff were the first to perform the APCD mappings of Medicare's TAP and Chronic Conditions Data Warehouse (CCW) formats, developing unique expertise that clients continue to leverage today. Onpoint was also among the first in the nation to map CMS's unadjudicated claim formats for the Multi-Payer Advanced Primary Care Practice (MAPCP) initiative, an effort that continued under the subsequent models of Comprehensive Primary Care Classic (CPC) and CPC Plus (CPC+). Onpoint also serves as the designated CMS Custodian for many of our clients.

For state Medicaid programs, we have performed the mapping of state Medicaid data to the APCD layouts. For those Medicaid programs that do the mapping themselves, we have worked closely with the state Medicaid programs and the selected mapping agency/vendor to support their mapping and submission efforts. This includes evaluating the analytic use cases for Medicaid-specific fields, intaking Medicaid-specific reference tables, accounting for Medicaid retroactive eligibility, and exploring other considerations specific to Medicaid programs.

Onpoint has developed an expanded data model and data quality validations to effectively integrate Medicaid- and Medicare-specific elements into an APCD, including the complex logic needed to identify overlapping dual-eligible, Part C, and Part D populations.

We are prepared to provide intake, mapping, and validation services to IDOI to integrate the State's Medicare FFS data. As noted above, Onpoint CDM's status reporting encompasses all payer types and reports on all files immediately upon processing. IDOI will have full access to all data validation reporting for Medicare FFS and Medicaid file submissions, which our staff will review with IDOI to ensure that control totals and other metrics align. Additionally, our proposed

solution will provide encrypted, segregated storage, with role-based access, for the State's Medicare data to comply with any security and storage requirements.

6.8 How would you ensure that data is submitted in an effective manner?

The effectiveness of the claims data submission process, in our experience, can be evaluated in the following ways: (1) usefulness, (2) timeliness, and (3) quality. Onpoint's data integration platform, Onpoint CDM, was developed in collaboration with clients, payers, and data users to create an APCD that exceeds expectations in each of these metrics.

- **Usefulness.** In launching a new APCD program, certain design elements are critical to ensuring that the full value of the APCD is achieved. These design elements include the collection of hashed vs. live identifiers, flexibility in submission specifications, and data enhancements that are designed to support a wide array of use cases (e.g., addressing market and payer differences; creating APCD-specific analytic tools and methods such as risk adjustment, episode grouping, service-line flagging); building summary tables and other aggregations; creating business intelligence reporting solutions to support ease of use by less technical end users; linking claims with other data sources (e.g., clinical, vital statistics, corrections, cancer, disease management programs); integrating additional data sources such as dental claims and workers' compensation; and integrating new data formats such as the APCD-CDL™.
- **Timeliness.** Timely data submission is key to the success of an APCD program. With claims data already lagging clinical data due to the adjudication process, it is important for APCD submissions to avoid additional lag due to submission delays.
- **Quality.** Three key components – standards, benchmarks, and statistics – are prioritized in Onpoint CDM due to their fundamental nature in verifying that submissions meet or exceed quality standards:

    1. **Standards.** Onpoint CDM includes a comprehensive set of data quality processes that scrutinize submitted data for conformance with national standards as well as for the relationships between specific fields (e.g., Admission Source is expected on certain inpatient claims based on the submitted Bill Type code). Upon receipt, Onpoint CDM unpacks each data submission and inspects it for quality and compliance with data requirements and assesses whether the data submission has met the requirements to allow its incorporation into downstream analytics.

        If files are rejected for not meeting required standards, data submitters are required to correct the issue and resubmit. However, for data submitters that are unable to meet the required thresholds, online variance requests can be submitted online. Onpoint CDM's variance workflow is handled collaboratively by Onpoint, clients, and data submitters through the Onpoint CDM portal using an intuitive interface that provides transparency, efficiency, and control to end users, allowing real-time access to the full workflow – from requests to justifications, approvals, and denials. Approved variances, which can be tuned by payer, file type, field, and duration, are documented in Onpoint CDM and are available 24/7 to the submitter and client to ensure understanding and transparency of the available data.

    2. **Benchmarks.** A suite of benchmarks, when combined with our library of thousands of data quality validations, provides unparalleled insight into the quality of incoming submissions. Regularly-employed benchmarks include those based on our cross-client

APCD experience, those that are specific to a client, those that are payer-specific (e.g., specific to the Medicaid and Medicare populations), and those that are externally available for quality assurance purposes. Onpoint CDM includes complex and customizable programming that fine-tunes validations and benchmarks to ensure that collected data will meet end users' needs, vetting submissions for anomalies and errors before they can make their way into the data warehouse.

3. **Statistics.** Statistical algorithms are used to determine valid ranges for key performance measures based on the available benchmarks (e.g., PMPMs), quickly flagging outliers at multiple levels of granularity for further investigation prior to approval.

Onpoint's extensive experience integrating commercial, Medicaid, and Medicare claims with clinical and other data sources across the country offers our clients unmatched expertise in ensuring that their APCD will be designed, developed, and maintained to meet the needs of even their most complex analytic use cases. Secure handling of protected health information (PHI) and other sensitive data are assured through HITRUST-certified procedures and technology safeguards. Our proven validation, standardization, and enhancement processes are backed by our highly trained and experienced staff, who are always available to assist payers through a transparent integration and validation process that ensures the highest quality and on-time delivery.

6.9 How would you capture non-claims-based payment information to have a more complete picture of the cost of health care (e.g., capitated, advanced primary care, bundled, and pay-for-performance payments)? Address the fact that the APCD-CDL™ does not include data elements that capture non-claims payments. If the APCD-CDL™ is adopted, would this data be submitted in a separate file?

Onpoint regularly identifies and collects payments made as part of alternative payment models (APMs), incorporating other non-FFS payments (e.g., capitation, advanced primary care, ACO payments, care management program payments) as aggregate amounts outside of the claim level for use in downstream analyses. Our approach always includes collaboration with key stakeholders to develop clear specifications and procedures for the collection of the non-claims payment data.

For example, to support value-based payment and population-health reporting initiatives in California, the integration of non-claims payment data at the person level is required. Onpoint continues to work collaboratively with the Integrated Healthcare Association (IHA) and payers in the market to capture this information in a supplemental non-claims file that captures capitation broken out by professional, facility, and global capitation; payment for other APMs; and other non-claims payments such as care management fees, case rates, and pharmacy rebates at the member level.

Onpoint staff participate on the NAHDO and APCD Council stakeholder workgroup for the development of a standard non-claims payment data layout. If a standard layout is not available in time for implementation of the Indiana APCD, Onpoint will work with IDOI and your stakeholders to develop a layout that meets the interest and reporting needs of IDOI's end users.

Recognizing that the APCD-CDL™ does not currently capture comprehensive APM information, we would propose a similar approach in Indiana: The collection of a supplemental, annual file to capture non-claims payments.

6.10 How would you capture and ensure nonduplication of data (e.g., pharmacy and third-party administrator claims)?

Onpoint's standard data sets delivered to researchers and analysts include many data enhancements and value-added fields. Included, for example, are a trio of flags to assist in the de-duplication of claims and eligibility records that are reported by more than one payer. These flags include:

6.11 Are there any technical limitations to data submission in your proposed system (e.g., volume, field structure, etc.)? Describe any limitations on file formats for sending and receiving data.

There are no technical limitations to Onpoint's data intake system, Onpoint CDM is a secure, configurable, and highly scalable system that can accommodate large volumes of data as well as state-specific requirements. To ensure the validity and security of incoming data, we do, however, require submitters to adhere to defined parameters such as file layout, field types, maximum field lengths, header/trailer records, and delimiters in order to support the validation of received data. Each of these specifications is defined beforehand in collaboration with the client and documented in the client's data submission guide. Onpoint also provides multiple webinars, supplementary documentation, and one-on-one meetings with submitters to ensure understanding of the specifications.

6.12 What is your proposed method for maintaining documentation of data submissions, including requests for data resubmissions and the submitters' responses to those requests?

The secure Onpoint CDM portal provides submitters, Onpoint, and IDOI staff with role-based access to real-time dashboards and file status reports for all submitted files across all reporting periods on a 24/7 basis. These dashboards include multiple key performance indicators related to the status of submissions, such as the number of submissions in review by file type, the number of variances requiring review (with drill-down), and a summary of overdue submissions. All credentialed users also have access to real-time, detailed reports regarding the status of their submitted files as they are vetted for quality at each of the three key automated validation stop-

gates: (1) proper formatting and file integrity, (2) data completeness and validity, and (3) data quality.

All file submissions, including resubmissions, are processed by Onpoint CDM using the same workflow and validation steps, providing credentialed users with access to a real-time view of their files' workflow, including updates on each file's status, data completeness, and any applied variances. Submitters are able to view detailed data quality feedback within Onpoint CDM and receive automated emails that summarize each file's status at each stage of processing.

Onpoint CDM also is adept at working with file resubmissions to prevent data duplication. Onpoint CDM flags all replacement or "corrected" files as those that should be used going forward and renders previous data for the same time period ineligible for extract or reporting. Whenever we receive replacement files without advance warning or discussion with the submitter, Onpoint CDM flags the file for review by an Operations analyst and the submitter prior to final approval and acceptance. Submitters' responses to resubmission requests are logged in Onpoint CDM and can be retrieved upon request. This step verifies that the file was intended to be sent as a replacement file, further guaranteeing data quality and integrity.

6.13 Describe your experience receiving and integrating historical data files, including output files such as risk scores and custom cohort lists.

Onpoint has collected historical data for each of our APCD clients. Typically, the span of historical data is confined to the three years prior to the collection start date due to retention limitations in payers' systems. Onpoint has no restrictions on receiving historical data that is available and formatted to the client's finalized DSG.

Onpoint fully integrates output files such as those resulting from processing the data though various groupers. Based on the grouper, the resulting output file is linked back to the quarterly data set based on a specific data element. Examples include:

- The results of Clinical Risk Groups (CRGs) results are linked back to the data set using the Onpoint-generated unique member ID for reported members' risk-score assignment
- The results of All-Patient Refined Diagnosis Related Groups (APR-DRGs) are integrated back into the data set using an Onpoint-generated unique inpatient discharge ID that identify a member's unique inpatient stay
- The results of Ambulatory Payment Classifications (APCs) are linked to the hospital outpatient records in the data set using a unique service line ID

Onpoint has in-depth experience integrating custom cohort lists and non-claims data sources with standard APCD claims data, most often through person- or provider-level linkage or ZIP code strategies. These other data sources enrich and expand the reporting possible when moving beyond using claims data alone. For our APCD clients, Onpoint currently is integrating a range of non-claims data sources, including laboratory results and other clinical data, vital records data (e.g., birth certificate, death certificate, cancer data), U.S. Census data, social determinants and survey data (e.g., Behavioral Risk Factor Surveillance System (BRFSS)), Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) patient experience data, socioeconomic data, incarceration data, chronic disease management program data, and more.

When linking custom cohort lists at a provider or member level, Onpoint works with our clients to ensure that the necessary patient and provider identifiers are included to allow for the best match to members and providers in the APCD. This process starts with providing process documentation and working closely with those providing the cohort data to ensure a smooth and efficient process with the highest possible match rate. The cohort files typically are transmitted via SFTP with PGP encryption, processed using Onpoint CDM's validation protocols and then continue through the data pipeline for member and provider clustering.

If linking on other data elements, such as ZIP code, crosswalk reference tables are submitted to Onpoint and integrated so that they can be easily included and delivered with every extract for ongoing analytics.

6.14 Which publicly available data do you propose to use to measure and analyze significant health care quality, safety, or cost issues that cannot be adequately measured with administrative claims data alone, and how would you use that data?

Onpoint has in-depth experience in incorporating other data sources to analyze data that cannot be measured using claims data alone. These external sources are dependent on the specific need and have included:

- U.S. Centers for Disease Control and Prevention (CDC) / National Health Interview Survey
- Behavior Risk Factor Surveillance System (BRFSS)
- Medicare chronic condition charts from the CMS Chronic Conditions Warehouse
- Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) patient experience
- Medicare and Medicaid Services (CMS) Hospital Compare

Data from these external sources have been used in research and analysis, public reporting, and state cost comparison websites.

Onpoint's Cost Proposal includes the intake, mapping, and integration of three (3) external data sets on an annual basis with the understanding that each type of data set (e.g., birth certificate, death certificate, BRFSS) will adhere to a consistent file layout for each subsequent submission to Onpoint.

6.15 How will you review submitted data to ensure consistency, timeliness, completeness, uniqueness, and validity? What is your method/tool for performing data validation and reasonableness checks, including assuring clinical consistency in the data?

All arriving data for our APCD clients are taken through an end-to-end, multi-phase quality assurance (QA) process that includes preliminary integrity checks, initial loading checks, completeness validation, data standardization, data-quality validation, consolidation, and trending analysis, followed by enhancement, additional QA, and extract for data delivery and/or analytic

services. The breadth and depth of Onpoint's quality assurance procedures are comprehensive, time-tested, and a differentiator in the APCD market.

Fundamental to APCD quality assurance is compliance with data collection regulations and specifications – the how, what, and when requirements of APCD file submissions. IDOI's file submission layouts will be configured within Onpoint CDM's secure online portal, with submitted fields mapped to data elements within our comprehensive data warehouse. An array of more than 2,000 data quality validations will be activated and customized for the Indiana APCD based on IDOI's specific collection regulations, a careful review of known differences and limitations of APCD data in the market, and the anticipated use cases that the APCD will need to support. These validations examine incoming data at the file, field, and payer levels and are built to handle the variability and nuances of individual payer's data, including payers in the Indiana market, Medicaid, and Medicare. These validations also include checks for clinical consistency in reporting (e.g., evaluating procedure and diagnosis codes in comparison to a member's gender). All data quality validations are always documented and available to credentialed users of Onpoint CDM's secure, online portal.

6.16 Describe your proposed data quality and validation framework. In your response, be sure to address all requirements listed in Section 5.2 of the Scope of Work.

Onpoint's data validations scrutinize submitted data at a data element level for completeness and conformance with national standards; within a file, looking at the relationship between data elements (e.g., procedure codes reported with proper gender codes); across files (e.g., per member per month (PMPM) metrics, claims supported by eligibility); and over time (e.g., consistency of counts and dollars). Onpoint's data quality validations are reviewed and updated regularly based on our scrutiny of incoming data across all clients, ensuring that lessons learned for one client are leveraged to enhance the data for all clients.

During annual review sessions, Onpoint works with key stakeholders to examine new billing standards and codes, evaluate changes to existing thresholds/acceptance criteria in light of improved data quality, create new validations based on any issues that have surfaced and evolving analytic use cases, and review current and proposed focus areas to target enhancement efforts for maximum support of data users.

Onpoint's standard approach to data quality involves trending analysis and comparisons to quality benchmarks and includes reporting for submitters to review for accuracy. Data trending includes evaluations of the number of members enrolled, claim volumes, total dollars paid and charged, PMPM statistics, percent of claims supported by enrolled members, and other profile statistics. Trending analysis is performed both before and after the data is transformed, allowing QA analysts to investigate data anomalies that are highlighted by the aggregation process. Final quality validation is done post-aggregation across the complete data set and prior to release to end users to ensure that all files included in each data extract are accurate, complete, have referential integrity, and align with expectations and national benchmarks. These post-aggregation analyses and validation checks are part of a formal and rigorous process by which Onpoint flags outliers and finalizes documentation of any data anomalies, their impact on analytics, and any remediation efforts that have been or will be performed.

Onpoint's standard quality assurance protocol also includes regular external validation via an attestation process with data submitters to ensure ongoing data quality. Onpoint-produced

attestation reports provide submitters with the opportunity to validate that Onpoint has received and processed their data accurately. Each data submitter receives a report that summarizes key metrics for their data spanning the most recent 12-month period, including total record counts, total dollars, distinct claim counts, and distinct member counts.

Prior to data delivery, Onpoint's comprehensive QA process combines automated checks with additional hands-on validation by dedicated health data analysts to provide a robust assessment of the quality of the post-load data. These metrics include comparison to benchmarks and employ statistical methods to flag outliers, which are reviewed and investigated by experienced analysts prior to delivery. Their findings are summarized in detailed release notes that accompany each extract. Onpoint has developed a library of standard QA metrics that evaluate the post-load data at the payer, month, service, and product levels, including demographics, member months, aggregated payments, service line counts, and identity resolution.

As a user of APCD data ourselves, Onpoint recognizes that data quality is both paramount and always evolving. We work with our clients both during implementation and throughout the life of the contract to continuously enhance data quality processes, including those addressing specific use cases identified by our clients and their end users – all with the goal of ensuring that the data is trusted, transparent, and useful.

Onpoint's APCD platform and data quality framework use the latest technologies and are built to easily scale, processing millions of records within minutes. We continue to evaluate emerging technologies, keep abreast of industry billing and coding updates, and regularly assess new methods and layouts for data exchange. Onpoint CDM is highly configurable, which allows us to meet the needs of our APCD clients and readily adapt to the changing needs and requirements in the healthcare industry (e.g., FHIR).

For Onpoint's systematic responses to the State's security and privacy requirements, please see our Technical Proposal's Section 2.4.5 ("Security & Privacy").

6.17 How will you develop submitter-specific thresholds?

All submitters credentialed to submit data to the APCD will be provided with access to Onpoint CDM's secure online portal and its intuitive, self-service interface that streamlines the variance request and review process. Files that fail a data quality threshold are prevented from passing through Onpoint CDM until further review is completed by our Operations analysts. For deficiencies that cannot be resolved – for example, if a submitter's system simply does not capture or retain data at the required volume – submitters are able to request a variance using Onpoint CDM's online variance module. The variance workflow is designed to be transparent and efficient. Clients and submitters have real-time access to their requests, justifications, approvals, and denials. Approved variances – which can be tuned by submitter, file type, field, and duration – are always documented and available in Onpoint CDM's online interface.

6.18 How will you provide submission feedback (e.g., a quality audit/error report/dashboard) to the supplier for each submission? What information would be included (submission status; the number of records processed; the number of records requiring correction; errors observed in the files; scores for timeliness, completeness, uniqueness, and validity; etc.)?

Onpoint's APCD data integration solution, Onpoint CDM, enforces a comprehensive, multi-stage quality assurance (QA) process for all file submissions. Upon receipt, Onpoint CDM unpacks each data submission and inspects it for quality and compliance with the client's requirements. Onpoint CDM includes complex and customizable programming that fine-tunes data quality validations and thresholds to ensure that collected data will meet end users' needs, vetting submissions for anomalies and addressing any errors before they can make their way into the data warehouse.

All validation results are automatically reported to submitters and will be available to IDOI and data submitters in the secure Onpoint CDM portal. Data submitters also receive automated emails notifying them of the status of their file. Emails regarding file submission failures are sent to the submitter at any processing step when a file fails to meet required standards and include the details for the failure, identifying each specific failure, the row number(s) of the failing records, details to support investigation and correction, and a required resubmission deadline.

Within Onpoint CDM, IDOI and submitters alike can see the resulting scores, rates, and calculated percentages of each data quality validation applied to their submission. Examples include two key stages of Onpoint's validation and QA processes:

- **Completeness thresholds.** One of Onpoint CDM's initial and fundamental QA processes is comprised of a series of completeness thresholds that focus on the population and validity of individual data elements. This battery of completeness and validity checks [redacted] If errors are detected, this process fails the submission, identifies the failed records and the percentage of complete and valid records, and sends a notification that cites the reason(s) for failure along with instructions regarding remediation.
- **Validation checks.** Building on the completeness thresholds, data next undergo a battery of quality validations that assess the interrelationships of individual data elements and evaluate rates against parameter-driven thresholds to spot anomalies and errors using Onpoint's library of more than 2,000 data quality validations (DQVs). These DQVs have been developed over the course of implementing more than 10 APCD systems and continue to evolve as the industry adds new data sources and data elements and expands the range of analytic use cases. The results of these data quality validations are reported as scores, rates, and percentages depending on the validation calculation.

These initial validation processes verify that data is ready for processing and are typically completed within hours following file receipt. While Onpoint CDM provides 24/7 self-service reporting through its secure portal, the system also sends automated email notifications directly to data submitters as their files move through each step of the validation process to keep files on track and ensure transparency.

6.19 How will you receive and process corrected and resubmitted files? How will you document all corrections and modifications to submitted data?

With our rigorous data quality checks in place, it is routine for resubmissions to be required and received, especially during the implementation phase. Onpoint CDM accepts resubmission files at any time – each of which undergoes the same validation process as regular production files, with the system automatically logging and tracking the new data for the specified reporting period. Onpoint CDM flags a successfully validated resubmission or replacement file and its records as those that should be used going forward, toggling the previous file and records to a retired status that excludes them from downstream processing and analytics.

6.20 Describe your methodology for linking data files provided without a unique ID (e.g., SSN).

Onpoint's master patient index (MPI) is a proven solution supporting multi-year analyses by our clients across the country. Our MPI relies on member/enrollee identity-resolution (or "clustering") algorithms that examine available data elements (e.g., Social Security number, name, date of birth, gender, contract number, submitter-supplied member identifiers, etc.) in combination with one another, using multiple clustering levels that are executed in a hierarchical fashion, with the most rigorous matching requirements occurring first.

Clustering levels may require exact matches on some elements (e.g., date of birth) but allow fuzzy matches on others (e.g., first name). Clustering levels are adjusted for each client and data submitter and optimized based on the range and quality of data elements being supplied (e.g., SSN not reported).

This same process is used when linking the APCD to other data sources. Onpoint has in-depth experience integrating other data sources with the APCD claims data through person-level linkage. These other data sources enrich and expand the reporting possible when moving beyond using claims data alone. For our APCD clients, Onpoint currently is integrating a range of non-claims data sources, including laboratory results and other clinical data, vital records, U.S. Census, social determinants and survey data (e.g., Behavioral Risk Factor Surveillance System (BRFSS), Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) patient experience), socioeconomic data, incarceration, chronic disease management program, and more. These other data sources have varying levels of completeness for member-identifying data that can be used to link to the APCD. Key member identifiers (e.g., SSNs) are not always available in the APCD or in data being linked to the APCD.

Onpoint works with our clients to ensure that the necessary member identifiers are included to allow for the best match to members in the APCD. This process starts with providing process documentation and working closely with those providing the non-claims data to ensure a smooth and efficient process with the highest possible match rate. The non-claims files typically are transmitted via SFTP with PGP encryption, processed using Onpoint CDM's validation protocols, and then continue through the data pipeline for member and clustering and assignment of the unique member ID.

Documentation on this linkage file is provided and will include a data quality report with metrics such as number of records received, number of matched records, etc.

6.21 Describe your methodology for handling activity data on Submitter files that cannot be linked to an existing census record.

As part of the APCD implementation, Onpoint will work with IDOI and your stakeholders to evaluate the APCD reporting and analytic needs to ensure that the correct data quality validations and thresholds are activated. This includes key data elements needed for linkage to other data sources such as the reporting of member ZIP codes to enable linkage to reference data provided by the U.S. Census Bureau.

6.22 Describe internal controls implemented to prevent and detect data integrity issues. For each control, designate if it is a manual or automated process and how errors are resolved.

As part of the data validation and integrity processes described above in our response to Question 6.16, automated controls have been implemented to ensure multiple data integrity steps. These include:

- **Data transformation rules.** Onpoint CDM's integration systems leverage a robust, cloud-based infrastructure to perform a series of complex yet flexible extract/transform/load (ETL) processes that standardize, cleanse, and consolidate arriving data. Onpoint CDM is architected to flexibly handle submissions using any format – traditional APCD, APCD-CDL™, CMS standard layouts, state- or payer-specific, etc. – with all submitted fields mapped to data elements within our comprehensive data warehouse. The transformation module includes more than 1,000 standard rules that can be configured for a client's APCD to standardize, cleanse, and integrate data across all payers. These rules are customizable by layout and data element to allow for optimized processing while providing deep transparency.
- **Maintenance of original values.** Onpoint maintains the as-submitted value for all transformed data elements.
- **Referential integrity.** Data sets are evaluated for internal consistency (e.g., all code values that appear in core tables also appear in associated reference tables).
- **Reference tables.** Onpoint CDM includes more than 200 reference tables that cover a large range of code sets to support look-ups across the delivered data sets. Licensed reference tables include:
  - [redacted]

[redacted]

6.23 Explain your proposed Extract Transform & Load process. Include detailed description of the technology platform and software used, flow charts/diagrams, and proposed processing timeline.

Onpoint CDM's extract/transform/load (ETL) process, which begins with our data integration platform and supports our Analytic Environment's data dissemination and reporting solutions is active 24/7.

Onpoint CDM's integration systems leverage a robust, cloud-based infrastructure that employs a series of complex ETL algorithms that standardize, cleanse, and consolidate the received data. Onpoint CDM has been in production for nearly 20 years and leverages distributed computing patterns in the Amazon Web Services (AWS) cloud to provide a secure, highly performant, scalable, and reliable solution. [redacted] Visual diagrams of Onpoint's technology stack and ETL workflow are provided in **Figure 6.23.A** and **Figure 6.23.B**, below.

Figure 6.23.A. Onpoint's Current Technology Stack

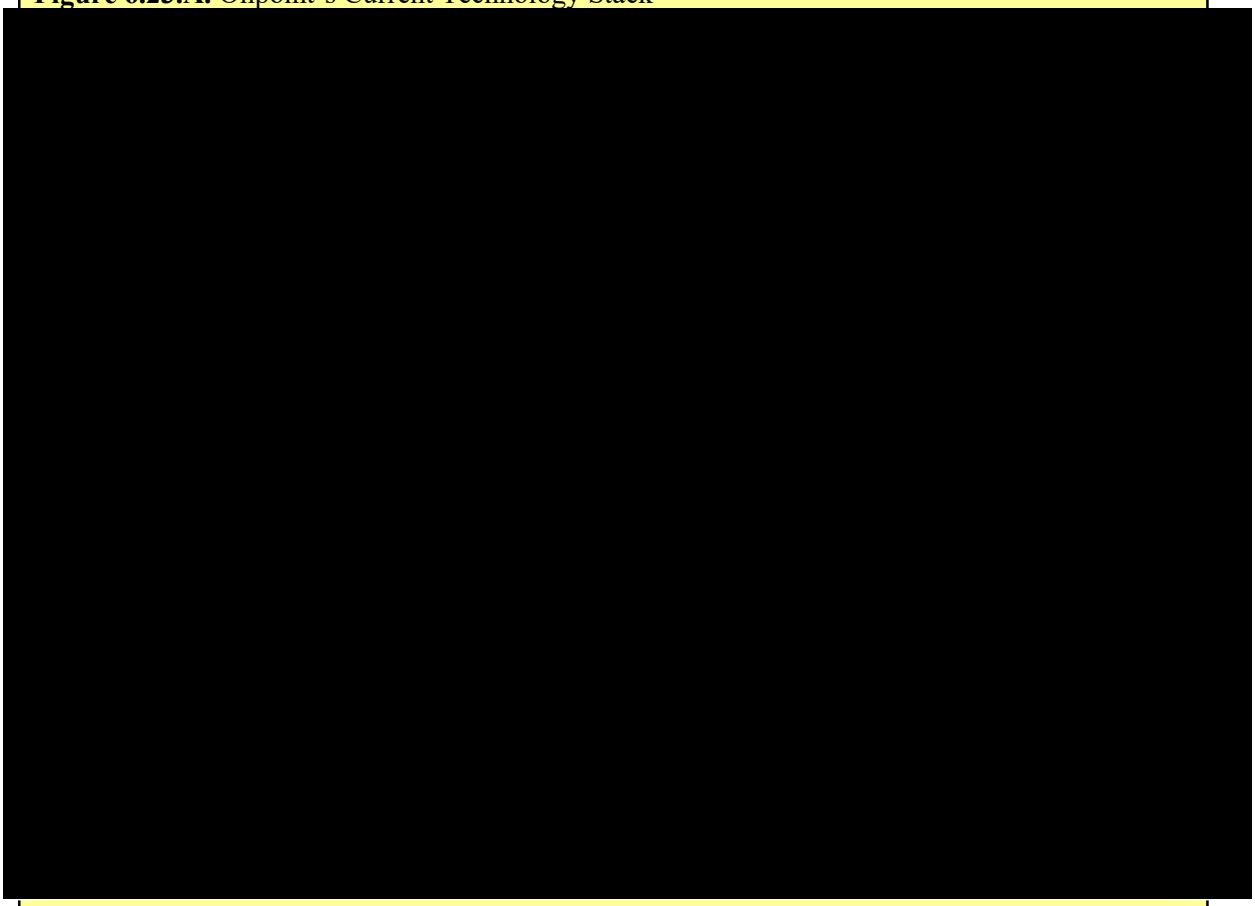


Figure 6.23.B. Onpoint's ETL Workflow

6.24 Describe your turnaround time regarding the following activities:

Receipt of data from Submitter

Data validation

Clean data uploaded to data warehouse

Total turnaround time (when data is ready for the State to view and run reports)

Any other steps in your process from data submission to acceptance or rejection

Each of the turnaround times requested above depends on the size of the submitted file. That said, Onpoint's initial validation processes are typically completed within minutes following file receipt. Data that is deemed "clean" (i.e., approved for data quality) is uploaded to Onpoint's data warehouse on a regular, rolling basis that typically completes within hours of file acceptance. The status of all received data files is available to the State 24/7 via Onpoint CDM's secure online reporting portal.

Delivery of the comprehensive analytic data set will be delivered within 30 days of all files passing validations and or approval of the State to move forward without submissions from all payers.

6.25 What is your process for determining "clean" data before it is loaded into the database?

As noted above, Onpoint's claims data integration solution, Onpoint CDM, is designed to identify and address data quality issues through a multi-stage data validation process spanning data intake through consolidation, enhancement, and extraction. At every stage, skilled data operations and analytics staff monitor compliance with data quality standards and address identified gaps or limitations with data submitters and clients.

An array of more than 2,000 data quality validations will be activated and customized for the Indiana APCD based on IDOI's specific collection regulations, a careful review of known differences and limitations of APCD data in the market, and the anticipated use cases that the APCD must support. These validations examine incoming data at the file, field, and payer levels and are built to handle the variability and nuances of individual payer's data, including Medicaid and Medicare.

Please see Onpoint's response to Question 2.16, above, for additional details regarding our approach to data cleansing and validation.

6.26 How do you reconcile the data in the database to the State's records from its Submitters (i.e., claims paid, enrollment counts)?

Onpoint's standard quality assurance protocol includes regular, external validation via an attestation process with data submitters to ensure ongoing data quality and accuracy. These attestation reports provide submitters with the opportunity to validate that Onpoint has received and processed their data accurately. Each data submitter receives a report that summarizes key metrics for their data spanning the most recent 12-month period, including total record counts, total dollars, distinct claim counts, and distinct member counts.

6.27 Describe how your system links data from multiple sources to one integrated record per individual in the data warehouse?

As noted above in our response to Question 6.20, Onpoint's master patient index (MPI) is a proven solution supporting multi-year analyses by our clients across the country. Our MPI relies on member/enrollee identity-resolution (or "clustering") algorithms that examine available data elements (e.g., Social Security number, name, date of birth, gender, contract number, submitter-supplied member identifiers, etc.) in combination with one another, using multiple clustering levels that are executed in a hierarchical fashion, with the most rigorous matching requirements occurring first. Clustering levels may require exact matches on some elements (e.g., date of birth) but allow fuzzy matches on others (e.g., first name). Clustering levels are adjusted for each client and data submitter and are optimized based on the range and quality of data elements being supplied.

Member data received from data submitters that has satisfied the required completeness and quality checks moves into the member-clustering pipeline and through a series of mapping algorithms that tie each record to Onpoint's MPI, which contains subscribers and members/patients. Members' detail-level records from all submitted files (e.g., eligibility, medical claims) are clustered together using Member IDs that identify the same individual, ultimately unifying under the same Unique Member ID, providing a mapping from the supplied data to the unique members. The same process applies to linking external data sources to the APCD using member identifiers. This assigned Unique Member IDs allow end users to be able to track individuals over time and across data submitters as both members and subscribers. (A parallel process is performed for providers to create Unique Provider IDs.)

6.28 Describe the database update process. How do you communicate to clients when new data is uploaded and ready to be accessed?

Data extracts and online reporting are updated on a pre-scheduled basis for each of our clients – most frequently on a quarterly basis. Onpoint's project managers communicate planned updates and data availability well ahead of time, providing updates throughout the process, including notification when the data refresh is available for the client's use.

For those clients electing to use Onpoint's SharePoint based Collaboration Zone, credentialed end users receive announcements regarding upcoming and delivered data/reporting refreshes as well as access to documentation such as data dictionaries, supplemental documentation, FAQs, and training materials. The Collaboration Zone also can be used by Analytic Environment users to foster knowledge-sharing, transparency, and collaboration.

6.29 Describe the data warehouse solution you are proposing to the State.

Onpoint CDM offers valuable, role-based reporting and self-service tools for submitters and clients to ensure understanding and transparency throughout the file submission and processing pipeline. Using Onpoint CDM's secure data submission and reporting portal, IDOI staff and data submitters alike will be able to follow each submission as it moves through the processing queue, accessing comprehensive real-time reporting about submission quality as well as comprehensive documentation of our transparent business rules. Onpoint CDM securely processes and validates a wide range of file types for all payer and plan types and easily handles proprietary layouts and

plan-specific elements. Onpoint additionally provides mapping and submission support services to Medicaid and Medicare plans and to any commercial plans requiring technical support in complying with our clients' submission specifications.

Onpoint CDM's integration systems leverage a robust cloud-based infrastructure that employs a series of complex data transformation algorithms to standardize, cleanse, and consolidate submitted data. Onpoint stores our clients' data in an enterprise system built for large data volumes and can readily accommodate IDOI's anticipated data volumes.

All arriving data are taken through an end-to-end, multi-phase quality assurance (QA) process that includes preliminary integrity checks, completeness validation, data standardization, data-quality validation, consolidation, and trending analysis, followed by enhancement, additional QA, and extract for data delivery. The breadth and depth of Onpoint's quality assurance procedures are comprehensive, time-tested, and a differentiator in the APCD market. Additionally, all files approved for data quality are retained in both their fully processed format and as they were originally submitted to preserve an historical record of the "raw" submissions in case of future needs.

Onpoint CDM offers a rigorous suite of iterative, multi-step QA processes, including a library of thousands of data quality validations (DQVs) that assess quality and completeness at the payer, file, and element levels. Our DQVs are reviewed and updated regularly based on scrutiny of incoming data, client input, and evolving analytic uses.

All data moves to a consolidated data warehouse based on final claims, which serves as the launching pad for all analytics. The Onpoint CDM platform is flexible and applies necessary adjustments aligned with submitters' systems. This is accomplished by engaging with each submitter to understand their adjudication process and by including more than 25 predefined consolidation algorithms that address the nuances and challenges associated with medical, pharmacy, and dental claims consolidation. These algorithms, developed and refined over nearly 20 years to reflect the differences in payer adjudication processes, are audited annually to ensure the accuracy and consistency of the final claims included in the consolidated warehouse. Onpoint's data quality validations also play a role in vetting data for accurate consolidation and are informed by our staff's experience working with myriad adjudication systems and consolidation algorithms. Onpoint also enhances the data by creating summarized tables, chronic condition flags, and other fields that make the data easier to use for analytics.

Final analytic data sets are produced in text format or in Parquet, a compressed columnar format, depending on the delivery method. Extract recipients are configured within Onpoint CDM, defining the access level of each recipient (e.g., recipients of encrypted SFTP transfers or users within the Analytic Environment). Once the extract has been reviewed by Onpoint's analytics staff, an automated process delivers the data to external recipients via SFTP, if applicable, and to Analytic Environment users through [redacted] Users within the Analytic Environment can then query the data through variety of tools such as DataGrip, as well as visualize the data through the use of Tableau and Onpoint's BI solution.

6.30 Which components of your solution are in-house and which components are outsourced?

Onpoint's client- and submitter-facing applications, including Onpoint CDM and our Analytic Environment, are solutions developed in-house and hosted in the cloud on infrastructure operated

by Amazon Web Services (AWS), with all system resources located inside of the continental United States in data centers that are SOC-2 certified.

Onpoint leverages AWS services and third-party applications in the design of this system. The Analytic Environment provides users with access to a variety of industry-leading analytical and querying tools, such as RStudio (for R), Anaconda (for Python), DataGrip (for SQL), and Tableau, while Onpoint CDM can be configured to leverage third-party grouper technology for risk scoring and episode grouping. Onpoint has been vetted and reviewed for privacy and security compliance by all of our state government clients and has successfully achieved HITRUST certification, the gold standard in health data security.

6.31 Describe any hardware and software that will be required by the State to maintain the proposed data warehouse solution.

Onpoint's solution does not require the State to install, purchase, or maintain any special hardware or software. Users can access the secure Onpoint CDM portal through any standard web browser. Users can log in to the Analytic Environment, which is a virtual Windows desktop, through the free AWS WorkSpaces client, which is available on Android, iOS, Fire, Mac, Windows, Chromebook, and Linux devices.

6.32 How would you make data from the database available, including what sufficient fee would need to be assessed, to researchers, companies, and other interested parties in analyzing the data?

Approach to Data Accessibility

Onpoint has been building and delivering database products to clients for more than 40 years. In that time, our approach to data access and dissemination has evolved to keep pace with emerging technology and the most rigorous data security standards.

Today, nearly all data and reporting services are made available to our clients and their approved users in one of two secure ways: (1) SFTP delivery with PGP encryption and SSH key exchange for downloading data sets to their own servers, and (2) Onpoint's cloud-based Analytic Environment solution hosted by Amazon Web Services (AWS).

Onpoint's recommended approach for making data available to end users is through a secure, cloud-based, enclave-type environment. Onpoint's Analytic Environment solution is cloud-based and hosted by AWS, which offers industry-leading security and scalability for an active APCD user community. The Analytic Environment features a highly performant data model that optimizes query-turnaround and data-visualization response times. Delivered through a secure environment with strictly enforced role-based access, the Analytic Environment provides users with access to only their authorized data sets and offers flexibility in the tools offered to our clients, their data users, and approved analysts.

We recognize that different clients and data users have different needs and preferences in working with data so we provide flexibility in how the data can be accessed. Accordingly, Onpoint provides a diverse menu of tools available in the Analytic Environment. Our standard offering features the Microsoft Office suite, RStudio, DataGrip (for SQL querying), and Tableau – the tools requested most often by our clients and their analysts. In addition, we offer a Tableau-based

BI reporting solution that is tailored to business users and features a suite of standard reports that provides rich insights into the APCD data across a diverse set of relevant domains. Supplementary tools such as SAS also can be made available.

Fee Structure to Support Access to the APCD

For data access beyond the 10 Analytic Environment seats already included in our Cost Proposal for IDOI staff, Onpoint's recommended approach to fees would be a subscription service to the Analytic Environment. The service would include access to the secure Analytic Environment, maintenance and updates, and data products refreshed per Indiana's preferred schedule. Onpoint can provide IDOI with our tiered pricing structure for additional Analytic Environment seats if wanted.

Based on experience across our APCD client base, fee schedules for access to data sets produced by APCD programs vary depending on the amount of external revenue needed to support the APCD, the complexity of the data sets, and the frequency of refreshes. In addition to core data products with established fee schedules, requests for custom data products arrive regularly and require ad hoc pricing and development.

We have found that ongoing, paid subscriptions to data products often consist of the following stakeholders:

- **Government agencies.** Fellow state agencies often are active users of the APCD.
- **Research organizations.** National and regional research organizations often will seek approval for use of the APCD to support various research initiatives focused on health policy.
- **Health systems or other provider organizations.** When health systems and provider organizations seek APCD data, access often is potentially tiered based on the size of the organization and/or the number of users.
- **Commercial vendors.** Software vendors looking to mine the APCD for a comparative database or to apply their analytic tools to the database are a common use case among data requestors.

Our experience is that fees generated from data product sales, while helpful for covering direct costs of producing these products, most often do not provide significant support for overall program costs. Most states rely on general funding, Medicaid match, payer/provider assessments, and grant dollars as primary funding sources. The final fee schedule for Indiana's APCD data products would best be considered by the APCD program leadership with input from key stakeholders.

6.33 Are you able to accept and process fees received from submitters and data purchasers?

We have experience with APCDs that handle this in different ways. In some state APCDs, the State chooses to collect fees directly from data purchasers and charges them more than Onpoint is paid to produce and deliver the data product. This surplus is used to support the overall APCD program. In other state APCDs, the state does not want to be involved in these transactions, and Onpoint invoices the data purchasers directly for the data products that the state has approved for

delivery. Onpoint can execute either of these models and will work with the State to develop a workflow that meets the IDOI's needs.

6.34 How many years of data are typically maintained on the production database?

The Analytic Environment will provide access to the APCD's quarterly data refreshes, which can include all years of data collected throughout the life of the contract. Data will go through Onpoint's suite of analytic enhancements during each extract cycle, allowing historical data to remain in sync with recent data submissions.

6.35 How many years of data can be maintained in archive? What is the process to identify data in need of archiving? Would the State have an ability to jointly determine that need?

Onpoint's proposed solution for IDOI's APCD includes the allocation of storage to accommodate the entirety of the State's data collected during the life of the contract within the Analytic Environment. Each quarter, Onpoint will deliver a data extract to the Analytic Environment that incorporates the most recent data provided by data suppliers with all years of historical data. Prior extracts will be removed from the production database and archived upon release of the new data. Archived data extracts can be restored whenever needed.

Onpoint will retain archived copies of all files submitted to IDOI's APCD that have been accepted for data quality as well as all data sets delivered to the State throughout the course of the contract. All archived data submissions can be retrieved and restored for the IDOI's use upon request. Onpoint CDM provides many configuration options for data extracts, including the time-period of the data to be delivered, allowing for easy adjustment from extract to extract, as Indiana's needs change. The State is welcome to collaborate with Onpoint to jointly determine when data can be archived.

6.36 What is the process for retrieving or accessing data in the archive? What is the average turnaround time for acquiring archived data?

Archived data is stored in Apache Parquet files, an open-source, highly compressed column-oriented file type, within AWS's Simple Storage Service. Upon request from Indiana, this archived data can be restored to the production database and made available for analytic querying within five (5) business days of receiving a written request via email to Onpoint's Project Manager. There may be a small fee associated with restoring an archived extract to reflect the infrastructure and labor expense to do this activity outside of the normal data workflow.

6.37 What services would you recommend be provided to external data users, such as researchers, if any?

Once in production and generating data products – and assuming that Indiana's APCD release regulations will permit broad accessibility – Onpoint recommends the following services be offered to external end users:

- Recurring, annual subscriptions to data services such as dynamic business intelligence (BI) reporting and the Analytic Environment that provide cloud-based, role-based access to approved data sets accompanied by a suite of querying and visualization tools (e.g., RStudio, DataGrip, Tableau, etc.)
- Training and documentation on the use of the data as well as significant changes to the data over time
- Providing full data sets, more-targeted data sets optimized for researchers, customized data sets, Safe Harbor data sets for the public and health plans, and more (e.g., public use files)
- Accepting supplemental data sources to the APCD for various research and analytic initiatives (e.g., public health registries (e.g., birth certificate, death certificate, cancer registry), clinical registries (e.g., lab values, blood pressure), social service programs, and corrections/incarceration registries

6.38 Describe your user license structure. Are there varying levels of access, such as read only, read / write, and or role-based profiles (i.e., different accessible data by user type)? If you provide role-based security access, what types of security access levels are offered?

Onpoint has developed, implemented, and operated role-based data access and reporting systems for nearly 20 years. We maintain rigorous access control and oversight of the data in our systems. Both of the client-facing solutions that are foundational to our secure, end-to-end APCD platform – Onpoint CDM for data intake and integration and the Analytic Environment for data access and analytics – employ role-based data access protocols for all credentialed users.

Access to Onpoint CDM. Onpoint requires all data submitters to register, be approved, and receive role-based credentials via secure email prior to submission or gaining access to Onpoint CDM's secure online portal. Onpoint CDM provides all credentialed users with access to real-time reporting regarding the stage and status of submitted files. This role-based functionality allows data submitters to view the progress of all of their (and only their) submitted files across all reporting periods. Onpoint and client staff are assigned a different role and thus have a broader view: The ability to look across all data submitters and all reporting periods at any time to fully monitor the status of all submissions to the APCD. Onpoint works closely with our clients and their data submitters throughout the project to regularly identify and confirm their users and assign role-based permissions with the appropriate level of access.

Access to the Analytic Environment. The Analytic Environment also employs role-based access control for our clients' analysts and data users. Through the use of Amazon Web Services (AWS) security tools, including AWS Identity and Access Management (IAM), AWS Microsoft Active Directory, and AWS Security Groups, roles and groups are created to enforce consistent role-based access and consistent network traffic control across services. Users are assigned to groups (e.g., data analysts, data users) based on client requirements. Groups are assigned to roles, and each role is assigned to a set of permissions (e.g., read-only access to the data extracts, read-write access [redacted] for data analysts to perform extract/transform/load (ETL) functions, read-only access for data users who can only view reports and dashboards, etc.). Additionally, the Analytic Environment provides users with access to only their authorized data

sets (e.g., comprehensive extracts, custom data sets, limited/researcher data sets), which can be adjusted at any time based on client requests and requirements.

6.39 What type of documentation, instruction material, and live support can you provide to IDOI and other State Agency users?

As the data aggregator and analytics vendor for many APCD programs, Onpoint well understands the importance of transparency and is committed to delivering it. To this end, we provide our clients and their end users with the supporting documentation necessary to understand, validate, and efficiently use the delivered data sets and their analytic enhancements. This documentation includes:

- **Release notes.** With each extract delivery, Onpoint provides a set of comprehensive release notes (sometimes called a "transmittal report") that details any changes in the data structure since the preceding extract, identifies which submitters' data is included, offers information about enhancements or data findings relevant to analysts, and features descriptive information about the specific extract, including the extract's reporting period, exclusions, and versioning. Additional features include triangulation reporting and data profiling updates.
- **Data dictionaries.** Onpoint's data dictionaries provide detailed information regarding each extract's tables, fields, formatting, source-to-target mappings, inter-table linkage, and useful tips for data users regarding specific fields (see **Figure 6.39.A**). Additional tabs in our data dictionaries provide users with code-level detail regarding data enhancements and walkthroughs of common use cases, identifying the tables that should be used and linked to explore such cases most efficiently. Onpoint's dictionaries are provided in Microsoft Excel format for ease of use, allowing end users to quickly find and filter data within tables to focus on desired information.

Figure 6.39.A. Onpoint's Data Dictionary – Emergency Room Flag (Excerpt)

Field Name	Common Name	Description	Origin	Notes	Additional Information
emergency_room_flag	Emergency Room Flag	This field contains a code that is used to identify specific emergency room (ER) revenue or procedure codes within a claim. Valid values are: N = No Y = Yes	This is a value-added field created by Onpoint.	This field is set only on the specific claim line where an ER-related revenue code, procedure code, or place of service code was found. To find true outpatient ER visits, select claim lines where this field is set to 'Y'.	Records are flagged as 'Y' where: Revenue code = 0450–0459, 0981 Place of service code = 23 (ER) Procedure code = 99281–99289

- **Instruction materials.** We also provide easy-to-understand explanations of how to use other included enhancements such as how to use our Member Month table to resolve confusion regarding a member's coordination of benefits when a member had more than one eligibility record reported by various payers in a given month.
- **Entity relationship diagrams (ERDs).** The relationships between tables within the data warehouse are integral to effective use and downstream analytics. ERDs supplied to IDOI and their end users will detail the relationships between fields, primary keys, reference

information, and the composition of every key table delivered in the IDOI's data sets. (**Figure 6.39.B**).

Figure 6.39.B. Onpoint's Standard Entity Relationship Diagram (Excerpt)

- **Training documentation.** During the onboarding process, users of the Analytic Environment also receive a series of trainings to orient them and ensure that they have the technical support to connect all available tools to their data sets. Users receive guided demonstrations of each tool available within the Analytic Environment and have access to all supporting documentation.

As part of the data delivery process, Onpoint's client-support and IT teams remain available to provide regular updates, check-ins, and technical support to ensure on-time and satisfactory delivery. Users will be able to easily request support from Onpoint's technical support staff about all aspects of the Analytic Environment and will be able to track any requests or issues through Onpoint's Jira-based help-desk ticketing system. In addition, Onpoint provides regularly scheduled user group meetings to inform end users of upcoming enhancements, provide focused trainings on data use cases, offer billing and claims data updates, and explore other topics of interest.

6.40 If the data warehouse can be accessed via a web browser outside of the State's network, explain how the secure communication between web servers and browsers will be managed.

Onpoint's proposed solution includes hosting of the data warehouse within Onpoint's Analytic Environment, which is a secure network dedicated to the State and hosted by Onpoint. The Analytic Environment is not accessible via web browser, and instead uses Amazon's native Amazon Workspace desktop client to create a secure connection between a user's machine and the environment.

Users must log in using multi-factor authentication to gain access to a remote virtual Windows desktop environment. The workspace leverages secure PC-over-IP display protocols, granting visibility into the data without requiring the data to leave Onpoint's environment.

As noted above, the free AWS WorkSpaces client is available on Android, iOS, Fire, Mac, Windows, Chromebook, and Linux devices.

6.41 Describe a user's accessibility and tools to data, including front end access and back-end database access. Is the system accessed by user desktop, browser-based, or other?

Designated IDOI staff will have access to the Onpoint CDM portal (front end) for real-time reporting regarding the stage and status of submitted files.

Once all processing, quarterly extracts, and analytic value-adds have been completed, State-designated users will have access to the back-end database in the Analytic Environment. Once successfully logged into the Analytic Environment using multi-factor authentication, users are presented with a familiar Windows 10 virtual desktop with shortcuts to their approved tools. Users also have access to a personal drive space for saving work products within the Analytic Environment as well as shared drive space to exchange code, reports, and tables with other credentialed Analytic Environment users.

The core back-end database will [redacted] and users can query and access the database with their choice of tool. We recognize that different clients and data users have different needs, skill levels, and preferences in working with data so we provide flexibility in how the data can be accessed. Tools available in our proposed solution for IDOI include the Microsoft Office suite, RStudio, DataGrip (a SQL query tool), Anaconda (Python), and Tableau – along with access to Onpoint's BI dashboards and underlying data marts.

6.42 Can you provide any offline usage capabilities? If so, describe.

While direct access to the Analytic Environment requires an internet connection, data can be exported for offline use as needed. The State may identify a group of users to be permissioned to export files through Amazon Simple Storage Service (S3) buckets. Onpoint does not recommend allowing users to export PHI or other sensitive data. However, summarized data and reports may be downloaded so that users can work locally or incorporate findings into other analyses. Onpoint will work closely with the State to create an export procedure that meets the IDOI's needs.

6.43 Confirm the ability to drill down to a level that will show individually identifiable data including pulling raw claims data. Can you enact role-based restrictions on the ability to drill down to a level that will only show one health plan member? Can you configure the reporting capability to set a minimum reporting sample size?

Onpoint CDM provides the needed flexibility and configurability to provide data access based on the specific data use agreement and use case. For each case, the level of detail in the data is tuned to provide a rich data set without exposing unnecessary, sensitive detail. Onpoint will enact role-based restrictions to provide secure access to individually identifiable data, reports, queries, and extracts hosted in the Analytic Environment to provide the ability to drill down to the claim-line detail. The role-based access can be enacted to show a single health plan member, or a complete data set, as governed by the data use agreement for the specific IDOI-authorized user. In addition, Onpoint routinely configures reporting capabilities to set a minimum reporting sample size and will collaborate with IDOI during the implementation phase to ensure that blinding complies with applicable rules and best practices.

6.44 Describe your protocols for secure file sharing and describe the secure file sharing services you use/support.

Onpoint follows strict administrative and physical safeguards to ensure secure data submission and storage. Protecting data in transit includes (1) the transfer of files using approved secure methods, either SFTP (Secure File Transfer Protocol) or Hypertext Transfer Protocol Secure (HTTPS), to ensure an encrypted transmission tunnel, and (2) file-level encryption prior to transmission using the OpenPGP standard and signed by a sender registered with Onpoint.

Analytic Environment users can have the ability (at the direction of the State) to import and export data using AWS's S3 buckets, which are mapped inside of the Analytic Environment for this purpose and are accessible from outside of the Environment. All query activity and S3 activity are logged for security purposes. Since the ability to browse the web as well as import and export data can present security threats, Onpoint locks down this functionality very tightly by default; these strict permissions, however, can be relaxed based on client requirements.

6.45 How will you make data available for direct ad hoc query and extract by the IDOI? Describe your query builder and fields from the raw data that would be accessible to the State. Provide an example of the user interface.

All data available to IDOI in the Analytic Environment will be fully integrated, enhanced, and query ready. Onpoint's data enhancements are consistently applied, allowing for ease in querying and comparing data across the entire data set, for specific time periods, and for specific payers and product types. Table and column names are intuitive and consistently used across all data products. Similarly, data transformation rules are consistently applied (unless otherwise specified) so that codes are standardized with consistent values, content, and formats across all data sets to make querying across data elements and data types reliable and efficient.

Data is stored [redacted] to which all Analytic Environment users will have access to query the data with varying levels of permissions. The Analytic Environment is extremely flexible, and users may query the data using a variety of tools. Onpoint's proposed tool set includes DataGrip (a SQL query editor), Tableau, and RStudio.

DataGrip allows users to [redacted] and assists users in the creation of SQL code through standard query editor features, such as smart code completion, schema exploration, and color coding of code to enhance readability.

Similarly, users may directly query the database from Tableau and RStudio. Tableau allows users to create new data sources that can be incorporated into new and existing data visualizations. RStudio allows users to easily and efficiently perform advanced analytical computations.

Examples of the user interface for various proposed query builder tools can be see below in **Figure 6.45.A** and **Figure 6.45.B**.

Onpoint would work closely with the State to identify the final structure of the data, as well as fields to be included within the data dictionary for the warehouse. Fields from the raw data that may be accessible to the State include:

- All fields submitted by data submitters, including standardized and cleansed versions of this data provided by Onpoint
- All fields included in Onpoint's analytic enhancements, including:
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

Figure 6.45.A. DataGrip User Interface Example

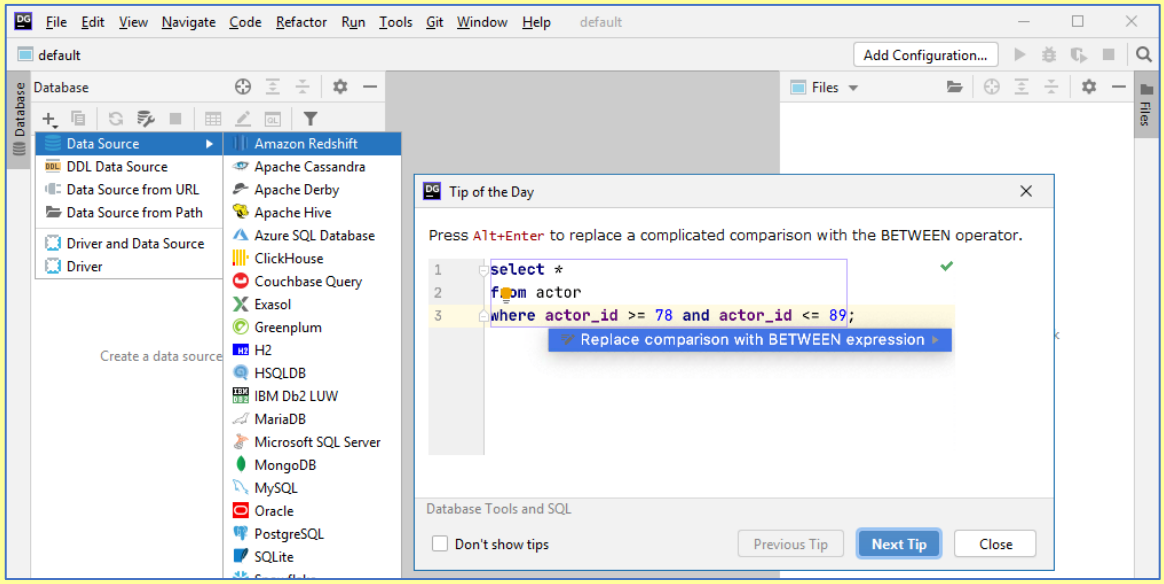


Figure 6.45.B. Tableau User Interface Example

6.46 Discuss your recommendations to implement rigorous privacy and security protections for the health information the APCD will receive, maintain, and release, including comprehensive administrative, technical, and physical safeguards. Be sure to specifically address the following:

Data use agreements

Review process for applications to use the data

Security and privacy protocols for data release (such as through a data enclave, data in transit, and data that are received and held by data users)

Authorized users and uses of the data

Disposal of the data once the period of use is completed

Attribution and acknowledgment of the use of the data

Penalties for violations

Health Information Privacy and Security Recommendations

The State can take a variety of approaches to ensure the privacy and security of the data collected in the APCD program. In general, the APCD Council and states with active data release processes such as Washington State are a great resource for Indiana as you develop your APCD program.

Data Use Agreements

IDOI can emulate and adapt APCD data use agreements (DUAs) used in other states. These DUAs typically specify the users of the data, the allowed uses, restrictions on further dissemination, a data management plan, restrictions on linkage of the data with other data sets (i.e., those that might, in combination with APCD data, allow for re-identification), and data destruction requirements at the end of the Agreement.

Review Process for Applicants to Use the Data

Applications typically are reviewed by a data release committee and approved by the state agency in charge of the APCD. These reviews ensure the appropriateness of the proposed use of the APCD data and that the applicant has the necessary administrative, technical, and physical controls in place to securely handle and store the data.

Security & Privacy Protocols for Data Release

The safest way to release data is often through the Analytic Environment as the data never leaves the control of the state (and its data vendor), all use can be monitored, and there is no uncertainty regarding whether the necessary safeguards are in place. States also can opt to send data sets to a data applicant (typically via SFTP) if the applicant can meet the state's data management standards in the DUA application process. Additional security and privacy also are provided by creating limited use data sets with identifiers removed and by creating aggregated public use data sets.

Authorized Users & Uses of the Data

Authorized users and uses of the data typically are decided by State in adherence with applicable federal and state privacy laws and the public policy objectives of the state agency leading the APCD.

Disposal of the Data Once the Period of Use is Completed

Typically, DUAs include provisions for the destruction of the data in accordance with NIST 800-88 at the completion of the agreement. For data access granted through the Analytic Environment, access to the Analytic Environment can be removed at the end of the agreement or at any time upon client request.

Attribution & Acknowledgment of the Use of the Data

States typically have guidelines and restrictions on the publication of reports from the APCD data. For example, there may be prohibitions on publishing cell sizes smaller than 11 in alignment with CMS standards to prevent identification of individual members. Publication and public uses of the data may require acknowledgement of the APCD data source or contain standard language when describing the APCD data source as the state's discretion.

Penalties for Violations

Onpoint would defer to legal authorities on the type and magnitude of penalties for violation of the state's APCD program policies, which often are determined by state law. Typically, in our experience, violations are very rare. Data use agreements typically have provisions that require adherence to federal and state law, allow the state to audit the recipient's use of the data, require disclosure of any unauthorized uses, require the recipient to assume the cost and liability of any breach of the agreement, require the recipient to indemnify the State for the recipient's actions, and note that any violations of the agreement may be reported to state and federal law enforcement officials.

6.47 Discuss your de-identification methodologies that can be used to create public-use data sets. Discuss the use of longitudinal identifiers as well.

De-identification methodologies for public-use data sets. Onpoint's data security protocols ensure that personally identifiable information (PII) and protected health information (PHI) are protected from unauthorized release in data sets and reporting delivered to meet our clients' requests. All data sets delivered on behalf of clients adhere to data use agreements that govern access to protected identifiers. No public-facing report produced by Onpoint will contain PHI or PII, according to our strict data release safeguards. Additionally, summary-level public reporting will adhere to standards for blinding from CMS and to IDOI-specific standards if more stringent. Onpoint routinely collaborates with our clients to create and deliver summary level public-use data sets that have been de-identified using the methods above. These public-use data sets include the following examples of downloadable and interactive dashboards generated for public websites for our clients:

- **APCD Snapshot.** A quick and easy way to explore how healthcare is being delivered and consumed across the state, including which medical procedures are most common, which drugs are prescribed most often, and which areas incur the highest costs for health plans and consumers. See **Figure 6.47.A** for a screenshot of the APCD Snapshot deployed for Washington State's APCD, which is available here: https://www.wahealthcarecompare.com/wa-apcd-snapshot

Figure 6.47.A. WA-APCD Snapshot (Top Medical Procedures Example)

Rank	Procedure Category	Type of Setting	Claim Count	Total Allowed Amount	Allowed Amount per Claim
1	Office/outpatient services - Office visits	Provider	26,102,584	$3,601,395,545	$137.97
2	Physical/occupational/speech therapy - Exercises	Provider	14,514,017	$755,618,753	$52.06
3	Laboratory - Chemistry and hematology	Independent Labs	10,443,493	$197,540,472	$18.92
4	Laboratory - Chemistry and hematology	Outpatient	9,052,538	$498,706,652	$55.09
5	Psychological and psychiatric evaluation, therapy	Provider	8,956,164	$1,174,723,444	$131.16
6	Prophylactic vaccinations and inoculations	Provider	7,762,652	$388,445,528	$50.04
7	Laboratory - Other	Independent Labs	5,823,347	$133,552,923	$22.93
8	Laboratory - Chemistry and hematology	Provider	5,339,916	$124,155,211	$23.25
9	DME and supplies	Provider	4,947,977	$742,640,083	$150.09
10	Medications (injections, infusions, other forms)	Outpatient	4,408,147	$2,033,942,232	$461.41
11	Alcohol and drug management, treatment, and rehab.	Provider	4,401,759	$186,783,505	$42.43
12	Ophthalmologic/otologic diagnosis and treatment	Provider	4,115,566	$298,685,187	$72.57
13	Laboratory - Other	Provider	4,047,025	$122,825,760	$30.35
14	Microscopic examination (e.g., lab, toxicology)	Independent Labs	3,949,149	$122,195,286	$30.94
15	Laboratory - Other	Outpatient	3,749,056	$206,853,573	$55.17
16	Radiology - Diagnostic (other)	Provider	3,748,654	$154,200,760	$41.13
17	Hospital inpatient services	Provider	3,504,019	$430,707,425	$122.92
18	Office/outpatient services - Preventive visits	Provider	3,174,912	$585,717,408	$184.48
19	Musculoskeletal procedures - Therapeutic (other)	Provider	3,055,851	$110,212,162	$36.07
20	Emergency department services	Provider	2,560,546	$356,315,063	$139.16
21	Microscopic examination (e.g., lab, toxicology)	Outpatient	2,478,395	$132,746,361	$53.56
22	Emergency department services	Outpatient	2,410,012	$1,118,239,396	$464.00
23	Office/outpatient services - Office visits	Outpatient	2,375,971	$308,316,624	$129.76
24	Medications (injections, infusions, other forms)	Provider	2,240,723	$1,500,451,276	$669.63
25	DME and supplies	DME (Durable Me..	2,008,065	$313,703,823	$156.22

- **Public use file download.** The Minnesota APCD provides no-cost downloads of public-use data sets, developed by Onpoint, across multiple domains, including services, primary diagnosis, utilization, prescription drugs, provider specialty, and member. The de-identification of these data sets uses the same principles as the APCD Snapshot, but the summarizations were developed to provide de-identified data at a less aggregated level. In this case, the redaction is iterative. That is, for cells with identification risk, geographical detail is redacted first; when recalculated cells continue to pose potential identification risk, member and paid amounts for one or multiple age groups are redacted next. In some instances, the remaining diagnosis information still poses potential identification risk and is therefore redacted completely. This de-identification method was chosen for this situation to maximize the retained total dollars. Examples of the public use files and documentation can be found here: https://www.health.state.mn.us/data/apcd/publicusefiles

Longitudinal identifiers. A signature component of Onpoint CDM is its ability to generate reliable master patient and provider indexes. Since health insurers often use multiple proprietary claims and eligibility systems that can differ across even their own products and regions, it often becomes difficult to track patients when they change health plans due to a change in employers, becoming Medicaid or Medicare eligible, or other life events. For this reason, it becomes critical to develop person-specific identifiers that allow analyses to track a single member both

longitudinally over time and laterally across payers. Onpoint CDM provides this important function through a proven, multi-phase member clustering process (**Figure 6.47.B**).

Figure 6.47.B. Building Longitudinal Patient & Provider Identifiers

Onpoint's proven approach is validated through the generation of survival analyses, which measure the number of covered lives at a given time period and for what length of time, both prospectively and retrospectively, each member can be identified within the APCD.

6.48 Discuss your recommendations to develop an infrastructure and implement a process that is adequately resourced to ensure timely release of data to approved data requesters. This process should be well-articulated, transparent, and include all steps involved, such as:

Information that must be supplied in an application

Receipt of application

Review of applications

Required modifications (if any) of the application to permit use and transmission of data to approved users

Transmission of data to approved users

Onpoint has worked with several clients to successfully launch a data release process. The process includes working with a data release committee to formalize the governance of the data, typically based on the enabling legislation for the APCD. Key areas of governance that the IDOI team will want to evaluate include the scope of data available for release, the types of eligible data recipients/users, the cost of the data products, and the data application process. Described below are additional details regarding Onpoint's recommendations.

Information that must be supplied in an application

To request data, applicants should be required to provide information that includes:

- Information about the applicant (e.g., researcher, government agency, other) and whether they are for-profit or nonprofit
- Description of the funding source for the work
- Type of request (e.g., custom data set, standard data set, analytic report)
- Where the data set will be accessed (e.g., IDOI's Analytic Environment, data user environment)
- Details about the project, timeline, and intended use
- What protected information is required for the user to achieve the goals of the study (e.g., financial information, geographic level of detail, age in months)
- Institutional review board status
- Frequency of request (e.g., one-time, quarterly refresh, annual refresh)
- Specific data elements requested and justification for their use
- Whether the data will be linked with additional data sources
- Data security credentials and data management plan

Receipt of Application

In Onpoint's experience, the annual number of data request applications ranges from 10–50, allowing a number of options for IDOI to receive applications – from a simple solution using email sent to a designated contact through more complex options that would leverage the Access IN website.

Review of Applications

Application review typically is performed through a multi-tiered process. First, a lead from the APCD will work with the data user to answer questions about the process, inform the available options, and ensure that the data requestor has all required elements completed. After receipt, data release committees often require that the application undergo a period of public comment. After public comment, the data requestor is often invited to discuss their application and allow the committee to ask questions. The committee then provides a final review, approval, or amendment to the application.

Required Modifications … to Permit Use & Transmission of Data to Approved Users

Once a data applicant has gone through the data release process, Onpoint would recommend having an abbreviated process for them to follow-up with any modifications to the original application. The modification process would allow requests such as adding a new use case or increasing the frequency of data receipt to be expedited.

Transmission of Data to Approved Users

Once an application is approved, the data set would be created and transmitted to the user. Onpoint recommends delivery of data sets within a secure environment so that IDOI can provide role-based access rather than delivering text files to external locations.

6.49 What would the process be for implementing updates and communicating changes to submitters?

Onpoint is committed to continuously improving the quality of the data received for our clients' APCDs so that they continue to meet the evolving needs of policymakers. Onpoint will review Indiana's DSG with IDOI, key stakeholders, and submitters at least annually to review programmatic changes, industry updates, and data availability that may warrant changes to the DSG, providing specific recommendations on any gaps that may exist and insights from across our client base. All layout changes for the APCD will be managed independently of other clients and will be implemented only after approval by IDOI.

Throughout the APCD's operations, data completeness thresholds will be continuously monitored and updated to target specific data quality improvement initiatives. In addition, whenever a field is added or updated, our staff make corresponding updates to Onpoint CDM's validations library, installing and/or updating validation logic to ensure that the data will be properly reviewed. Onpoint's validations can be updated whenever needed and are confirmed prior to final roll-out using a thorough testing process. Similarly, threshold updates based on DSG changes are possible at any time based on IDOI's approval and are coordinated with proactive communications and lead time for submitters. With every update, all associated documentation is updated and refreshed in the Onpoint CDM portal to ensure that submitters always have the latest specifications. Onpoint will provide DSG updates and trainings via Submitter Workgroup Meetings as needed to provide overviews of key changes to the latest version of the DSG, including any revisions to general submission guidelines, file submission methods, data quality requirements, and data submission timelines.

These trainings are supplemented by scheduled one-on-one check-ins with each participating submitter to learn details about their data submissions and any possible challenges that they may foresee with data submissions. Training sessions also are not restricted to project implementation: Whenever a new submitter is identified or a situation arises that requires action by a submitter, Onpoint will work with them to address their questions and ensure that the State's data collection remains on track.

All submitters have the ability to submit test files via Onpoint's CDM portal at any time. These test files are used most often during onboarding to verify accurate coding of submitters' data files and also are helpful to test updates related to DSG changes or whenever submitters undertake system changes. Although test files can contain true "test" data, Onpoint CDM is engineered with the same security controls for all files and allows submitters to use actual production data from their systems to verify that their data is being pulled correctly. This latter approach improves Onpoint's ability to validate submitters' actual data and helps submitters shift to production submissions more seamlessly.

6.50 What will the intake process be for new submitters, and who will be responsible for which required activities?

Onpoint's approach to onboarding new submitters mirrors our approach to onboarding the State's first submitters. Our onboarding approach is focused on active support that includes both real-time solutions such as webinars, screen-sharing, and phone calls as well as documentation such as user

guides, and reference materials. These on-demand resources are available 24/7 at the secure Onpoint CDM portal, which is a familiar and regular resource to our clients and their submitters.

Onpoint's Data Operations team works diligently to promote collaborative and results-oriented relationships with data submitters. Our staff prioritize collaboration and provide steady communications using a suite of tools that keep stakeholders connected every step of the way – a process that is key to helping them understand the requirements and reporting the necessary data. This always-available approach is a hallmark of Onpoint's work and is recognized by data submitters as a differentiator. We pride ourselves on the close relationships that we build with our clients' data submitters, recognizing that strong support is key to maintaining their cooperation, collaboration, and the critical buy-in and data accuracy needed for an APCD.

While Onpoint CDM has been designed to deliver intuitive and user-friendly support, we also value face-to-face time with submitters to provide real-time support and engage with them. Each client's dedicated Data Operations analysts are backed by a team of health data analysts and technical staff who are available to work one-on-one with each submitter to resolve any issues and questions as quickly as possible.

While Onpoint's skilled Data Operations team is responsible for the onboarding process, IDOI would be responsible for initial communications with new submitters that the State identifies as potential participants in the APCD and approval of their participation in the APCD prior to onboarding beginning.

6.51 How will you advise first time data submitters on how to map existing fields in their system to the APCD format?

To help submitters become familiar with state collection regulations, Onpoint always provides a data submission guide (DSG) that includes links to relevant laws and regulations regarding data collection, data specifications, and detailed mappings to applicable standards (e.g., UB-04, HCFA 1500, HIPAA ASC X12-270/-271 transaction sets for eligibility data, X12-837/-835 transaction sets for claims, ADA Dental Claim form, NCPDP guidelines, etc.). DSGs also feature detailed information about the data submission process, registration and submission timelines, details regarding data security and encryption, and specifications related to the required data elements (e.g., field definitions, layouts, and acceptance thresholds).

Clear direction in the data submission guide helps guarantee an accurate understanding of the required data elements, accelerating the onboarding process and enhancing the quality and consistency of data across payers. DSGs should be reviewed with payers and other stakeholders at least annually and should be updated whenever collection requirements change.

6.52 What type of documentation, instruction material, and live support can you provide to data submitters?

Onpoint prioritizes collaboration and provides steady communications with submitters using an array of tools that helps keep them connected every step of the way. In addition to the Data Submission Guide described above, these tools include direct outreach from Onpoint's Data Operations team via email and phone calls, all-submitter calls and webinars, email updates with

helpful tips, and other notices. **Table 6.52.A**, below, outlines some of the standard key meeting types and content that we provide for our APCD clients.

Table 6.52.A. Standard Key Meeting Types & Content

Meeting	Objectives	Related Resources
Data Submitter Meeting: Onpoint CDM Overview	Provide an overview of the approved IDOI Data Submission Guide (DSG), including general submission guidelines, file submission methods, data quality requirements, and data submission timelines	• IDOI data submission overview presentation materials • IDOI DSG • IDOI Schedule
	Provide an overview of the Onpoint CDM online interface, which will serve as a resource for authorized submitter contacts to monitor the status of their submissions, request variances, and access up-to-date quality and variance management reporting	• Onpoint CDM registration • Onpoint CDM user guide • Onpoint CDM video tutorials • Onpoint CDM technical appendix
	Provide an overview of Onpoint's secure file submission methods, including how technical submitter contacts can establish SFTP connectivity and encrypt their file submissions using the OpenPGP standard	• SFTP and PGP support presentation materials • SFTP and PGP user guide • SFTP registration form • Onpoint's PGP test file
Data Submitter Meeting: Data Submission Updates	Provide an overview of key changes to the latest version of the IDOI DSG, including any revisions to general submission guidelines, file submission methods, data quality requirements, and data submission timelines	• IDOI DSG • IDOI Schedule
Data Submitter One-on-One Meetings	Ad hoc meetings for submitters to ask questions that have arisen. The 1:1 support typically takes one of two forms: (1) Office hours that allow for any submitter contacts to call-in at a regular time each week and ask questions, and (2) scheduled meetings dedicated to a specific submitter.	• IDOI DSG • IDOI Schedule • Onpoint CDM • Submission quality reports

Data submitter feedback from our most recent implementations includes the following unsolicited comments (blinded to protect privacy):

- *"Onpoint provided very complete guidance on connecting to their submission portal and making submissions. Bravo for good documentation."*
- *"Very good communication and willingness to help on the part of Onpoint."*
- *"And I want to take a moment to let you know how much I appreciate working with you. Throughout my career I usually dread being assigned to work with a third party vendor data person. But (at least from my point of view) you and I have developed a really good working relationship. I just wanted to let you know that this is noticed and much appreciated. Thank you."*
- *"Thanks, Onpoint! We truly appreciate your support and insight through this process!"*
- *"I would also like to add my thanks for all the work Onpoint has done with us. I can speak for all of us at [payer name redacted] that we are very appreciative of the responsiveness and helpfulness of all of you."*

6.53 What are your policies for data destruction upon termination?

Onpoint's standard transition plan includes the transfer of the State's historical data to a vendor as directed by IDOI, followed by the documented destruction of all data provided to Onpoint by submitters and the State related to the APCD contract in accordance with the State's policies and timelines regarding such destruction. Additionally, Onpoint follows U.S. National Institute of Standards and Technology (NIST) 800-88 guidelines for sanitizing devices at end of life to ensure secure data disposal. Hard drives, which contain only encrypted data per standard policy, are overwritten and then shredded, and information and electronic media are disposed of in accordance with NIST guidelines.

6.54 Health payers (insurance carriers, specifically), expend a great deal of time and money trying to analyze, design, negotiate, and maintain health care provider networks. Even with these efforts, provider networks commonly contain inaccuracies and outdated information.

a. What mechanisms would you propose to help carriers and providers streamline and simplify the process of maintaining network participation data in real time?
b. What additional functionality would you add to help providers find established networks, and to join or leave a network?
c. What tools would you recommend be added to help carriers and the State analyze provider networks for network adequacy?
d. Would you recommend charging carriers, providers, or researchers for these tools, services, or data, and if so, what would the fee structure be?
e. Provide a supplement to the Cost Proposal Template (as a separate attachment; not as part of this Technical Proposal response) to reflect the added expense/income associated with this enhancement.

APCDs can be a useful support to the development of a reliable provider directory solution. On their own, APCDs are insufficient to meet all of the identified functional requirements. Consistent provider-to-practice, practice-to-contracting entity, and contracting entity-to-health plan relationship information is not reported to an APCD. State APCDs, however, can serve as an important, complementary data source in building a provider directory. The hard work of maintaining provider relationship data will require dedicated planning, investment, and a specific technology solution. A provider directory solution would become the source of truth used to resolve inconsistencies and inaccuracies in provider affiliation information across health plans, provider groups, and other organizations.

a. What mechanisms would you propose to help carriers and providers streamline and simplify the process of maintaining network participation data in real time?

We would recommend that the State invest in a dedicated provider directory solution to efficiently maintain accurate, real-time network participation data. The provider directory would be updated electronically by health plans or contracting entity provider network databases or systems.

Relevant data elements captured within an APCD that can support or supplement a provider directory include rendering and billing provider information, rendering provider group practice National Provider Identifiers (NPIs), and an in- and out-of-network indicator, for example. An "In-/Out-of-Network" indicator reported on claims by the submitters to determine participating and non-participating providers, which is common in many state APCDs, would serve as an initial building block for the determination of in-/out-of-network providers used for analytics and

reporting. With this field included in a provider table in the quarterly data extract alongside other fields like NPI, specialty code, and provider street address, analysts could identify network attributes as submitted by the health plans.

A provider directory solution would standardize the approach and decrease the number of processes that any one organization would need to implement in order to participate. A provider directory solution would centralize roster maintenance, enabling health plans and others to log in and identify and update provider relationship information in real time. A provider directory solution would facilitate IDOI's evaluation of network performance and make data available that can be exported from the system and provided to stakeholders.

b. What additional functionality would you add to help providers find established networks, and to join or leave a network?

Functionality that would be required for providers to find networks and to evaluate whether they should participate would begin with a centralized repository that contains a directory of networks and participating providers that can be easily and regularly updated. Two options available from Onpoint that could meet this need, at least in part, would include:

1. Use an application that offers provider roster maintenance functionality. Onpoint would propose that the State evaluate its specific needs in collaboration with key stakeholders and invest in the most appropriate process and technology. If it is unable to pursue a full-blown provider directory solution, as a starting point, Onpoint has a roster management module within our Performance Reporting Portal (PRP), which would be a relatively low-cost starting point. The PRP would be an appropriate solution if tied into IDOI's public-reporting initiative, which could include a review and reconsideration process as well (a typical requirement associated with provider-identified reporting).
2. Add specific data to the APCD submissions that would include a network indicator, member plan identifier, and details about the rendering and billing providers. This information would be required in the claims information to allow for the attribution of members and providers to networks. The advantage of this method is that it minimizes the effort for data submitters; its disadvantage is that the data is updated only quarterly and requires further processing to display and inform a directory.

c. What tools would you recommend be added to help carriers and the State analyze provider networks for network adequacy?

Through an APCD, the State can assess all providers across the state, including their specialties, the services they deliver, and the cost and quality of those services. To evaluate network adequacy, the State would need a provider registry to accurately affiliate individual providers with groups and networks. We can, through the claims and provider file submissions to an APCD, develop an individual provider-to-payer network directory that would include provider specialties, provider locations, and affiliations with hospitals, for example. APCD enrollment data could be used to assess the population being served by health plan networks and whether the population's needs are being met.

Another tool that we would recommend for analyzing provider networks and network adequacy would be the reporting solution detailed in this proposal's responses to questions #10.4 through #10.7 in Section 10 ("Analytics"), which could be expanded to include reporting on networks. The Tableau-based reporting solution and associated data marts would allow the State more flexibility

around aggregating data and drilling into questions regarding network adequacy. Onpoint would collaborate with IDOI to create custom dashboards focused on metrics for evaluating networks.

d. Would you recommend charging carriers, providers, or researchers for these tools, services, or data, and if so, what would the fee structure be?

To the extent that IDOI expands Onpoint's scope of services to include, for example, additional data collection, reporting services, or leveraging Onpoint's roster management module within the Performance Reporting Portal application, the State would be assessed fees depending on the scope of services as detailed in Onpoint's Cost Proposal Supplement: "Onpoint - IN RFP 22-70302 - 2.5.4 - Cost Proposal Supplement (2022-04-04).pdf". In turn, IDOI could seek to recoup some of these costs from carriers, providers, and researchers through a subscription-style service model that provides access to data and reporting. In other states, this process has started with a market survey to gauge customer interest, collect feedback on specific reporting and data that might be of particular value, and determine appropriate pricing.

e. Provide a supplement to the Cost Proposal Template (as a separate attachment; not as part of this Technical Proposal response) to reflect the added expense/income associated with this enhancement.

For details related to the cost of including potential services Onpoint has outlined above, please see Onpoint's Cost Proposal Supplement: "Onpoint - IN RFP 22-70302 - 2.5.4 - Cost Proposal Supplement (2022-04-04).pdf".

7. Data Production and Consumer Website

7.1 How would you establish a public web portal for individuals to compare prices quickly and easily for the full spectrum of medical billing codes as well as check quality ratings of health care providers?

Among the primary use cases to be supported by the Indiana APCD will be a new, public-facing transparency web portal that delivers timely data to consumers and other stakeholders regarding the cost of common services and quality of care being delivered by providers across the state. Onpoint will leverage our experience designing similar solutions for other states, such as Washington State's award-winning consumer website (Washington HealthCareCompare), and work collaboratively with the IDOI team to design a solution that addresses the State's needs and vision. Our proposed solution for IDOI includes a new website featuring a suite of consumer-facing dashboards that provide insights into the cost and quality of care.

Our solution will include interactive dashboards developed using Tableau, a market-leading data visualization tool with a dynamic interface that allows end users to flexibly choose the reporting dimensions of their choice, search the data, filter the data, and drill down into specific areas of interest. The Tableau dashboards will be embedded within a public-facing, mobile-friendly website that provides clear instructions for navigation and use, extensive flexibility, a rich set of functions and features from which to choose, beautiful visualizations, easy-to-understand language, and the ability to regularly update content throughout the product lifecycle.

Approach

Onpoint will leverage our experience in designing public-facing reporting solutions along with the lessons learned from other successful consumer-focused reporting tools. Onpoint's flexible approach distinguishes our team from other contractors. We will work iteratively through the

specifications, design, development, and reporting process. During requirements gathering and report design sessions, Onpoint will draw upon our many years of experience using APCDs to analyze cost, utilization, access, quality, equity, and member demographics to deliver meaningful, intuitive public-facing reports and websites. Each of our public-reporting initiatives is distinct and tailored to our client's specific audience, requirements (legal and other), communication strategy, and budget, and we will follow that same approach in support of IDOI to ensure that Indiana's consumer-facing site addresses all RFP requirements.

Onpoint will lead initial planning sessions to address any open questions regarding the vision, purpose, and topic areas of interest and then shift to content and design questions. We will work with IDOI to identify desired geographical and other stratifications, demographic breakouts, and other considerations.

Our experience with other public reporting initiatives has emphasized the importance of working collaboratively with IDOI staff and stakeholders to create a user-friendly, well-designed website that will provide consumers and other stakeholders with useful comparative information regarding healthcare services being delivered in Indiana. Furthermore, our previous experience in designing and implementing public-facing reporting has equipped us to recognize and respond to the privacy and security requirements associated with this type of reporting. These include the engineering of public use data sets through statistical de-identification, small-cell blinding, and incorporating client-specific data security requirements.

The requirements-building process will be collaborative in nature and employ Agile principles in order to deliver a product that effectively addresses IDOI's vision and requirements in a timely manner. Related tasks include:

- Collaborating with IDOI to collect requirements that inform the design and content of the website and reporting/dashboards
- Providing recommendations for IDOI's review and approval regarding measures selection and the corresponding methodology documentation to be included in the first release
- Developing public reporting templates and mock-ups that display comparative information geared to consumers
- Iterating report development as needed to satisfy IDOI's agreed-upon requirements and design standards
- Collaborating with IDOI's technical staff and design resources to plan for and design an appealing integration of Tableau-based dashboards into a public facing, mobile-friendly website
- Deploying the public-facing dashboard reporting within the new website
- Refreshing the data sets and public-facing reporting on an annual basis
- Providing technical assistance and documentation to IDOI and end users
- Collecting stakeholder feedback to inform updates for future releases

In some states – Washington, for example – prior to public reporting, providers are often allowed to view their results and provide feedback or challenge the findings. Onpoint's Performance Reporting Portal (PRP) is a useful tool for this type of review and reconsideration as well as for provider roster management. While we have not budgeted for deployment of the PRP based on the

RFP's requirements, it is a possibility if Indiana would like to explore that option. Features of the PRP are explored further in our responses to the Technical Proposal's questions #2.6 and #6.54.

Summary of Content

Onpoint proposes to develop four (4) content-rich dashboards in conjunction with IDOI staff to be provided on the consumer site. Anticipated dashboards would be designed to answer the following questions:

1. **What are the typical prices of common shoppable healthcare procedures in the state?** This dashboard would provide statewide median for key healthcare procedures as well as the 25th and 75th percentiles. Data would be provided for the commercial population by geographical region as well as by commercial carrier. Typical member out-of-pocket payments for each procedure also would be presented.
2. **How do prices vary by provider facility?** This dashboard would provide the median allowed amount (plan plus member paid) as well as the 25th – 75th percentile range for key healthcare procedures at specific provider facilities. Consumers would be able to filter by service and to search by ZIP code or other geographical stratification to find and compare providers in a specific area. Where there is sufficient service volume by carrier, median prices by commercial carrier for each service and median out-of-pocket costs also would be presented at the provider level. Inpatient facility quality measures would be provided alongside cost when available.
3. **How does quality of care vary by facility in Indiana?** This dashboard would provide information regarding the quality of care at inpatient facilities throughout Indiana using national standard metrics for quality of care to allow consumers and policymakers to compare quality throughout the state and regionally.
4. **How do total cost of care, healthcare utilization, healthcare access, and quality of care vary within Indiana?** This dashboard would provide information on population health within the state, focusing on variation in cost of care, utilization of services, access to care, and quality. Data would be compared at a geographical level (e.g., county or hospital service area), with options to stratify/drill down by major payer (i.e., commercial, Medicaid, Medicare), age group, and gender. Data from the American Community Survey would be linked in to provide insights at the ZIP code level regarding how the healthcare measures corelate with race, income, and education. We have not budgeted for primary care practice reporting of quality in this proposal but have done this for other states and could do so for Indiana if desired.

Our proposal includes a dedicated Analytic Engineer with strong claims data analysis and data visualization expertise to support IDOI in the requirements gathering and report development processes, which will be collaborative and iterative. Once launched, the reports will be refreshed annually with new data.

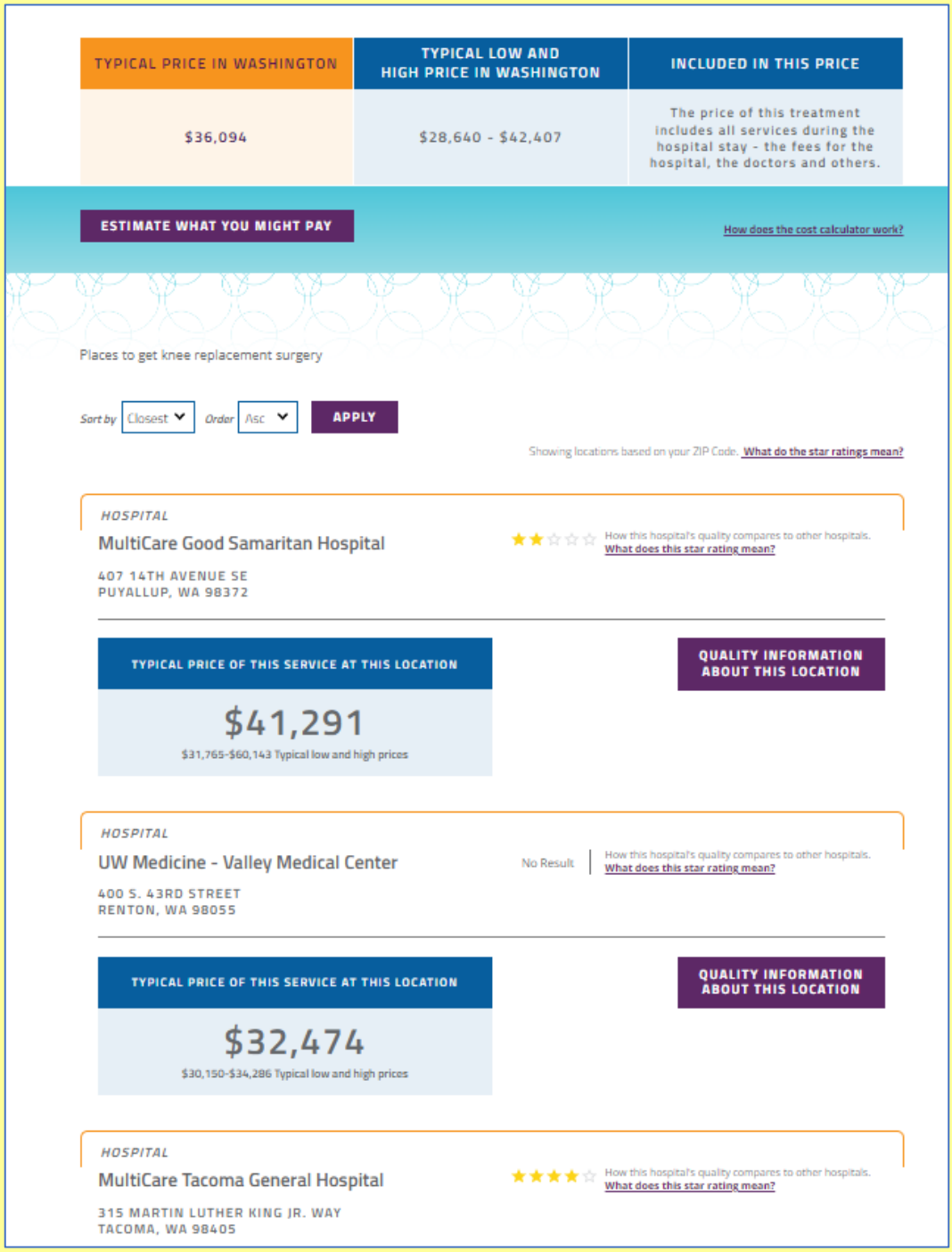
7.2 How do you propose to display average negotiated charges by each health carrier for specific health care services provided by an individual health care provider, as well as the quality metrics for facilities and providers for specific health care services? (Note: For the purposes of this question, facilities and providers include hospitals, physician groups, ambulatory outpatient surgical centers, physical therapy offices, imaging centers, laboratories, infusion clinics, pharmacies, and any other location providing health care services.)

Displaying average negotiated charges by each health carrier. To create comparative cost reporting for Indiana, Onpoint proposes to our Service-Focused Episodes (SFE) grouper. Unlike most commercial groupers, Onpoint's SFE grouper is fully transparent and was developed in collaboration with our state APCD clients and stakeholders in support of public transparency reporting. Our SFE grouper generates episode costs that can be reporting using a wide array of groupings (e.g., facility, geographical location, major payer, carrier). The grouper uses four different methods to group the data by claim type: inpatient, outpatient surgery, outpatient diagnostic, and professional. Data are rolled up into episodes of care, which include all claims for the episode (e.g., all facility and professional claims for an inpatient stay; all claims billed during an outpatient surgical visit; both the facility and professional component for a diagnostic test), to ensure that the full cost of a procedure is captured. The full allowed amount / average negotiated charges that we display includes both the plan paid amount and the member responsibility amount (i.e., coinsurance, copay, deductible). Median allowed amounts are used to reduce the impact of high-cost outliers, and the 25th – 75th percentile is also presented to give the consumer an idea of the typical range of payments. Our reporting assumes that we will use information from claims and not payer/provider retroactive settlements or non-claims data.

For Indiana, we plan to provide data at the statewide and carrier levels, with geographical drill-downs for each procedure. We also will provide median allowed amounts and out-of-pocket amounts at the billing provider facility level, with breakouts for each carrier that has sufficient volume at each facility. Consumers and policymakers will be able to search by ZIP code or another key geography to find and compare facilities located in a specific area that provide the procedure in question. The address of each location will be provided. Data at the carrier level for each facility might result in small numbers in some situations. In alignment with CMS suppression standards, we typically blind any data with fewer than 11 services for public reporting to address privacy concerns.

These methods and tools have proven effective for Washington State's consumer website (**Figure 7.2.A**) and in our work with the APCDs in Connecticut and Vermont. We plan to generate an annual refresh of data.

Figure 7.2.A. Washington HealthCareCompare Consumer Website (Example Screenshot)

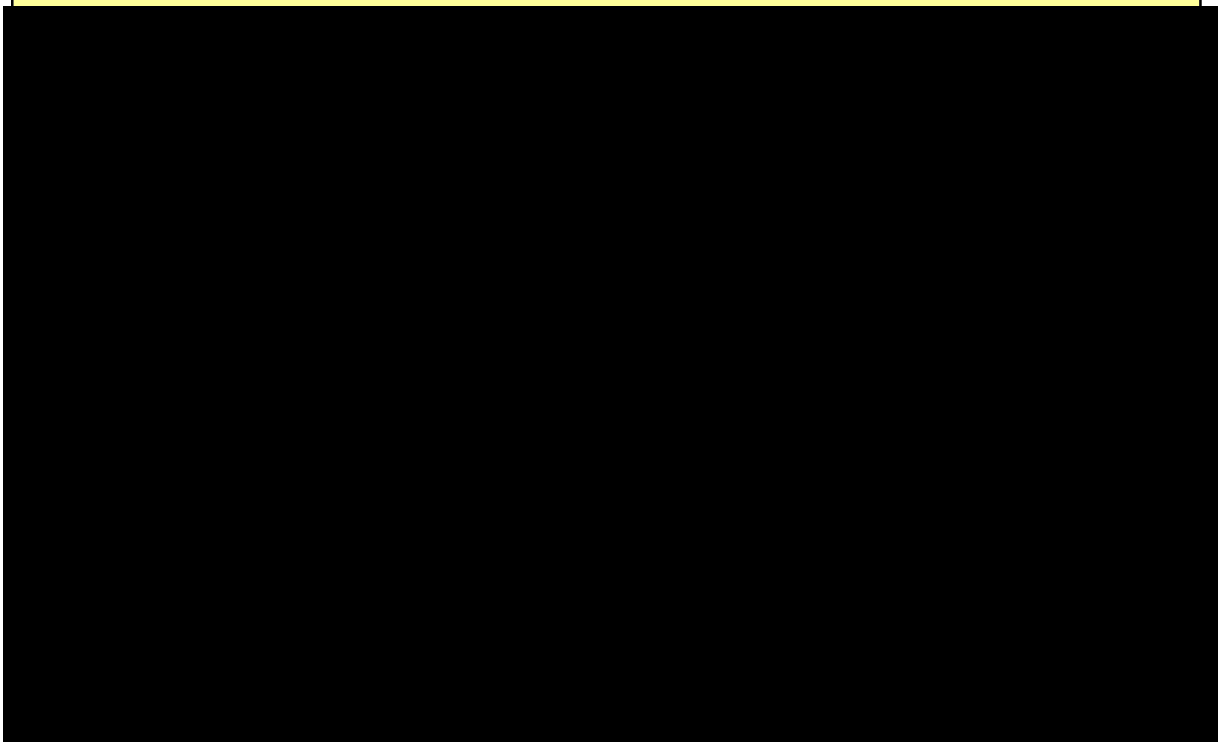


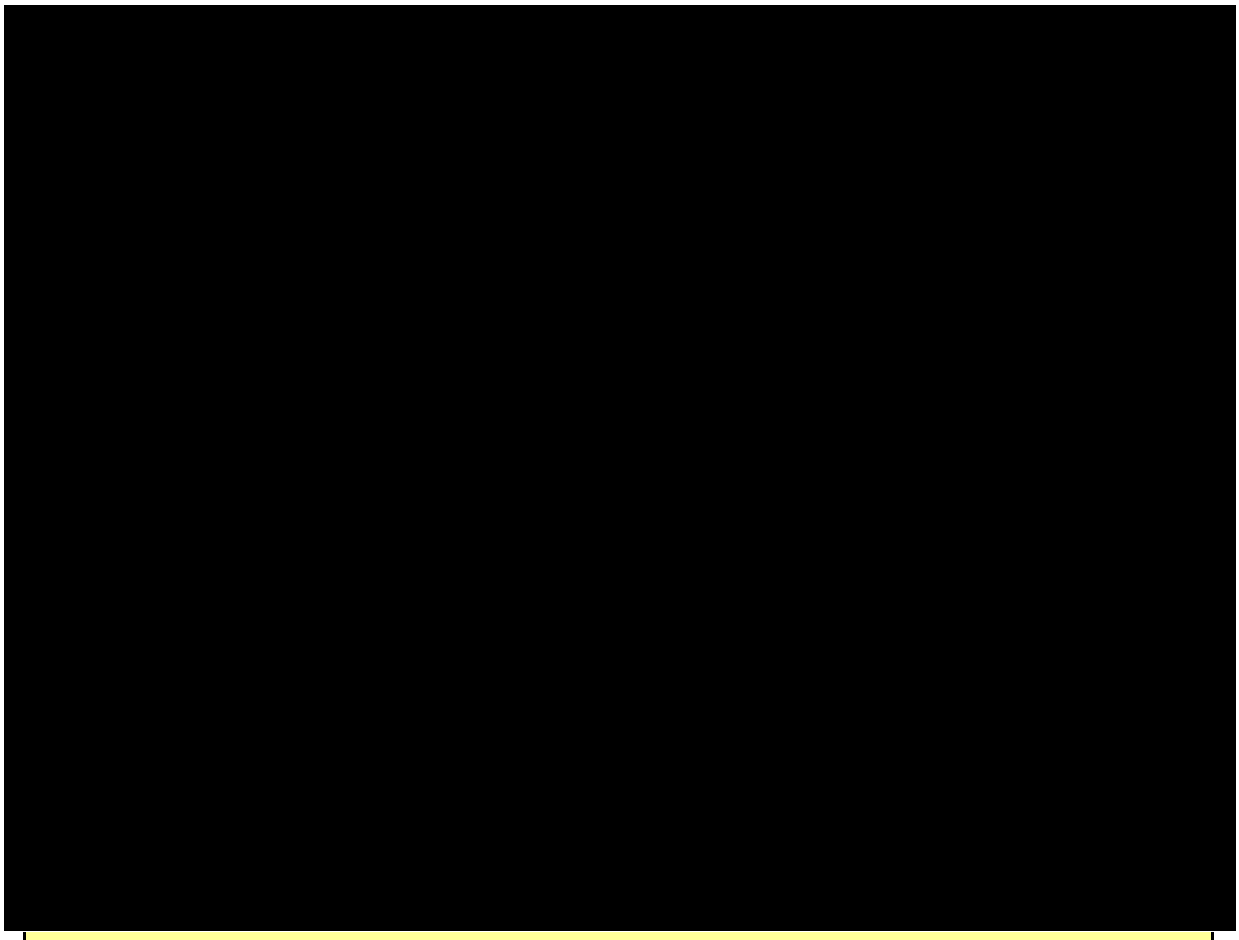
For Indiana, data will be provided using a set of Tableau-based dynamic dashboards embedded within a public-facing website. The Tableau approach will allow for comparisons of the data across facilities by procedure but will be highly flexible and allow for easy drill-downs and analytics. An example of some of our price transparency reporting in Tableau is shown in **Figure 7.2.B**.

Figure 7.2.B. Tableau Reporting on Facility Services & Episodes of Care (Mock Data)

Onpoint's SFE grouper includes an extensive list of 125 shoppable services that has been refined over time. A sample of the specific services that Onpoint proposes to include in price transparency reporting for Indiana are listed below in **Table 7.2.A**. We understand that Indiana is looking for services that may be provided at pharmacies. A comparison of drug prices at various pharmacies throughout the state could be done but would need to be evaluated separately.

Table 7.2.A. Sample of Services Proposed for IN APCD Consumer Transparency Reporting



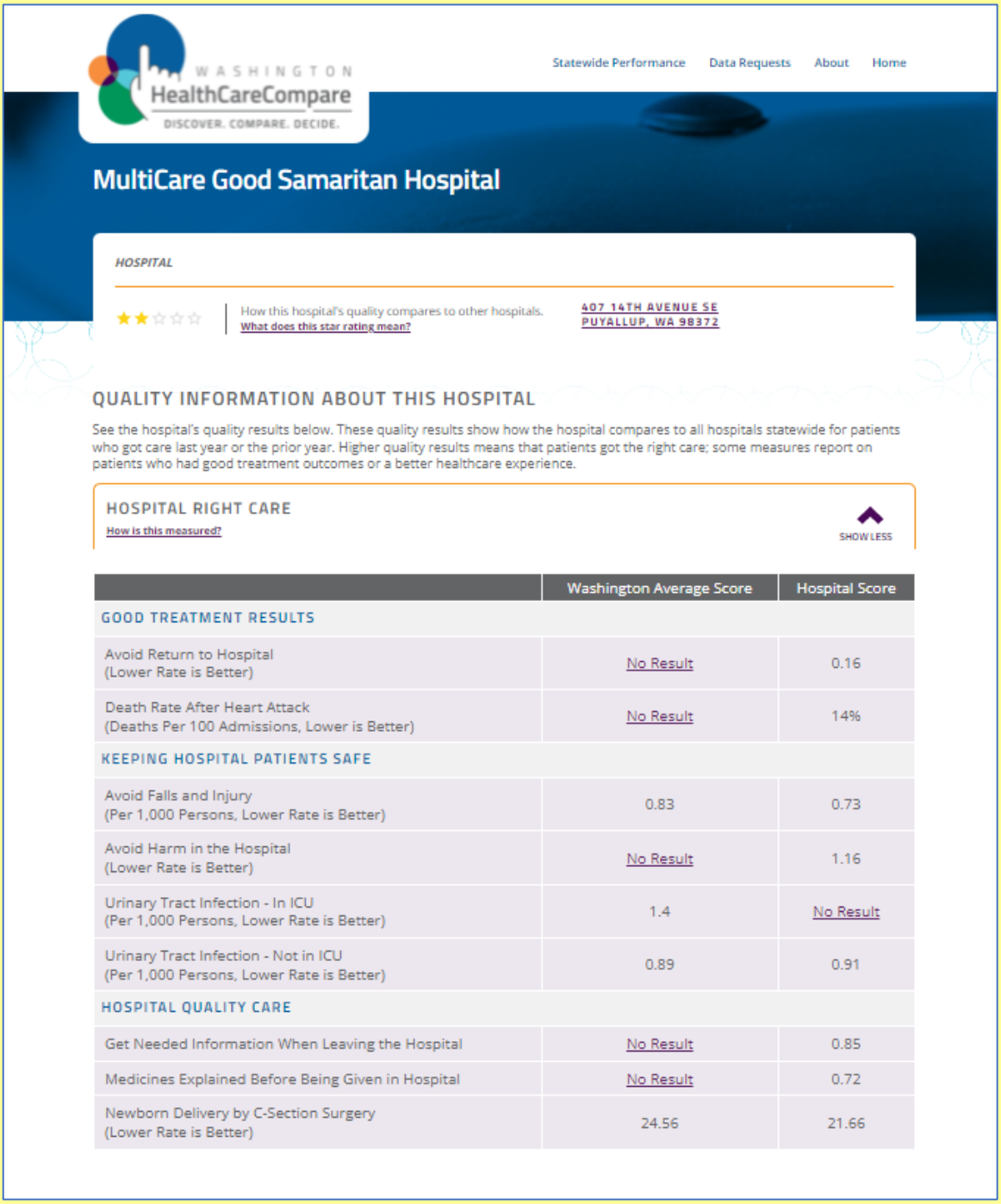


Displaying quality metrics for facilities and providers. It is important to include quality metrics for facilities and providers along with cost information to provide a full picture of care received at specific facilities and to ensure that quality, not cost alone, can be a consideration when selecting a facility. Onpoint plans to link in quality information with cost, when available, and provide a separate dashboard focused on quality at the facility/provider level.

For hospital facilities, Onpoint will include quality measures from CMS Hospital Compare. Specifically, Onpoint plans to leverage the composite star system (1 to 5 scale) plus five additional measures available in the CMS Hospital Compare data to inform and empower consumers. Hospitals with particularly high or low ratings will be flagged.

Examples of the types of information that will be provided in this dashboard can be found at the Washington HealthCareCompare website (**Figure 7.2.C** below).

Figure 7.2.C. Washington HealthCareCompare Price-Transparency Website



WASHINGTON HealthCareCompare
DISCOVER. COMPARE. DECIDE.

Statewide Performance | Data Requests | About | Home

MultiCare Good Samaritan Hospital

HOSPITAL

★★☆☆☆ How this hospital's quality compares to other hospitals. What does this star rating mean?

407 14TH AVENUE SE
PUYALLUP, WA 98372

QUALITY INFORMATION ABOUT THIS HOSPITAL

See the hospital's quality results below. These quality results show how the hospital compares to all hospitals statewide for patients who got care last year or the prior year. Higher quality results means that patients got the right care; some measures report on patients who had good treatment outcomes or a better healthcare experience.

HOSPITAL RIGHT CARE

How is this measured?

SHOW LESS

	Washington Average Score	Hospital Score
GOOD TREATMENT RESULTS		
Avoid Return to Hospital (Lower Rate is Better)	No Result	0.16
Death Rate After Heart Attack (Deaths Per 100 Admissions, Lower is Better)	No Result	14%
KEEPING HOSPITAL PATIENTS SAFE		
Avoid Falls and Injury (Per 1,000 Persons, Lower Rate is Better)	0.83	0.73
Avoid Harm in the Hospital (Lower Rate is Better)	No Result	1.16
Urinary Tract Infection - In ICU (Per 1,000 Persons, Lower Rate is Better)	1.4	No Result
Urinary Tract Infection - Not in ICU (Per 1,000 Persons, Lower Rate is Better)	0.89	0.91
HOSPITAL QUALITY CARE		
Get Needed Information When Leaving the Hospital	No Result	0.85
Medicines Explained Before Being Given in Hospital	No Result	0.72
Newborn Delivery by C-Section Surgery (Lower Rate is Better)	24.56	21.66

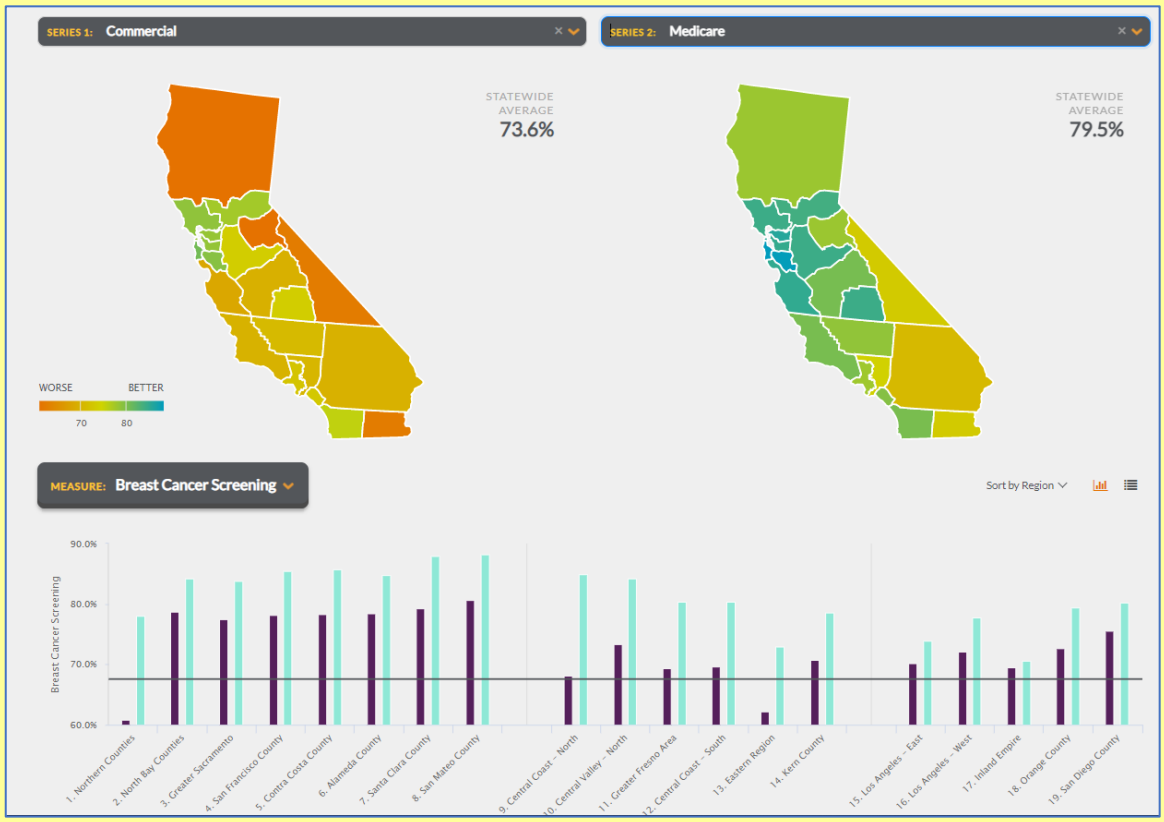
7.3 How do you propose to display health care utilization, expenditures, and quality and safety performance data?

Onpoint has performed a wide range of analytic services, including running cost, quality, and utilization measures, for APCD programs and other clients across the country for nearly 20 years

in order to support program evaluation and to help the public and policymakers identify gaps in care or variation in care. Several examples of public reporting of healthcare metrics and performance data include:

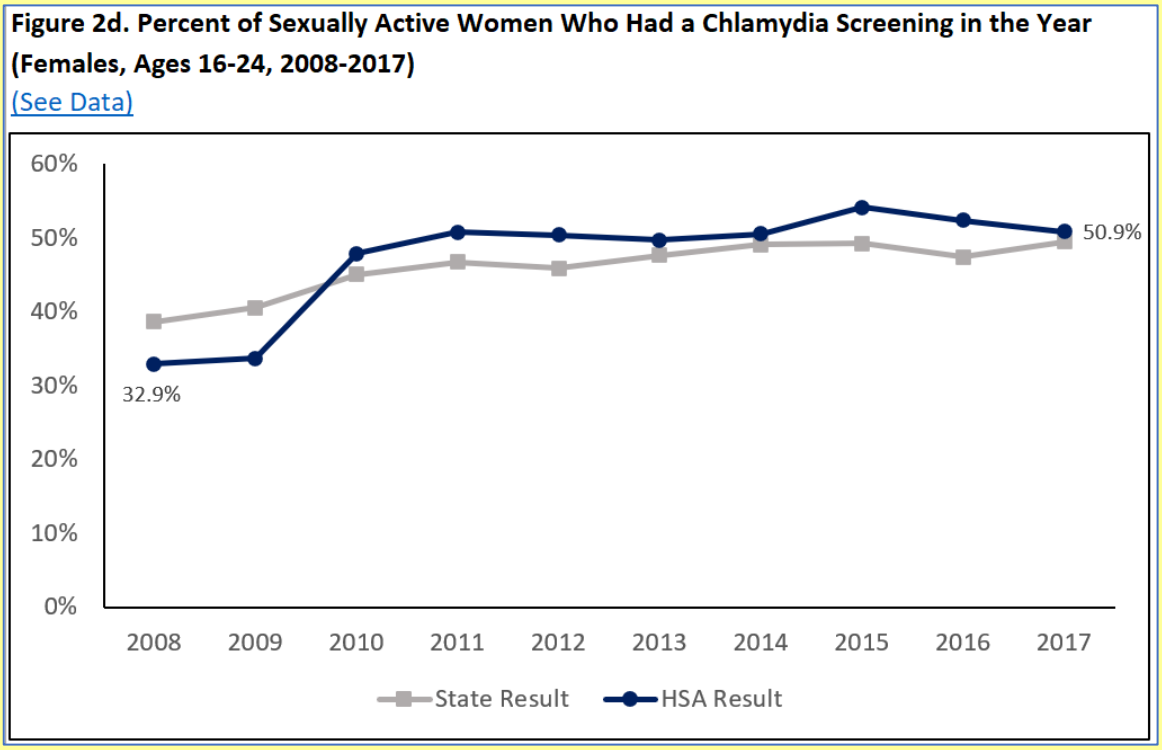
- IHA's California Cost & Quality Atlas – for which Onpoint calculates and produces results – provides variation reporting by geography, payer and product type, and payment design characteristics (**Figure 7.3.A**). Users can easily apply desired filters in order to compare cost and quality across regions by product type, for ACO vs. traditional PPO and HMO plans, as well as by type of provider risk sharing.

Figure 7.3.A. IHA's California Cost & Quality Atlas



- For the state of Vermont's Blueprint for Health, Onpoint conducted multiple evaluations of the state's Hub & Spoke opioid treatment model, which involved linkage of the APCD with clinical registry, incarceration, and other data sources, in addition to generating profiles by treatment site. Additional reporting for Vermont includes developing profiles for analytic priorities of the Vermont Blueprint's Women's Health Initiative, including providing a view of the health status of women and their access to primary care and preventive screenings, contraceptive care, and mental health and substance use disorder treatment (**Figure 7.3.B**). Onpoint analysts also have co-authored publications with Blueprint staff regarding data infrastructure to support population health management within a diabetes population.

Figure 7.3.B. Vermont Blueprint's Women's Health Initiative Reporting (Barre Example)



- In support of Washington State's Common Measures Set, Onpoint annually runs a set of HEDIS measures and links in additional measures provided by the state at the geographical or state level to support public reporting via the Washington HealthCareCompare website (**Figure 7.3.C**).

Figure 7.3.C. Washington's Statewide Common Measures Set Results (HealthierHere ACH Example)

KEEPING PATIENTS SAFE

How is this measured?

SHOW LESS

	Target	Washington Score	ACH Score
Avoid Wrong Medication for Bronchitis	70%	66%	74%
Appropriate Testing for Cause of Back Pain	83%	72%	75%
Avoidable Emergency Room Visits	No Result	44.08	38.02
Checking Patients on Blood Pressure Medications	87%	78%	80%
Getting Prescriptions for Both Opioids and Sedatives (Rate per 1,000 Persons)	No Result	15%	17%
Testing Children with Throat Infections	86%	78%	77%

Our solution for Indiana will include a base set of chronic condition flags, total cost of care measures, HEDIS quality of care measures, and utilization measures (**Table 7.3.A**). These will be

the building blocks for the Tableau-based reporting on cost, use, and quality. Users will be able to view geographical variation in rates of chronic conditions, quality of care, and utilization of services. Drill-downs by major payer (i.e., commercial, Medicaid, Medicare), age bands, and gender also will be possible.

Table 7.3.A. Measures for Indiana Public Reporting

[redacted]

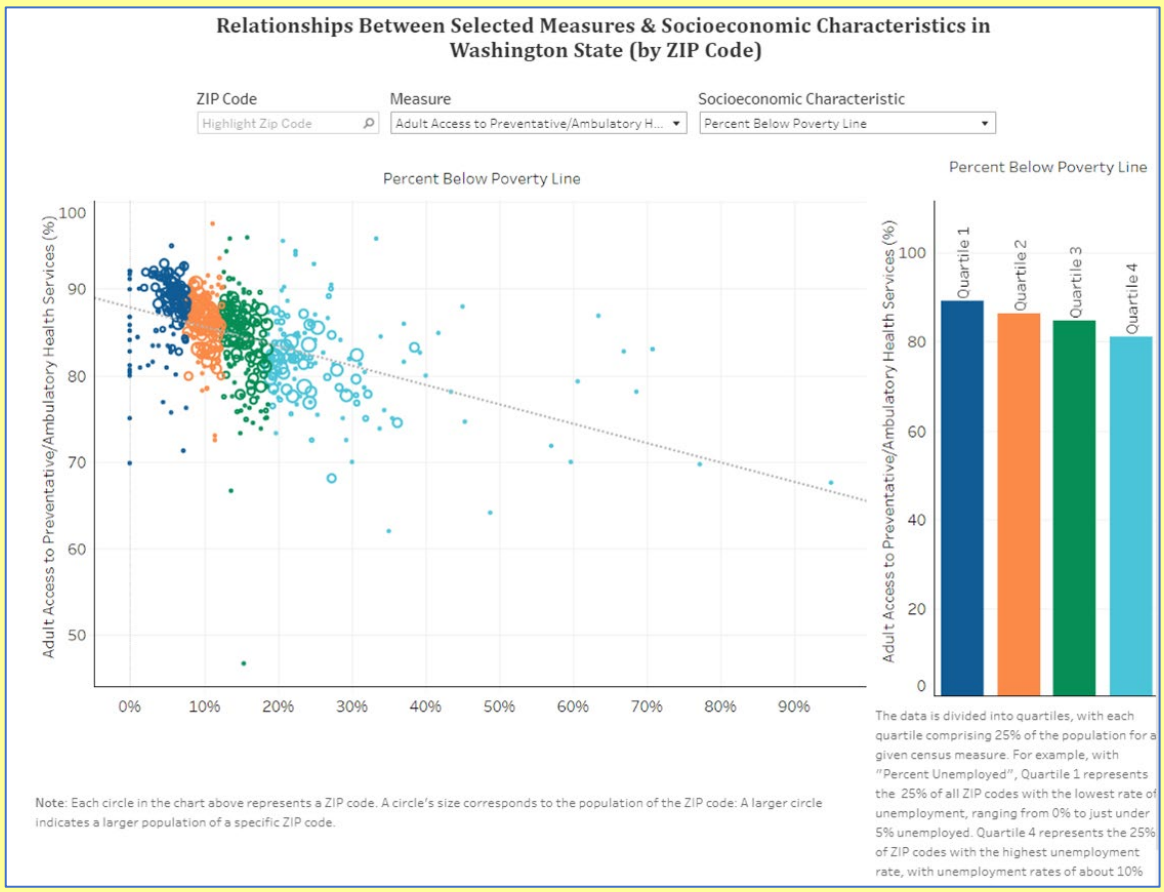
7.4 How do you propose to present data to allow for comparisons of geographic, demographic, and economic factors and institutional size?

Onpoint's price transparency reporting and our quality reporting both will have some comparisons of geographical, demographic, and economic factors and institutional size. On the price transparency side, our reporting solution for Indiana will include data on the volume of procedures and market share as well as the number of hospital beds at the facility. This will enable us to evaluate relationships between the cost of procedures and the volume of procedures and/or the size of the institution. Price transparency reporting also will include geographical comparisons to determine if there are disparities by geography (e.g., areas of the state where all hospitals are higher cost for a specific procedure).

The quality reporting will have comparisons by geography as well as by demographic characteristics (e.g., age group, gender, major payer type). Additional demographic and economic factors will be included at the ZIP-code level by linking in data on race, education, and poverty from the American Community Survey and examining correlations between demographic and socioeconomic characteristics and measure results.

An example of a project for which we performed similar linkage is the population health dashboard for Washington State (**Figure 7.4.A**). This dashboard allows users to compare ZIP-code level results from a select set of healthcare quality and cost measures, including adult access to preventive care and total cost per member per month, to socioeconomic characteristics such as the percent of the population living below the poverty line.

Figure 7.4.A. Washington State Social Determinants of Health Reporting



7.5 How will you ensure data (and its associated trends) is presented in a consumer-friendly manner? Describe and provide context for any external or internal metrics, ratios, or scales you will use.

Onpoint will include a glossary section of the website that provides definitions and context for every metric included as part of the site's content. In order to ensure that the site's content is interpretable by members of the public, all definitions will be written using language suitable for a non-technical audience, and reports will utilize industry-standard visualization methods and adhere to best practices for web accessibility as outlined below in our response to Question #7.8. Furthermore, definitions will include clear documentation of how each metric is calculated by explaining and defining the numerator and denominator (if applicable) used to derive each metric. Lastly, the site will include narrative text within each dashboard to explain and contextualize any significant trends or events that may affect the data being presented, such as the COVID-19 pandemic or the *Gobeille v. Liberty Mutual Insurance Company* decision.

7.6 What services would you recommend be provided to consumers, if any?

As part of Onpoint's public-facing website solution, we would recommend that Indiana's website provide services that allow consumers to do the following:

- View how people's health and care compare across Indiana, including being able to explore:
  - Better or poorer health (e.g., differences by region/geography)
  - Safe, quality care rankings by area
  - Health markets' quality (e.g., employer sponsored, Medicaid)
- Download and explore data sets
- Submit data requests and related information, including:
  - A data request overview (e.g., how to request data, data availability, pricing)
  - View a history of data requests
- Review a healthcare shopping page that provides links to assist consumers in being more informed and make better healthcare decisions. Onpoint would recommend links be categorized by:
  - Health insurance plan finder and marketplace calculator
  - Questions to ask your doctor, pharmacist, or surgeon
  - Questions about procedures, tests, and treatments
  - Procedure cost look-up
  - State of Indiana health resources
  - Federal agency health resources
  - Consumer advocates / help for financial, insurer disputes, and other needs
- Access support via a "contact us" link or page
  - Contact information for general APCD questions and listserv/newsletter sign-up option
- Learn about the IN APCD through summaries and supporting materials drafted in consumer-friendly language
- Read an FAQs page
- Review various methodologies related to the APCD, including information about data processes, measures development, and medical service pricing

7.7 Do you have a recommended approach for presenting the total cost of care for episodes, including out of pocket expenses?

Onpoint's Service-Focused Episodes (SFE) grouper is transparent and includes four categories of reporting: inpatient, outpatient surgery, outpatient diagnostic, and outpatient professional. Details for each category include the following:

- **Inpatient.** [redacted]

[redacted]

- **Outpatient surgery.** [redacted]
- **Outpatient diagnostic.** [redacted]
- **Outpatient professional.** [redacted]

For each of the above categories, Onpoint will calculate the total paid amount, as well as the plan paid amount and the member's out-of-pocket expenses (i.e., copay, coinsurance, deductible). Each episode is assigned to a facility based on the billing provider reported on the claim. Each episode also is associated with a member and a carrier, which allows for reporting at various stratifications.

We recommend calculating the median, 25th percentile, and 75th percentile for each facility for each service as well as similar statistics for statewide totals, carriers, and geographical regions to allow for benchmarking and comparisons by facility, carrier, and geography.

7.8 How will you ensure that the consumer website adheres to Section 508 of the Federal Rehabilitation Act of 1973 (Section 508)?

Onpoint follows industry-best practices in making pages accessible to individuals with disabilities, such as including alternative image text, following color-contrast guidelines, and allowing for keyboard navigation. Onpoint performs regular Section 508 compliance testing to ensure the accessibility of the pages within our online solutions. Indiana's website also will undergo this testing before any major release as well as annually if no major release occurs in a given year. If any pages are found to be out of compliance, changes will be made to remediate the identified accessibility issues.

8. Project Management

8.1 Complete Attachment J1 (Resource Usage Template) to provide the number of hours the Respondent expects to commit to the project and the number of hours estimated for the State resources. These amounts should be based on the functionality the State desires, included in this RFP. Any assumptions related to the number of the Respondent Project Team and the State Team staff, roles of staff, and duration of involvement used in the development of the resource hour estimates should be outlined here.

Onpoint has completed Attachment J1 ("Resource Usage Template") and has detailed the number of hours that our team anticipates committing to this project. Onpoint, along with our

subcontractors, will provide key personnel and a project team with the experience and dedication to ensure the success of Indiana's APCD. During implementation and ongoing, Onpoint will collaborate with IDOI and your stakeholders to translate IDOI's program vision and goals into concrete action items. Our proposal relies on State team resources to fully meet the requirements outlined in the RFP. Assumptions related to the number of the Onpoint project team and the State team staff, roles of staff, and duration of involvement used in the development of the resource hour estimates are outlined below.

Communication and project management. Onpoint's team of skilled personnel will oversee, track, and manage the project and will closely collaborate with IDOI and other key stakeholders to ensure the on-time execution of deliverables. Onpoint anticipates that the State Team staff will:

- Attend and actively participate in the project kick-off and ongoing project status meetings
- Assist with the scheduling and planning for any on-site meetings
- Review and approve the Project Management Plan and timelines
- Review and approve change-control processes, risk and issue logs, Communication Management Plan and schedules, and transition plans as needed
- Track and coordinate the resourcing and timely completion of Indiana staff responsibilities

Data collection and management. Onpoint will support issuers every step of the way – from onboarding through production – ensuring that complete, high-quality, and timely data is available for analytic use. Onpoint anticipates that the State team staff will:

- Support issuer onboarding by assisting with issuer outreach and communications and reviewing and approving a data submission guide (DSG) and other technical support documentation
- Enforce data collection deadlines and validation requirements
- Participate in data submission user acceptance testing (UAT) processes and system approvals prior to go-live

Onpoint also requests support from IDOI's data submitters and anticipates that data submitter staff will:

- Assign a single point of contact to coordinate submission of required data
- Respond to questions about data issues in a timely manner
- Attend onboarding webinars and training session, as needed, to promote efficient data submission processes

Data processing and validation. Onpoint will process and validate both historical and ongoing data submissions. Onpoint anticipates that the State team staff will:

- Review and provide approval regarding identified data quality findings
- Provide "go/no-go" decisions on when to move forward with quarterly data set refreshes in the event that data submitters are unable to adhere to submission deadlines
- Perform UAT upon the delivery of the quarterly data set refreshes

Data enhancement for analytics. Onpoint will provide an array of data enhancements as part of the quarterly extract delivery to IDOI and authorized data users in the Analytic Environment. Onpoint anticipates that the State team staff will:

- Attend trainings and review documentation associated with analytic enhancements contained in the State's data sets
- Review and approve configuration parameters and verify that outputs and results meet expectations for groupers, performance measures, and other third-party tools applied to the data as part of implementation UAT process

Data extraction and Analytic Environment access. Onpoint will provide role-based access to approved data sets, tools, and reporting systems through the Analytic Environment. Onpoint anticipates that the State team staff will:

- Conduct UAT upon configuration of the Analytic Environment to ensure sign-off regarding systems and applications
- Collaborate with Onpoint on the configuration of planned quarterly data set refreshes
- Identify the roles and appropriate access for IDOI's approved users

Data analytics and reporting. Onpoint will provide access to both standard and custom reports and models through Tableau and other tools in the Analytic Environment. Onpoint anticipates that the State team staff will:

- Collaborate with Onpoint's analytics team on all ad hoc report requests, including requirements, methods, and design
- For those functional requirements where IDOI's requirements stipulate that the vendor will enable Indiana staff to create or run analytics on their own, the State team would provide the staff with appropriate training or skill to take on these responsibilities once the reporting system, model, or query is built and/or training is provided by Onpoint's team
- QA analytic deliverables and provide timely feedback and acceptance of deliverables

End-user training and support. Onpoint will enhance the usability of the extracted data sets through documentation, transparency into technical processes and methodologies, and a comprehensive training and support model. Onpoint anticipates that the State team staff will:

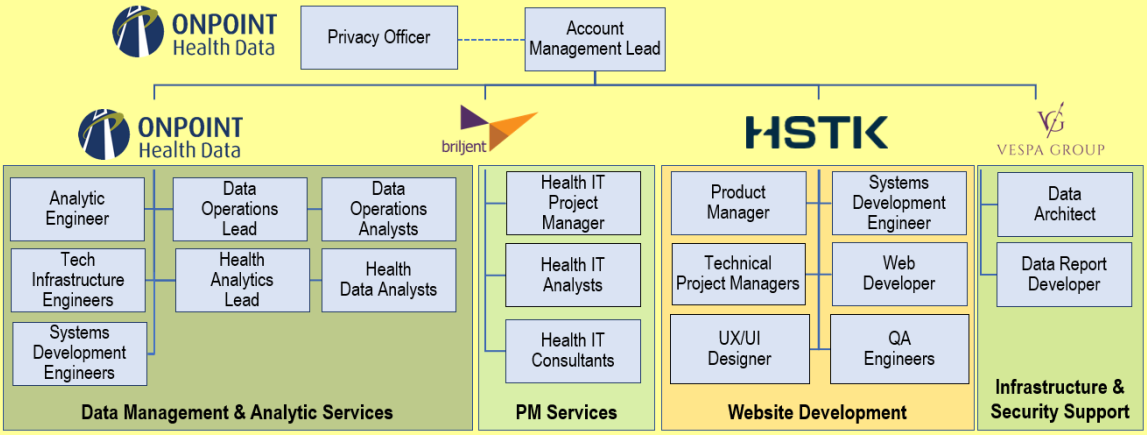
- Review and approve training plans, custom documentation, and schedules
- Attend training sessions designed for various stages of data integration, enrichment, and use to become efficient in the use of the Analytic Environment's systems, processes, tools, data products, data structures, and reporting applications
- Ensure that analytic staff are aware of the respective roles and responsibilities of IDOI's and Onpoint's team
- Assess and prioritize training and support needs on behalf of IDOI as necessary

8.2 Provide an overall project organizational chart that includes roles / responsibilities on your team as well as expected roles / responsibilities at the State to help ensure project success. This should mirror the roles outlined in Attachment J1 - Resource Usage Template.

Project Organizational Chart

Figure 8.2.A features a project organization chart encompassing staff from both Onpoint and our subcontractors that shows the reporting structure and lines of accountability across all partners.

Figure 8.2.A. Project Organization Chart



Project Roles & Responsibilities – Onpoint Team

Role	Responsibilities	Organization
Account Management Lead **Key Staff*	• Serves as primary point of contact for IDOI's Contract Administrator and other IDOI project sponsors for all project activities • Resolves issues that are escalated by project team • Oversees Onpoint's Contingency Plan and assignment of resources according to performance agreements	ONPOINT Health Data
Health IT Project Manager **Key Staff*	• Serves as primary project manager and chief liaison to IDOI • Ensures delivery and compliance of all information and project documents as outlined by IDOI • Is responsible for successfully initiating, designing, planning, controlling, executing, monitoring, and closing the project • Employs standards set by the Project Management Institute to help the project team and IDOI successfully monitor, track, and achieve project goals related to APCD planning, development, and implementation • Schedules and reports project activities, coordinates personnel resources, documents and resolves issues and risks, and manages IDOI implementation • Leads biweekly status meetings during implementation and schedules ad hoc meetings as needed • Ensures that all operational task and objectives are met on time and on budget while engaging with a wide range of stakeholders and gathering requirements and technical specifications	briljent
Technical Project Managers	• Keep the website development project on track and deliverables organized • Manage the majority of communications related to the website design and functionality and ensure that all parties remain on the same page throughout the design project	HSTK
Health IT Consultant **Key Staff*	• Is responsible for engaging with IDOI and other state agencies and stakeholders to provide subject matter expertise, recommendations • Gathers information related to the planning, solution design, governance, implementation, and delivery of APCD solutions	briljent

Privacy Officer **Key Staff*	• Is responsible for overseeing Onpoint's privacy and security program and compliance activities and serving as the regular point of contact for privacy and security matters with IDOI • Manages ongoing reviews to ensure that our solutions continue to meet all relevant federal and state data privacy and security requirements • Reviews the results of regulatory examinations, compliance reviews and audits, and third-party vulnerability assessments and penetration tests • Oversees the development and implementation of new policies and necessary standards and security enhancements	ONPOINT Health Data
Data Operations Lead **Key Staff*	• Ensures that IDOI data submission and reporting requirements are met • Manages interactions with data submitters as well as informational resources pertaining to inquiries, Onpoint CDM system configuration, and data files • Creates, documents, reconciles, and maintains logical and physical data models • Captures, integrates, and publishes descriptive metadata across the various applications • Analyzes and measures data quality levels, identifies data quality issues, and works with data stewards, users, and other IT functions to improve data quality • Establishes, manages, and monitors data aggregation and data quality procedures to ensure data integrity	ONPOINT Health Data
Data Operations Analysts	• Analyze data and underlying systems to ensure the quality of Onpoint's data and analytic deliverables • Design and implement enterprise data governance standards, guidelines, and policies (e.g., master data, metadata, reference data, data collection, data quality, data lineage) • Ensure effective management of the data collection process up to and including preparing the data for QA and extract to IDOI's data warehouse	ONPOINT Health Data
Health Analytics Lead **Key Staff*	• Leads efforts related to analyzing data for improving healthcare delivery, supporting health policy initiatives and programs, and informing healthcare transformation initiatives • Leads the development of ad hoc reports and special analyses • Serves as the go-to resource for technical questions regarding analytic approach and methodology, training, problem-solving, quality assurance review, and general technical advice • Serves as HEDIS measures subject matter expert, sharing knowledge of claims data and mapping data to HEDIS measures, including advanced analysis, design, development, and implementation of software solutions • Documents the results of queries and analysis, including their interpretations	ONPOINT Health Data
Health Data Analysts	• Work closely with Onpoint's Health Analytics Lead to review, analyze, and provide graphical and verbal presentations of healthcare data • Prepare graphical reports using PowerPoint, Excel, Tableau, and other statistical programs • Support analytic work by running Onpoint's data quality processes for extracts and other Onpoint products and reports	ONPOINT Health Data
Health IT Analysts	• Are responsible for gathering project requirements by talking to APCD stakeholders and documenting/capturing them through reports and other methods • Perform extensive research of business practices and stakeholder interviews	briljent
Analytic Engineer	• Designs, develops, tests, and implements reports and dashboards that utilize the underlying data stores, data warehouses, and data marts	ONPOINT Health Data

	• Participates in business analysis activities to gather required reporting and dashboard requirements • Translates business requirements into specifications that are used to implement the required reports and dashboards potentially created from multiple data sources • Provides support as required to ensure the availability and performance of developed reports and dashboards for both internal and external users	
QA Engineers	• Assist with building automated testing processes • Review applications at regular intervals throughout projects and report bugs, queuing them for triage	HSTK
Technical Infrastructure Engineer **Key Staff*	• Provides cross-client IT support responsibility for data integration, Analytic Environment, and reporting systems for IDOI • Facilitates the design and implementation of Onpoint's cloud-based Analytic Environment • Provides end-user support and training for the Analytic Environment and all hosted software tools • Ensures the security of the Analytic Environment and data delivery	ONPOINT Health Data
Systems Development Engineer **Key Staff*	• Serves as the team lead for Onpoint's extract and reporting systems development • Plays a key role in supporting data submitters and end users, providing expertise in extract/transform/load (ETL) and root cause analyses as part of continuous improvement efforts • Responsible for all back-end data integrations and API builds related to the public-facing website • Ensures that data flows smoothly and efficiently between the front end that users see and the back-end software	ONPOINT Health Data HSTK
Product Manager	• Serves as the primary strategist for the public-facing website solutions • Performs all up-front tasks around documenting the current challenges, diagramming the proposed solution, and providing an outline to the design and engineering resources	HSTK
Web Developer	• Responsible for the front-end coding of the web interface. This includes all HTML, CSS, and JavaScript that brings the designs to life, as well as compliance with ADA and other accessibility provisions	HSTK
UX/UI Designer	• Is responsible for understanding the user's journey and sketches out the most intuitive paths for accomplishing tasks • Is responsible for creating the final designs for engineers to build once low-fidelity wireframes are complete	HSTK
Data Architect **Key Staff*	• Translates complex business processes into technical data architecture solutions • Ensures end-user, application, system integration, and compliance requirements are met in the design, testing, deployment, and maintenance of data storage and processing systems	VESPA GROUP
Data Report Developer	• Works with end users and stakeholders to understand reporting and dashboarding requirements and translates those requirements into various analytical products and reports • Assists in designing data storage and processing solutions to meet the needs of the organization	VESPA GROUP

The following is a summary of the specific anticipated roles and responsibilities of IDOI staff. We are glad to work within the State team's available staffing resources and budget.

Project Roles & Responsibilities – State Staff (IDOI)

Role	Responsibilities
Program Manager	• Addresses all contractor questions and communications • Ensures appropriate resources are available to perform assigned tasks, attend meetings, and answer questions • Reviews and approves all design documents, SLAs, and all Onpoint plans (e.g., System Security Plan, Test Plan, Knowledge Transfer and Training Plan, UAT Plan, Maintenance & Operations Plan, Transition Plan), consulting IDOI leadership and subject matter experts as needed • Provides access to business and technical documents • Identifies and provides access to subject matter experts • Ensures that decisions are made in a timely manner and escalates risks/issues as needed
Project Manager	• Provides input into and approves project management documents (e.g., Project Management Plan, Project Schedule, Work Breakdown Structure) • Attends and actively participates in biweekly program status meetings • Coordinates IDOI resourcing for analytic and other deliverables to ensure that milestones and timelines are met • Supports the development of training sessions from a content, logistics, and attendance standpoint • Assists with coordinating submitter onboarding processes during implementation • Provides ongoing communications regarding project status, results, and risks identified by IDOI associated with their needs and the responsibilities of their project staff • Communicates updates to relevant IDOI leadership • Manages IDOI project resources to ensure that timelines are met
Senior Analyst	• Collaborates around the development of analytic requirements • Provides input around analytic design • Works with the appropriate subject matter experts and Onpoint's team to curate and maintain dashboards and standard reports • Coordinates and conducts an array of analyses and operational initiatives in support of the APCD project • Oversees the State UAT and QA processes • Provides recommendations based on areas of expertise
Junior Analyst	• Supports efforts of the Senior Analyst • Works with the appropriate subject matter experts and Onpoint's team to assist with the development of dashboards and standard reports • Coordinates and conducts an array of analyses and operational initiatives in support of the APCD project • Participates in the UAT and QA process

8.3 Provide a description of your project management approach, development methodology, process, roles, responsibilities, and tools.

Briljent will support the Onpoint team with on-the-ground project management services to benefit the entire team and provide direct support to IDOI. The Briljent Health IT Project Manager

is a professional whose sole duty is to ensure that the project is completed to the best of their team members' abilities. All Briljent project managers are PMP®-certified by the Project Management Institute and will work diligently with each stakeholder to provide clear, concise, and regular communication and ensure that milestones meet expectations.

Briljent will collaborate with the Onpoint Account Manager, who also is PMP®-certified, to deliver a plan within the flexible and robust Project Management Body of Knowledge (PMBOK®)

framework. A clearly defined and reliable project schedule and a keen focus on quality of delivery will be followed.

Project Management Approach

We will actively engage with the appropriate project team and subject matter experts (SMEs) to ensure that the delivered solution fully meets business goals and quality expectations. The Health IT Project Manager role helps establish effective processes and standards while providing the following:

- Development of project charter, including key contacts and project governance
- Annual Project Management Plan and schedule within one month following contract execution
- Identification of critical milestones and management of team activities to meet them
- Regular communication and status reporting with designated stakeholders
- Assignment and management of appropriate team resources
- Assurance that deliverables meet quality expectations for IDOI's stakeholders
  - If there are concerns regarding performance, actions will be corrected within 14 business days following notification of non-performance by IDOI
- Coordination with IDOI's technical teams and end users to ensure efficient deployment and receipt of deliverables
- Responsive change control as needs and scope evolves
- Full partnership and team effort in supporting IDOI's mission and APCD project objectives

Additionally, we will define mutually agreed-upon standard procedures and protocols to support collaboration and sustained work throughout the duration of the project. These guiding principles will be established in the project kick-off meeting and reinforced through regular communication protocols. A sample of proposed project principles follows:

- The Health IT Project Manager will be the primary contact for any project-related communications.
- All team members will maintain their contact information on the team contact list with their contact preferences.
- All members will attend required meetings and conference calls; if members are unable to attend, the meeting organizer should be notified. If a key contributor is unable to attend, a request to reschedule the meeting should be sent to the organizer.
- All project team members will have access to the Project Management Plan and project logs (in a standard document format) and will be aware of the assigned tasks and due dates.
- All project team members will proactively notify the Health IT Project Manager about tasks, duration, or dependencies that they believe are missing (or any other needed changes to the plan) and confront issues directly and promptly.
- All team members will own, follow up on, and provide updates on the assigned task, including, but not limited to, identified risks, issues, changes, approvals, and clarification

from the customer. If any delay is observed, the issue should be escalated to the Health IT Project Manager.

- All meeting minutes, key decisions, assumptions, and business rules must be documented, and all action items must be followed up and assigned to a resource by the expected completion date.

Project Management Plan Development Methodology

Collaboration is a core principle at Onpoint and extends throughout our work across teams, including clients, subcontractors, and project stakeholders. To facilitate communication among team members, Onpoint uses a suite of proven and industry-standard tools and resources – regular calls, webinar check-ins, Mavenlink, Jira, Confluence, a SharePoint-powered Collaboration Zone, and on-site meetings – all backed by our commitment to providing unmatched customer service.

Onpoint's approach to project management is designed to carefully manage both the implementation and operations phases to ensure that we meet our commitments while fostering a collaborative, nimble approach to the work. Project and schedule management will be conducted using Mavenlink, a robust project management tool that will be used to track the project schedule, including milestones, deliverables, tasks, and requested/approved changes.

Jira's ticketing functionality also will be used daily by Onpoint staff to track and manage issues and support requests and will be rolled out to IDOI and other team members to encourage transparency and engagement throughout the project. IDOI and other project team members will be credentialed to use Jira at the appropriate access level, allowing all team members to remain up to date regarding the status of requests.

The Health IT Project Manager will utilize the Schedule Performance Index (SPI) as a key project metric for status reports. The SPI describes the relationship at the project or task level between the planned schedule and the actual schedule. Project managers will review this metric to identify tasks or projects that currently are tracking ahead of or behind schedule at any given point. Used in combination with the task status, the SPI will allow the Health IT Project Manager to take corrective action to keep the project on schedule instead of managing from a reactionary position.

Project Management Process

We will adhere to the following project management phases and activities:

Phase 1: Initiation

- Project charter development
- Stakeholder identification

Phase 2: Planning

- Project Management Plan development
  - Develop project management and resource management plans
  - Plan communications
- Scope development
  - Collect requirements, plan for quality, and define the scope
  - Create the Work Breakdown Structure (WBS)

- Risk development
  - Plan risk management and identify risk
  - Perform qualitative and quantitative risk analysis
  - Plan a risk response
- Schedule development
  - Define and sequence activities
  - Estimate activity resources and durations
  - Develop the schedule

Phase 3: Execution

- Project execution
  - Direct and manage project execution
  - Assist with the quality assurance and UAT communications
  - Manage stakeholder expectations

Phase 4: Monitor & Control

- Project work
  - Monitor and control risks
  - Perform quality control measures and verify the scope
- Project performance
  - Control the schedule and costs
  - Report on performance
- Project change control
  - Monitor and control project work
  - Control the scope and perform integrated change control

Phase 5: Close

- Project close-out
  - Close project phases as appropriate

Project Management Roles & Responsibilities

The Onpoint team will work together to ensure the successful implementation and ongoing operations of Indiana's APCD, with Onpoint providing an experienced Account Management Lead to serve as an APCD subject matter expert, and with Briljent providing a PMP®-certified Health IT Project Manager. Responsibilities of the Health IT Project Manager include:

- Preparation for and attendance at the project kick-off meeting
- Manage the Project Management Plan, including risk management, quality management, resource management, scope management, and change management

- Create and update the comprehensive Project Management Plan, which includes all subsidiary plans, the tracking of project deliverables, and project progress reports
- Conduct regular partner, client, and internal team meetings
- Attend client meetings as appropriate
- Project close-out tasks
- Summarize lessons learned

Project Management Tools

The tools listed in **Table 8.3.A** will be used by Onpoint and Briljent to ensure seamless project management in the execution and management of Indiana's APCD.

Table 8.3.A. Project Management Tools

Deliverable	Tools	Project Management Plan
Tracking Deliverables (Project Kick-Off Meeting, Work Plan, Biweekly Planning Meetings)	• Mavenlink • Gantt chart • Stakeholder registry • Change request log	• Schedule and time management • Communications management
Quality Management	• Responsive and consistent reporting – Utilize issue item/change log • Lessons learned	• Quality management • Communications management
Issue & Risk Management	• Responsive and consistent status reporting • Issue log • Jira	• Risk management • Communications management
Change Management	• Change/Issue log • Jira	• Risk management • Communications management

8.4 How will you define, review, confirm, validate, elaborate, and understand the State's requirements? Include examples of requirements documents generated for similar projects. Identify and describe the tool(s) used to capture, track, and manage requirements throughout the project.

Scope Validation Session

The scope validation session is an opportunity to dive more deeply into the proposed project activities and gain agreement regarding key aspects of the proposed scope of work. Ideally, this meeting will be conducted immediately after the kick-off meeting. The outcome from this session will be a clear understanding among all participants of how the project will be conducted and managed. The resulting decisions, issues, and action items will be documented in the Project Management Plan. Topics for the scope validation session will include:

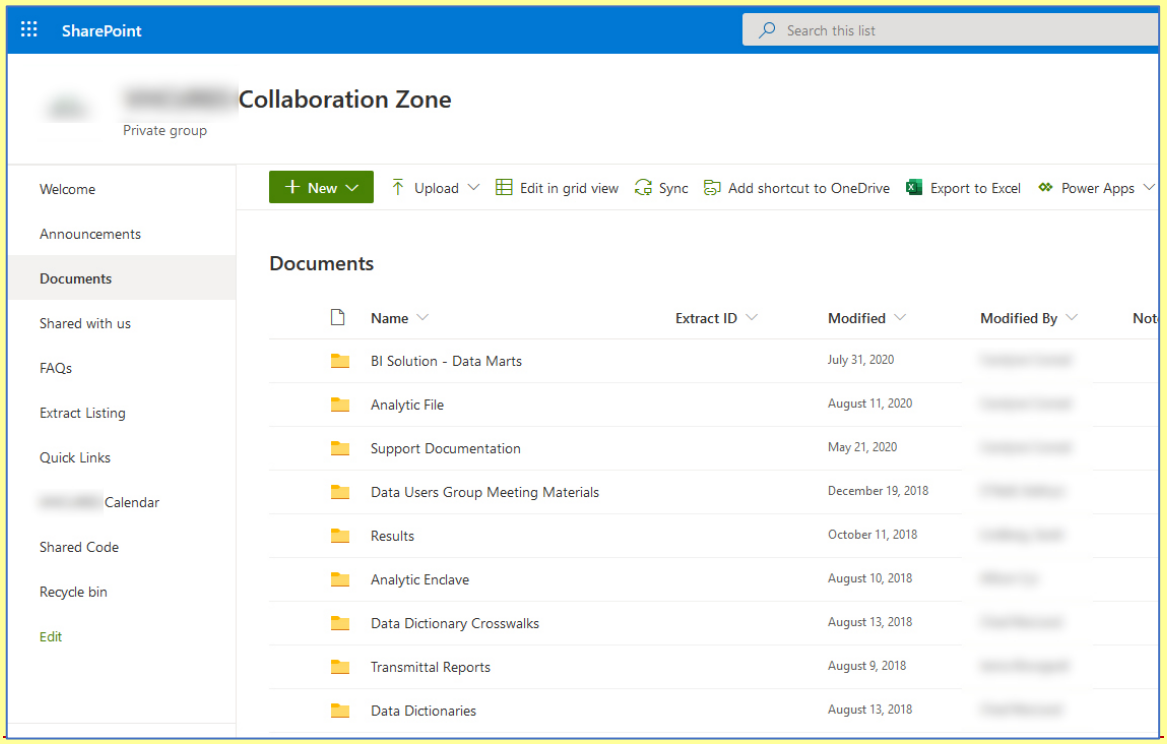
- A review of the project intent and proposed methodologies, including any suggested refinements that may be indicated based on the kick-off meeting
- Discussion and agreement on key milestones and task deadlines
- Project governance: Key decision makers, responsibility assignment matrix communications, meeting cadence, review cycles and process, and management, distribution, and version control of resource documents and output

- Identification and discussion regarding potential risks and mitigation strategies
- Identification of critical stakeholders and discussion of plans and protocols for interviews and meetings with these individuals
- Identification of all available critical documents and artifacts, such as strategic plan/vision documents, policies and procedures, system and/or data architecture documents, and other relevant material

All project management artifacts, including agendas, meeting notes, and biweekly and ad hoc progress reports will be maintained for always-available reference using the SharePoint-based Collaboration Zone. The Collaboration Zone provides a centralized online hub for sharing documents, notes, findings, FAQs, and more (**Figure 8.4.A**). Using SharePoint, the project team can share reports, provide updated documentation, and archive project status updates and schedule timelines. Action items will be specified, with the accountable party and a target completion date for each.

The SharePoint site also can be leveraged as a convenient storage location for ready access to the project's documentation deliverables, including the Communication Management Plan, Organizational Change Management Plan, Schedule Management Plan, Resource Management Plan, Scope Change Management Plan, Configuration Management Plan, Issue Management Plan, Risk Management Plan, and Quality Management Plan. Additionally, the Collaboration Zone's resources can be partitioned using role-based access, providing IDOI with access to these contract-related documents without releasing them to all parties (e.g., analysts and data users) that may be credentialed to access the Collaboration Zone.

Figure 8.4.A. SharePoint Example (Blinded)



Stakeholder Engagement Process

Our discovery process involves gathering sufficient information to ensure that our team has a thorough and comprehensive view of IDOI's information, data, practices, and needs. We recognize the importance of minimizing disruption for busy state staff and leaders so, whenever possible, we will begin with independent research, using existing documentation that is publicly available online.

In addition to this independent research, our stakeholder engagement and outreach process can include a combination of the following information gathering methods in collaboration with IDOI:

- Existing business process and technology documentation provided by IDOI and other state agencies
- Stakeholder focus groups
- Individual stakeholder interviews (for a deeper dive into information)
- Online surveys (to gather feedback on state agency data needs)

Through this discovery and research phase, we will capture high-level user stories and data requirements. We will document the user experience with a focus on the monetary, time, and opportunity costs of the APCD platform and process configurations. We anticipate that these user stories will be done by user type to demonstrate utilizing workflows for each end-user role. We will work with IDOI to identify critical user types and the number of stories for each. A plan for high-level user stories (**Table 8.4.A**) and an example user story (**Table 8.4.B**) can be found below.

Table 8.4.A. Plan for High-Level User Stories

Plan for High-Level User Stories	
Step 1	Identify the impacted users (e.g., data analyst, executive, administrator) and understand processes and potential pain points
Step 2	Define the optimal workflow to achieve the user's goals
Step 3	Document the value that this process will bring to the users (both direct and indirect) and the overall system or process
Step 4	Define success criteria and suggested implementation strategy

Table 8.4.B. Example User Story

Title	Determine the number of submitters with outstanding submissions after the monthly due date
User Story	As a compliance officer, I want to know how many submitters have successfully submitted data to the APCD.
Acceptance Criteria	Given that I am logged into the application successfully as a credentialed user, I can generate a report and filter dashboards to provide information on successful submissions to IDOI.

Jira also will be used by the Onpoint team to track and manage issues, tasks, and projects internally and will be rolled out to allow external support for the Indiana APCD. We will use Jira to develop tasks and subtasks for the APCD's business requirements, assign and hand off tasks to team members for execution, and monitor and prioritize the status of each. IDOI team members will be credentialed to use Jira at the appropriate access level, ensuring that the full team remains on the same page regarding status, progress, and next steps.

Onpoint's team will collaborate with IDOI to ensure that requirements for all project deliverables are gathered and documented clearly in standard requirement templates. **Figure 8.4.B** and **Figure 8.4.C** offer examples of requirements documents utilized in similar APCD projects.

Figure 8.4.B. Sample Requirements Document – Communication Management Plan Deliverable

3.1 Deliverable Requirements & Acceptance Criteria

List specific requirements for the deliverable and acceptance criteria for those requirements, including critical success factors, required artifacts or documents, quality measures, content metrics, and/or adherence to standards.

Requirement	Acceptance Criteria
1. Identification of the Onpoint team responsible for maintaining regular and ongoing communications with the client, APCD submitters, and other stakeholders	A. Communication Plan includes: i. Organizational chart of Onpoint's project team ii. Table of key project staff, a description of their role, and email and telephone contact information
2. Concise description of the types of project communications, their frequency, and communication method(s)	A. Communication Plan includes communication types, frequency, and methods for the anticipated communication types outlined in Section 2: i. Project Management ii. Submitter Support iii. End-User Support iv. Master Index Module Vendor
3. Concise description of where project information will be stored and organized to ensure accessibility	A. To ensure transparent and collaborative communication, we will use the following resources: i. Client-hosted SharePoint site ii. Onpoint-hosted Jira
4. Concise description of how Onpoint will work with the client to convey data quality status and improvement plans to submitters, the client, and other stakeholders (e.g., data users).	A. The Communication Plan will describe ongoing data status reporting using the following resources: i. Onpoint CDM's dashboards ii. Variance review and monitoring iii. Annual DSG review
5. Concise description of how Onpoint will maintain the Communication Plan.	A. The Communication Plan will include the frequency and approach for maintaining the Plan.

Figure 8.4.C. Sample Requirements Document – Onpoint CDM Submitter Registration

3.1 Deliverable Requirements & Acceptance Criteria

List specific requirements for the deliverable and acceptance criteria for those requirements, including critical success factors, required artifacts or documents, quality measures, content metrics, and/or adherence to standards.

Requirement	Acceptance Criteria
1. Identifying and corresponding with mandatory and voluntary plans and submitters to begin onboarding and provide orientation to the Portal's registration module	A. Notification to potential plans and data submitters identified by the client of prospective participation in the APCD B. Notification to potential plans and data submitters identified by the client of upcoming training webinar(s) C. Tracking activities related to identified potential data submitters and outreach dates D. Developing and maintaining a schedule of registration-related communications with plans and submitters
2. Providing plans and submitters with documentation and training regarding how to use the Portal's registration module	A. Delivery of documentation regarding the Portal's registration module B. Hosting of webinar(s) for plans and submitters to set registration expectations and provide an overview of the registration process C. Upload training recordings to the Documentation section of the Onpoint CDM portal for new staff or plans and submitters unable to attend the scheduled webinar D. Establishment of a support email address for the client's APCD submitters and telephone number, including agreements on response times E. Schedule an annual registration review meeting with the client to address status and any proposed changes F. Maintain and update these resources at least annually, as needed
3. Configuring and launching the portal's registration module, enabling plans and submitters to register on an ongoing basis	A. Collaborative development and finalization of a registration module requirements document that includes the following: i. The specific registration information fields that will be collected ii. The timeline for entities to complete their registration(s) iii. The timeline for review and approval of plan and submitter registrations iv. The roles and responsibilities of both Onpoint and the client for the following activities: a. Reviewing, verifying, and establishing contact with the initial list of plans and submitters expected to participate in the APCD program b. Reviewing and verifying plan and submitter registrations and relationships B. Documentation of all registration requirements, including client review and approval C. Configuration and testing of the registration module in alignment with the registration module's requirements document D. Documentation of the Onpoint registration module Test Plan E. Facilitation of a UAT period for the client to review and confirm that the registration module meets the requirements outlined in the registration module's requirements document F. Closure of any issues identified during UAT G. Launch of the portal's registration module

8.5 How will you conduct solution design planning and associated communication to the State? Provide example design documents generated for similar projects. Provide an example of the communication plan for this project to include roles responsibilities, communication types, methods of delivery, audiences to receive, timing, etc. How will your company monitor and confirm communications are working and adjust as needed?

Solution Design Planning

A key responsibility for Onpoint's team will be communication across the many stakeholders participating in Indiana's APCD program – IDOI, stakeholders, data submitters, Analytic Environment users, and others – to ensure clarity in project direction, responsibilities and tasks, dependencies, timelines, progress, issues, and actions items. At all times, IDOI and the APCD's data submitters, as well as IDOI contractors and stakeholders, will have ready access to all key personnel on the Onpoint team, including the Account Manager and the Health IT Project Manager. In addition to these key personnel, Onpoint's deep bench of support staff from our operations, IT, engineering, and analytics departments will be on hand to provide assistance and engagement whenever needed. Onpoint will use the requirements identified through stakeholder engagement activities to conduct solution design planning.

Communication Management Planning & Management

Our approach to communication management planning and management promotes collaboration between all team members and works to keep all project team members informed of key accomplishments, issues, risks, action items, decisions, and accomplishments. Communication is accomplished through a combination of meetings, reports, documentation libraries, emails, and interviews. As part of our team's day-to-day communications responsibilities, we will:

- Communicate and work directly with the IDOI project leads and key staff
- Attend project management meetings and share/disseminate meeting outcomes with the appropriate stakeholders
- Establish and confirm internal department processes and procedures
- Ensure that internal department policies, processes, and procedures are followed
- Provide leadership, support, direction, and assistance to team members
- Resolve issues and address concerns
- Review and approve all training materials and provide feedback
- Track and expedite issues and concerns
- Communicate project status and impacts

Communications are most effective when they are consistent and targeted. Our team will work closely with the IDOI project sponsors to ensure that communications are developed with specific stakeholder groups in mind and targeted to the appropriate group using the most effective methods. Our team will manage and update the various communication vehicles that will be identified in the Communication Management Plan and will ensure that all communications are approved by IDOI.

The Communication Management Plan will include the following:

- Identification of critical audiences and their needs, including preferred frequency and methods of communication
- Key information about scope changes
- Recommended timing and sequence for communication activities
- Recommended communication formats and templates
- Talking points for leaders

Once all stakeholders have been identified and communication requirements are established, the Onpoint project management team will maintain this information in the project's Stakeholder Register and use this in coordination with the project communication matrix as the basis for all communications. Communication strategies will be reviewed regularly to ensure that our team is able to understand what is working well and learn what works, what does not work, and for whom. When performing evaluations of project communication activities, we will evaluate and report on questions such as:

- Did communications go out on time and to the correct audiences?
- Were clear objectives identified before meetings to ensure project goals are supported?
- Did we identify audience-focused key messages in our communications?
- Did we identify achievable action items during meetings?
- Did we define success in clear, measurable ways?

The Communication Management Plan will be reviewed and updated as necessary on an annual basis. Please see **Figure 8.5.A** for an example Communication Management Plan.

Figure 8.5.A. Example Communication Management Plan

REVISED 2.15.2022

	Activity/ Document	Participants	Purpose/Description	Process/Format	Lead	Frequency
1	Project Management Plan (PMP)	Project Team	• Detailed project and quality management methodology and oversight • Detailed description of steps to accomplish each task	• Draft due after 30 days per agreement with IDOI • Update draft PMP based on IDOI feedback; final PMP submitted to IDOI for final approval	Project Management (PM) Team	• Draft • Revise and resubmit Final PMP • Annual updates
2	Project Timeline	IDOI	• Detailed schedule • Tasks and timelines for completion of each deliverable per contract requirements	• Current project schedule to be included in all PMP versions	PM Team	• Updated with each PMP iteration • Updated upon any approved change requests
3	Task Deliverables	IDOI	• Detailed description of each deliverable provided in deliverable outline, if needed • Detailed steps, timelines, and responsible Onpoint staff/subcontractors for review and approval of each deliverable within the scheduled timeline • Draft and final deliverables due to IDOI for review and feedback	• To be reviewed and approved by PM Team • IDOI and Project Officer to provide feedback and/or approval on draft and final deliverables	Onpoint Team Task Leads with input and oversight from PM Team	• First review: allow 10 business days for IDOI response • If a second review is needed: allow 5 business days for IDOI response
4	Biweekly Status Calls	IDOI Project Officer and Onpoint Team	• Document progress on project deliverable schedule, outstanding issues, accomplishments, risks, change management, and action items	• Inputs include project schedule, team status reports, and active PM updates • Discuss, address, and remove barriers necessary for project success • Review and track previous and future action items • Complete meeting summary notes and submit to IDOI	PM Team	• Biweekly meetings (1-hour duration)
5	Task Communication	IDOI	• Process for IDOI to contact appropriate Onpoint Team members regarding a specific task	• Use the email distribution list assigned to the specific task • Email subject header should include the task number and title of the work	IDOI Team	• As needed
6	Branding	IDOI	• Standard format to be used when creating a product (applies to reports, presentations, memos, minutes, etc.)	• Use IDOI logo and name • Use standard Microsoft Office templates for uniform look on all deliverables	Onpoint Team Task Leads	• As needed
7	Stakeholder Events	IDOI	• Standard format for conducting a speaking engagement	• Team member will introduce themself as a member of APCD Project Team working on behalf of IDOI	Onpoint Team SME Lead	• As needed
8	Communication with IDOI Partners, Community Members, and Other Agencies	Onpoint Team	• Formal email communication	• Identify self as part of APCD Project Team • Copy IDOI Program Manager • Copy the PM Team on all communication with IDOI and partners/states to assist with task monitoring and completion of action items • Email subject header should include the task number and title of the work	Onpoint Team SME Leads	• As needed
9	Communication with IDOI	Onpoint Team	• Formal email communication to IDOI Project Officer and APCD Project Team members regarding task status	• Respond to IDOI's email to acknowledge receipt of email as soon as possible, no later than 24 hours after email has been received from IDOI • If unable to provide a complete answer immediately, alert IDOI of a timeline of when to expect a complete response or ask any questions that may be needed before a complete response can be provided • Copy PM Team on all communication with IDOI, as it is critical to monitor action items and task progress for auditing purposes, and for awareness of information provided to IDOI • Email subject header should include the task number and title of the work	Onpoint Team SME Leads	• As needed
10	Internal Biweekly Meetings	Onpoint Team	• Review and management of project activities within PMP and schedule parameters • Resolution of issues, mitigation of risks, and modification of processes and/or procedures	• Meeting focuses on review and management of project status and anticipating actions to address tasks to be undertaken or completed • Includes task leads from each firm • Provide direction on resources and scheduling • Review and track action items	Onpoint and Subcontractor Leads	• Biweekly meetings (1-hour duration)

	Activity/ Document	Participants	Purpose/Description	Process/Format	Lead	Frequency
11	Internal Review: Deliverable Expectations	Onpoint Team	• Team write-up and discussions on deliverables and IDOI's expectations • Determination of plan and process for completion prior to development	• Onpoint Team lead responsible for the deliverable prepares the Deliverable Expectation Document (DED) (i.e., a short [max. half-page] document presenting the expectations for preparation and goals for the deliverable) • Onpoint Team lead responsible for the deliverable presents the DED to the PM Team for approval; sets up a conference call (if needed) with the PM Team to discuss the DED • PM Team approves DED and development commences	PM Team	• As needed for each deliverable • PM Team to review DED in up to 10 business days (includes call time if needed)

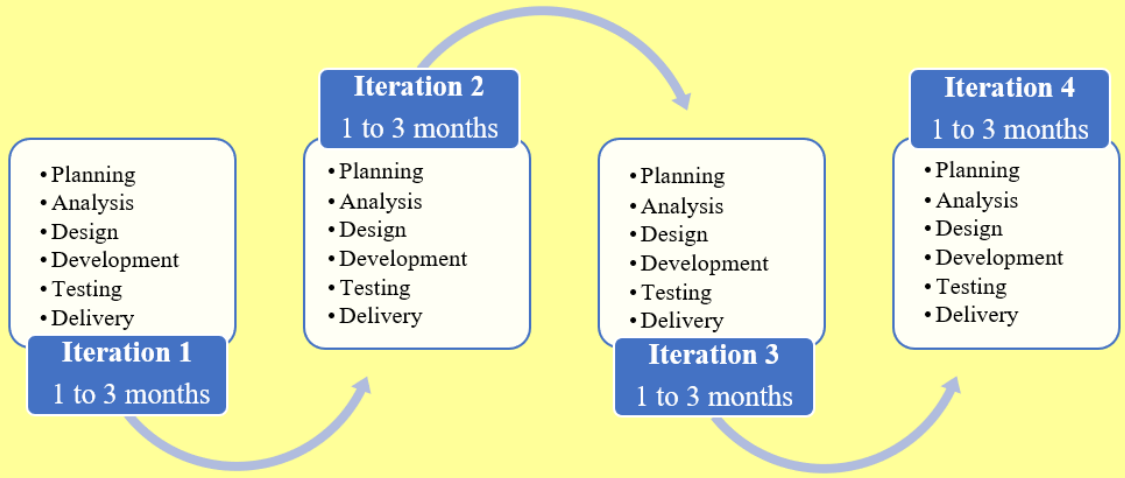
12	Internal Review: Task Deliverables and Materials	Onpoint Team	• Process to create and finalize APCD deliverables before IDOI submission	• Internal APCD discussion and review of outline
				• Onpoint Team lead does the following:
				  ◦ Creates material or deliverable
				  ◦ Sends material to firm lead for review and approval
				  ◦ Once in final format, sends to the Technical Lead for QA check
				• Onpoint Team lead completes final editing after PM Team approval
				• PM Team submits deliverable to IDOI to streamline communication
					Onpoint and Subcontractor Leads	• As needed for each round of review of the material
						• Team will allow 5 business days for each PM Team review of materials

8.6 What key activities, deliverables, and milestones will be necessary to complete the required tasks? What is your proposed iteration cycle in terms of time and areas of focus?

Onpoint envisions a Project Management Plan that is updated regularly as needs change and that contains the tactical objectives and timeline to successfully guide the project's implementation. Onpoint will develop and deliver a comprehensive draft of the Project Management Plan no later than thirty (30) days following contract execution and will begin implementation following IDOI approval. We have included a draft Work Plan below in our response to Question #8.10 (**Table 8.10.A**) to illustrate the key activities, deliverables, and milestones that we anticipate will be involved in both the implementation and ongoing production phases. Major project milestones also are noted, and high-risk tasks are identified and accompanied by a brief mitigation strategy for each.

During the project implementation stage Onpoint will frequently request feedback to help the team understand IDOI's and other stakeholders' expectations in areas where requirements are not already clearly defined and where scope will need to be managed based on continuous, collaborative learning. We will regularly refine our Project Management Plan, scope documents, and product specifics base on these learnings. During each project iteration cycle, we will execute planning, analysis, design, development, and testing phases, and will then deliver results at the end of the defined iteration cycle. We anticipate that the Indiana APCD implementation planned by IDOI for this project will have three-month iteration cycles to ensure that IDOI has ample opportunity to provide valuable input. See **Figure 8.6.A**, below, for an example of Onpoint's approach to project iteration cycles.

Figure 8.6.A. Project Iteration Cycles



8.7 What critical dependencies and key risk factors are associated with the proposed solution and how do you plan to mitigate those risk factors?

Describe your risk / issue management processes.

Identify and describe any tools that are used to help manage risks / issues.

Identify some of the key risks / issues / barriers you have faced on projects of similar scope, size, and complexity. What mitigation / contingencies were put in place for those risks?

How have you used governance to resolve risks / issues / barriers?

Throughout the project, team meetings and status updates will offer multiple checkpoints for providing input and any necessary approvals. The Health IT Project Manager and daily point of contact for the APCD will provide monthly and ad hoc project status reports that will include updates regarding all of the items specified by IDOI, including work accomplished since the previous report, current and upcoming tasks, risks and issues as well as their mitigation plans, and future milestones and their anticipated completion dates. This is our standard approach and will ensure that communications remain open, team members and goals have clear direction, and project status is fully transparent.

Risk/Issue Management Processes & Tools

All issues and risks will be proactively identified and documented in the Issue Management Plan and Risk Management Plan. Potential risks to the project will be managed by the Health IT Project Manager by identifying, assessing, documenting, and monitoring events identified as risks. Risks will be identified and documented in a risk register at the beginning of the project. Throughout the project life cycle, new risks will be added to the risk register as they arise.

As new risks are identified, the information will be communicated by the Health IT Project Manager to IDOI, and a risk assessment will be completed. Each risk will be assessed for severity and likelihood of occurrence. Risk mitigation strategies will then be prepared for each risk, including communication to stakeholders as needed (**Table 8.7.A**).

Table 8.7.A. Example Risk Assessment Grades

Risk Aspect	High	Medium	Low
Severity	Major impact to schedule and/or budget	Moderate impact to schedule and/or budget	Minor impact to schedule and/or budget
Likelihood	71% – 100%	36% – 70%	1% – 35%

The Health IT Project Manager will lead the team in developing responses to each identified risk. In the event that risks are identified, they will be qualified, and the team will develop avoidance and mitigation strategies. The Health IT Project Manager, with the assistance of the team, will determine the best way to respond to each risk to ensure compliance with these constraints (**Table 8.7.B**).

Table 8.7.B. Risk Mitigation Strategies

Risk Grade	Mitigation Strategy
High	Mitigation actions need to be identified and implemented to reduce the likelihood and/or seriousness of the risk.
Medium	Mitigation actions need to be identified and planned for possible future action.
Low	Risk is to be monitored for changes in grading over time. No immediate action is required.

Onpoint's team will use the following tools to help manage risks and issues:

- **Biweekly project status meetings.** IDOI will be kept apprised of all data quality deficiencies as part of the biweekly project status meetings and updates. These communications will include a description of the deficiency, its impact, potential resolution, and projected timing for resolution. If a data deficiency cannot be remediated prior to the kick-off of the quarterly extract cycle, IDOI will want to determine rules regarding whether and how to proceed**.**
- **Jira.** Jira is used daily by Onpoint staff to track and manage issues, tasks, and projects internally and will be rolled out to allow external support for the Indiana APCD. We will use Jira to develop tasks and subtasks for the APCD's business requirements, assign and hand off tasks to team members for execution, and monitor and prioritize the status of each. IDOI team members will be credentialed to use Jira at the appropriate access level, ensuring that the full team remains on the same page regarding status, progress, and next steps.
- **Release notes.** Release notes that also function as transmittal reports are part of the documentation package that accompanies every extract deliverable. Release notes include details regarding the nature, timing, scope, impact, and remediation plan for identified data quality issues or deficiencies. A change log updated with each subsequent data release as issues are resolved and remediation completed.
- **Support documentation.** For data quality deficiencies that result in changes to logic for transformations or downstream value-adds, Onpoint provides detailed documentation regarding the update so that end users can understand the change and anticipate any impacts or advantages for their specific use cases.
- **Onpoint CDM notifications.** Updates to data quality validations and thresholds are communicated through the portal notification stream as well as through email communications directly to submitters.

- **User group meetings and webinars.** During regularly scheduled data user group meetings and webinars, information is provided regarding updates, enhancements, and workarounds for data quality issues or deficiencies. These webinars also will be used to invite and collect feedback from users on their suggestions for enhancements to data conversion, processing, extract creation, and documentation.

Risks, Issues, & Barriers to Management on Similar Projects

Onpoint recognizes that there can be technical risks associated with implementing a new APCD, several of which we have detailed below. Our team will develop a thorough strategy to mitigate risk wherever necessary during implementation – from preparations prior to kick-off to system quality assurance checks after implementation concludes. Our experience implementing APCDs in numerous states will allow us to anticipate and plan for potential risks and effective mitigation strategies associated with a transition. Onpoint will review our implementation experience with IDOI along with our recommendations based on that experience.

Table 8.7.C provides a description of several potential risks and that corresponding mitigation strategies our team would employ. These risks and mitigation strategies are based on our experience working on similar projects with other state APCDs. Our lessons learned will limit any risks and will result in efficient resolution if/when risks occur.

Table 8.7.C Potential Risks & Mitigations

Risks	Mitigation Strategy
Limitation of state resource availability	Traditionally, APCD projects pull significantly on government resources. We are committed to the opposite. Our team recognizes that there is significant information available for the project. We are prepared to effectively manage and organize this information through planned onboarding and independent research, rather than by consuming valuable state staff time through lengthy interviews and surveys.
Technical challenges faced by submitters delay the APCD project	Minimizing barriers for health plans to submit claims to the APCD is critical to ensuring that data is received on a timely basis and is of the highest quality. There are many factors to consider, including the following: • One of the largest barriers to effective use of APCDs for informing policy are data submission delays. Our APCD solution, Onpoint CDM (Claims Data Manager), was created through collaboration with payers nationwide, resulting in a user-friendly interface that reduces lag time for data submissions through a payer-optimized workflow. Onpoint CDM is an industry-leading tool that facilitates secure submission uploads, cleanses, and standardizes incoming data, performs rigorous quality review, and then aggregates, consolidates, and enhances the data to support analytics. Each of these steps should be assessed for prospective vendors. • Accompanying Onpoint CDM's intuitive interface is the support from Onpoint's staff. Onpoint's Data Operations team supports payers by removing submission barriers through diligently efforts to promote collaborative and results-oriented relationships with payers. Examples of the value of dedicated Data Operations members is highlighted in the onboarding process, which can be especially intensive during start-up. Our Operations team helps ensure that payers feel supported, informed, and invested by providing regular all-payer calls and webinars, email updates with helpful tips, notices detailing any upcoming system or rule changes that may impact payers, one-on-one solution sessions, and open office hours. Our dedicated Operations staff also is available to address emails, phone calls, and questions anytime they arise. • Data layouts are always a consideration when working to minimize technical challenges for payers. We have found that one of the most important considerations when implementing an APCD's layouts is providing the critical support for payers via accessible staff and detailed documentation that contains clear definitions, mappings, and expectations for each file being provided to the APCD.

	• Providing industry-standard tools and different options for data submissions is also a way to minimize the barriers of submitting data to the APCD. Onpoint supports data transmissions via SFTP with PGP encryption as well as via a secure drag-and-drop utility within Onpoint CDM's secure online portal. We have found that most payers prefer to submit data using SFTP since this allows for the automation of data submissions, a streamlining of the process, and more timely submissions. Supporting the multiple ways in which payers store and report claims adjustments to APCDs is also a critical consideration. Based on the variation in payers' approaches that our team has encountered across the country, our data integration solution, Onpoint CDM, currently includes more than 30 consolidation methodologies that reconcile and resolve original claims and their subsequent adjustments to report and deliver a final claim to end users. Included in our library of methodologies are standard versioning and aggregation methodologies as well as customized, payer-specific methodologies. This enables payers to easily report claim adjustments as stored in their warehouse rather than shoehorn adjustments into a one-size-fits-all solution that may not accurately reflect their claims.
Change in stakeholder support	We understand that the APCD landscape can be complex, political, and sometimes contentious with ever-changing stakeholder demands. We also understand the importance of the roles that stakeholders play in sustaining and supporting such initiatives. For this reason, our team will emphasize stakeholder coordination and engagement to ensure a unified vision for future initiatives that aligns across government and non-government stakeholders.
Alignment with federal guidance and funding opportunities	Briljent specializes in the alignment of federal requirements through their experience working with federal HHS and has experience securing more than $1 billion nationwide to support various state health information technology initiatives. Briljent will evaluate alignment throughout each task and ensure that IDOI can maximize future federal funding availability.
End users lacking trust in APCD reporting	Onpoint has successfully fostered collaborative relationships with end-user communities across our client base, including researchers, policymakers, payers, and providers. We have a proven, transparent, and tailored approach to training and support, which is foundational to building users' understanding of and trust in any complex data resource, including the Indiana APCD. We will be readily available to the APCD's user community, offering one-on-one support and ongoing user group training as needed to recipients of the data sets.

Governance to Resolve Risks, Issues, & Barriers

During implementation of an APCD, the ability to provide clear expectations for compliance as well as penalties for non-compliance, decreases risk of a lengthy implementation period as well as reduces late and incomplete submissions. Onpoint will collaborate with IDOI to provide recommendations regarding compliance-related regulations that have removed barriers for submitters to provide timely and complete data sets, including:

- Expected turnaround for validation questions to submitters
- Penalties for non-compliance
- Clear requirements around submission of information critical to insuring the APCD can produce consistent and meaningful reporting

8.8 What is your scope management strategy / processes to include capturing, costing, prioritizing, and approving potential scope changes?

Scope Management Strategies

Our scope management strategies include:

- Defining and confirming scope through the scope validation session
- Creating and updating the Project Charter document
- Collecting and tracking project requirements
- Developing and maintaining a Work Breakdown Structure (WBS)
- Creation and approval of a Quality Management Plan, Risk Management Plan, Resource Management Plan, Communications Management Plan, and Stakeholder Management Plan to ensure that all parties are in alignment
- Holding frequent client meetings to ensure scope alignment and discuss change orders
- Tracking and logging risks to be prepared for any scope complications

Scope Change Process

All change requestors will input their change requests to the Health IT Project Manager in writing. The Health IT Project Manager will triage the requests and enter each one into the designated project management tool for tracking and reporting. During the project kick-off phase, the Onpoint and IDOI teams will mutually decide on the stakeholders that will comprise a Change Control Board (CCB). The CCB review process will be built into the existing meeting structure.

Any change request items will be reported in the status report. The report will provide a high-level description, the status, and the responsible party. The Health IT Project Manager will review each request for completeness, risk, need, and impact. Incomplete requests will be routed back to the requestor for additional input. Requests that are deemed unnecessary will be rejected and the requestor notified.

Requests that are approved will be marked as "Team Approved" and routed to the appropriate stakeholders responsible for implementing the change. The following request designations will be used for routing purposes and will be the responsibility of the Health IT Project Manager:

- **Team Approved.** All requests in "Team Approved" status will be reviewed each week, and appropriate follow-up steps will be taken. "Team Approved" status items will be set to "Scheduled" status when they have been acted upon or will have the request process changed back to "In Review" if IDIO APCD project leads raise objections. The latter will then be placed back in the process for evaluation at the next meeting, with the objections noted.
- **Success.** Scheduled change requests will be updated by the Health IT Project Manager, who will coordinate with the stakeholder making the change on the scheduled implementation date with the status of "Successful," "Partially Successful," or "Unsuccessful." "Successful" and "Partially Successful" requests will be automatically closed by the system. "Unsuccessful" requests will be routed back to the next biweekly meeting for appropriate action. The assigned stakeholder will be responsible for follow-up on "Partially Successful" requests and for submitting a new request as appropriate for incomplete or unsuccessful tasks.

8.9 To what extent do you expect your team members to be on-site at the IDOI or off-site at your facility?

Onpoint's team is committed to building a strong partnership with IDOI, and our proposed staffing and budget will allow the level of nimble, hands-on support and attention that the APCD initiative requires. We are prepared to meet the service-level agreements that are established, achieve deliverables and milestones in compliance with the Work Plan and schedule, provide rapid responses to any time-sensitive requests, and deliver in-person support on site in Indiana on a frequent basis.

Based on our most recent experience implementing state-mandated APCD systems, we plan to have staff on site for all key meetings (e.g., stakeholder, requirements gathering, training, and strategy focused) and during planning-intensive periods. During implementation, we plan to be on site at least monthly, pending IDOI interest, with flexibility to increase or decrease the frequency of in-person meetings at IDOI's preference. Additionally, the presence of our subcontractors in the state of Indiana will make ad hoc, on site meetings easily accommodatable. Briljent's experienced project management team will function as an "on-the-ground conduit" with IDOI and stakeholders, creating project reports and support documents, following up on the action items, and tracking next steps, key questions, and issues while working as an integrated part of the Onpoint account management team.

8.10 Describe your company's implementation strategy (Pilot, phased rollout, "big bang", etc.)

Provide a preliminary implementation work plan that outlines all key steps for plan implementation, responsibilities, and expected timeframes based on the effective date. Clearly indicate the proposed implementation commencement date in anticipation of a Contract effective date no later than 10/1/2022.

Provide an example of an implementation checklist for this project that defines and describes the detailed steps required and the associated owners for those steps as part of the go-live activities.

Provide an example of a back out strategy / plan if issues are encountered with the new application post-production. Include roles / responsibilities for both your company and the State.

Implementation Strategy Overview

Onpoint envisions a phased rollout of Indiana's APCD. The first phase will be focused on data intake – building consensus around data layouts, definitions, and thresholds, registering and onboarding data submitters, and standing up our Onpoint CDM platform for data intake. The second phase will be focused on data extract delivery, analytics, and standing up our Analytic Environment for end users. The final phase will be focused on designing and deploying the public-facing website and reporting for the Indiana APCD. While we view these three phases as distinct, our Project Management Plan and timeline include overlap between phases to ensure that the APCD is live and providing value to Hoosiers in a timely manner.

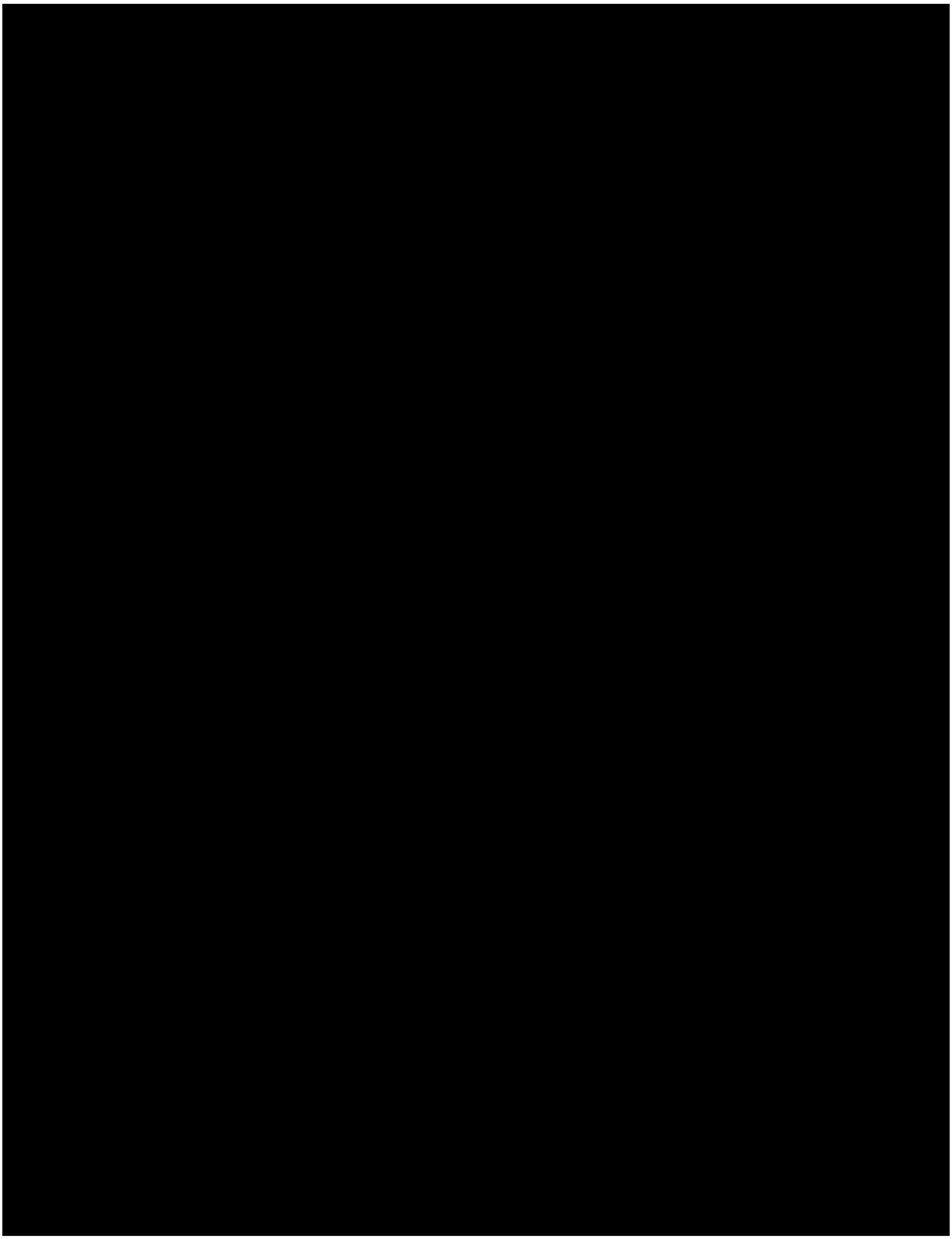
Preliminary Implementation Work Plan

Onpoint's proposed preliminary implementation Work Plan can be found below in **Table 8.10.A**. Our Work Plan is based on an implementation start date of August 1, 2022, and illustrates the key tasks, dependencies, and timeline that we anticipate would comprise implementation. Major project milestones also are noted, and high-risk tasks are identified and accompanied by a brief mitigation strategy for each. As part of our Work Plan, we have allocated three (3) months to

configure and deploy Onpoint's data submission portal, allowing for submitters to begin testing their file submissions four months after project kick-off. We understand that this may be more rapid than the contract solicitation's timeline, and our accelerated timeline can be adjusted based on the interests of the State and your submitters.

Table 8.10.A. Work Plan

REVISED 2.15.2022



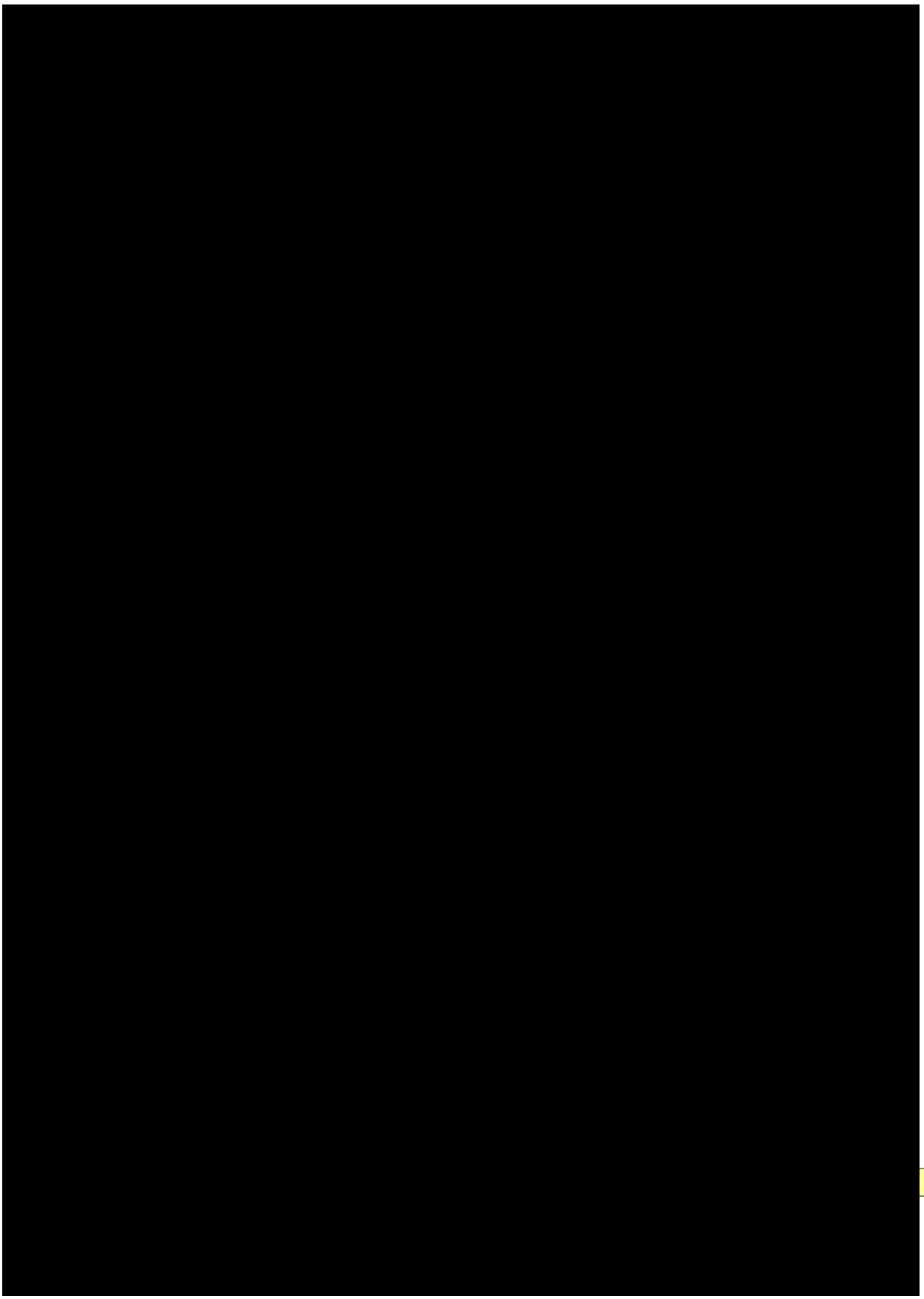
[redacted]

Implementation checklist example. Onpoint has provided an example implementation checklist below in **Table 8.10.B** that defines and describes the detailed steps required and the associated owners for those steps as part of Onpoint's proposed go-live activities.

Table 8.10.B. Implementation Checklist

[redacted]

REVISED 2.15.2022



Back-out Strategy Plan

Onpoint's proposed solution for Indiana's APCD includes time-tested and reliable applications that we have implemented in many other states and that have been in continuous operation for nearly two decades. While we do not anticipate any issues with our applications post-production, we will ensure that, throughout the project, team meetings and status updates will offer multiple checkpoints for providing input and any necessary approvals to mitigate risk. Our Health IT Project Manager and daily point of contact for the APCD will provide monthly and ad hoc project status reports that will include updates regarding all of the items specified by the State, including work accomplished since the previous report, current and upcoming tasks, risks/issues as well as their mitigation plans, and future milestones and their anticipated completion dates.

If any post-production issues should arise for data submitters, Onpoint CDM logs communication with our clients' data submitters, documenting our outreach and response efforts so that communication and compliance are readily monitored. IDOI will have access to this outreach information whenever needed. All submitters are encouraged to report issues and ask questions via Onpoint's Support Desk, which automatically creates a support ticket for tracking from start to resolution and allows for transparency in communications. Ticket creation automatically alerts the Operations team to the registered issue, triaging the ticket to the appropriate resources for resolution. If major issues are reported, Onpoint CDM would be restored to the previous release version.

Users provisioned with an Analytic Environment account will be provided with hands-on support and training by Onpoint's technical staff to ensure that they are able to securely and efficiently access the data sets and tools provisioned for them. Users will be able to easily request support from Onpoint's technical support staff about all aspects of the Analytic Environment and will be able to track any requests or issues through Onpoint's Jira-based help-desk ticketing system. In the Analytic Environment, multiple schemas are maintained as data sets are created, allowing for the team to shift to a previous version of an extract deliverable if significant deficiencies are reported.

Communications will always remain open, team members and goals will have clear direction, and project approach will be transparent.

- **Roles & Responsibility – Onpoint Team**
  - Data Operations Lead
    - » Triages reported issues related to Onpoint's data submission and integration platform, Onpoint CDM, and communicates with IDOI staff to resolve issues
  - Analytic Engineer
    - » Triages reported issues related to Onpoint's Analytic Environment and communicates with IDOI staff to resolve issues
  - Health IT Project Manager
    - » Documents all application changes and any related scope changes as needed

- **Roles & Responsibility – State Team (IDOI)**
  - IDOI Analysts
    - » Participates in the UAT process for applications prior to production, providing recommendations based on areas of expertise
    - » Reports issues and concerns via Jira or Onpoint's Help Desk if they should arise
    - » Assist with review of reported issues
  - IDOI Program Manager
    - » Approves post-production application changes and any related scope changes as needed

8.11 Provide an example of a high-level project management plan and project schedule for this project. This should include your tasks, sub-contractor tasks if applicable, and State tasks in an integrated fashion. Include key tasks as part of development, testing, training, data conversion, other key areas of the project.

Describe your method of creating the schedule and the method and frequency of maintaining the schedule throughout the project.

Identify and describe the tool(s) you use to create and manage the schedule.

Describe methods you use to measure schedule performance and how you will know when to escalate schedule risk?

High-Level Project Management Plan & Project Schedule

For a high-level project management plan and project schedule please see **Table 8.10.A**, above.

Schedule Creation

We use PMBOK® best practices when creating the schedule and the Work Breakdown Structure (WBS). The schedule will be created with approval from the IDOI stakeholders and subcontractors and will be updated, if necessary, on a weekly basis.

Schedule Management Tool

Schedule management will be done using Mavenlink, which is a robust project management tool used to track the schedule, milestones, deliverables, tasks, and requested/approved changes.

Schedule Performance

The Schedule Performance Index (SPI) describes the relationship at the project or task level between the planned schedule and the actual schedule. Our project managers review this metric to identify tasks or projects that are currently tracking ahead of or behind schedule at any given point. Used in combination with the task status, the SPI will allow our Health IT Project Manager to take corrective action and to escalate to the greater team to keep the project on schedule instead of managing from a reactionary position.

8.12 Provide a test plan / strategy document that among other things describes the overall testing process and the types of testing that may be in scope before application functionality is implemented.

What is your approach and frequency to testing online portals before and after "go live"?

What communication avenue will be available to the State if defects are found in testing? Will your company use tools to track / manage defects?

Describe and provide process flow of the defect management process.

What is your approach for validating end user documentation and business process?

What is your approach to testing data backup procedures?

Where will test cases/scripts be captured and maintained?

Provide an example of a Requirements Traceability Matrix used on a similar project.

Identify and describe any automated testing tools that will be used.

What roles / responsibilities do you see for your company and for the State in testing the application?

Identify and describe the testing environment(s) that your company recommends as part of the project and why.

Testing Approach & Frequency

Onpoint performs testing throughout the various stages of our system development lifecycle. We use Jira to track all development tasks whether they are enhancements or bug fixes. As part of any Jira development task, a quality assurance analyst develops a test plan to ensure that the development task meets its expected objectives. Developers working on the task write unit tests in conformance with the test plan. These tests are then executed and must be passed before code is incorporated into the main code branch. Onpoint uses Jenkins to run automated unit and regression tests using the following steps:

- The developer commits code to the source code repository using a source control tool (e.g., Bitbucket).
- Jenkins creates a new build with the new code commit incorporated into the latest successful build.
- The build runs through automated unit and regression tests.
- If all testing passes successfully, the build is approved for release at the next scheduled deployment. If the build breaks, the development team is notified that fixes are required.

When applicable, load testing of applications is performed in a staging environment prior to release to the production environment. Load testing is performed on client-facing systems. In addition to software testing, Onpoint's QA analysts run automated and manual tests on data outputs to ensure that the data meet QA acceptance standards and will be sufficient for downstream analyses and reporting. All development and testing are performed on representative test data. No client PHI/PII is used in any development or testing environment.

As part of our security protocol, Onpoint has third-party security consultants test our external-facing websites and applications to ensure that no security vulnerabilities are identified. This testing is performed weekly using Nessus and annually by a third-party penetration testing firm.

Communication Avenues & Tools for Managing Defects

Onpoint's utilizes both email and Jira's ticketing functionality to track and manage issues and defects and will be rolled out to IDOI and other collaborating contractors to encourage transparency and engagement throughout out project. IDOI can report issues and ask questions via email to Onpoint's Help Desk, which automatically creates a support ticket in Jira (**Figure 8.12.A**) for tracking from start to resolution and allows for transparency in communications. Ticket creation automatically alerts the Operations team to the registered issue, triaging the ticket to the appropriate resources for resolution. Through Jira's Client Dashboard (**Figure 8.12.B**) IDOI team members will be able to easily review the status of all tickets to ensure questions and issues are resolved.

Figure 8.12.A. Jira – Ticket View (Blinded Example)

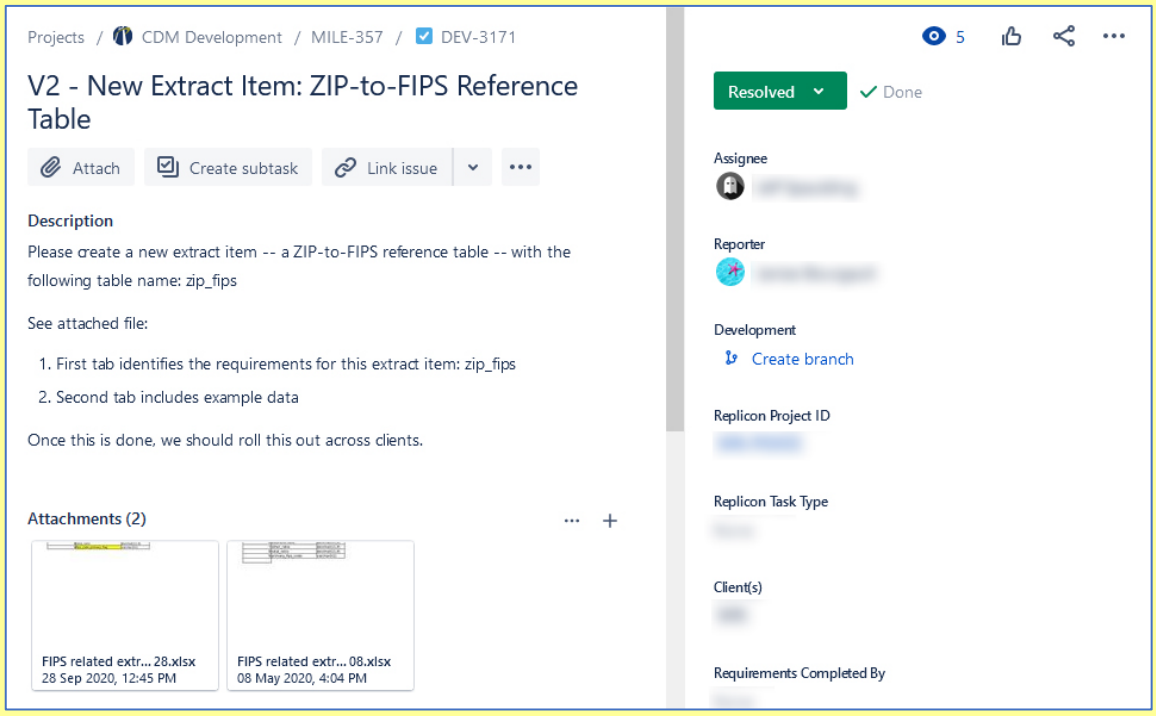
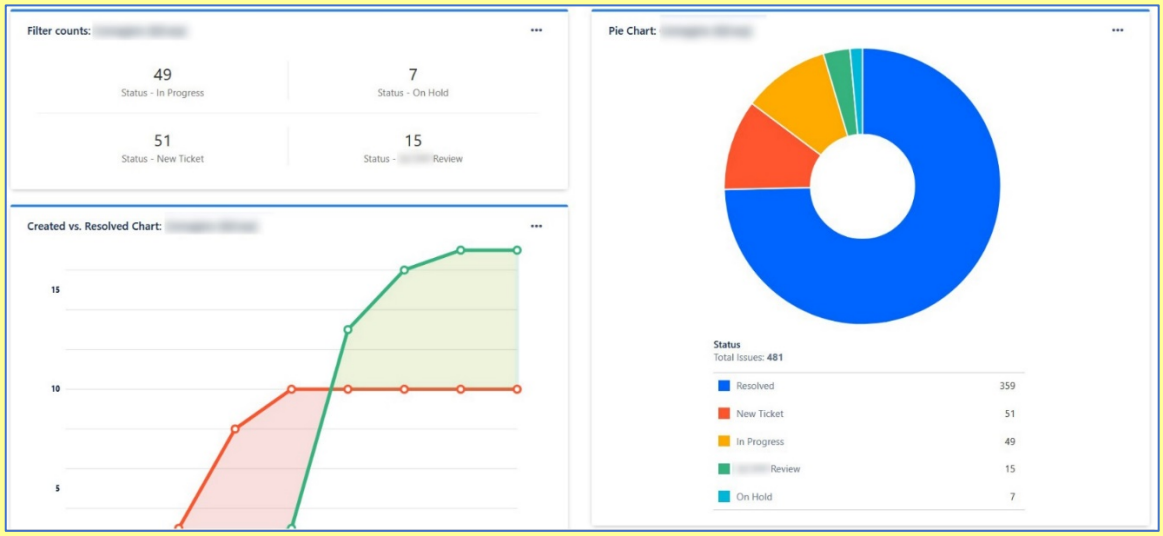


Figure 8.12.B. Jira – Client Dashboard View (Blinded Example)



Defect Management Process Flow

All development requests – whether standard maintenance, a bug fix, or an enhancement – are entered and prioritized in the product backlog. Any serious software flaw is addressed as a hot fix and deployed as soon as possible. Hardware and other application upgrades and patching follow a similar lifecycle, with all application and hardware changes first deployed to a test environment for thorough evaluation prior to being deployed to production.

This systematic yet flexible approach is strengthened by Onpoint's use of Atlassian, an industry-leading project management and collaboration platform that includes Jira and Confluence. Onpoint uses Jira for tracking all planned and unplanned software application and infrastructure tasks. Confluence is used for documentation of product requirements, technical designs, and technical operating procedures.

Jira: Our online workspace. In order to support systems development and testing efforts, Onpoint uses Jira as an issue-tracking and Agile project-management tool. Jira allows our team to create and estimate stories/requirements, build a sprint backlog, identify team commitments and velocity, visualize team activity, and report on team progress. Jira's issue-tracking tools, which we supplement with its sister product, Confluence, provide reporting and requirements documentation and capture a wide variety of tickets and their key components, including:

- **Stories.** In the Agile Scrum methodology, a "story" is a feature or enhancement requested by the product owner on behalf of clients, the development team, or another participant that would produce business value for the organization and its users upon implementation. Stories define major planning and development activities.
- **Acceptance criteria.** Acceptance criteria are added to individual stories to provide additional detail and establish a common definition of completion. For client requests, the user stories and acceptance criteria are reviewed and approved by the client prior to initiating development.
- **Tasks.** Tasks are used to keep track of activities that need to occur, but which are not directly related to planning/building the new system or functionality. Tasks are often

administrative activities (e.g., conducting a call with an API service provider, updating a financial report, adding content to the system, etc.).

- **QA tests.** The team uses Jira to track individual QA tests. Each test is associated with an individual story and verifies that the changes made to the system to implement the intended functionality as defined by the story and its acceptance criteria were completed.

Confluence: Our documentation tool. Onpoint uses Confluence to document product requirements, technical designs, test plans, development and support processes, and release notes. For product requirements, Onpoint uses a Confluence template that includes gathering information in the following areas to ensure that both clients and Onpoint have agreement on requests, requirements, and solution expectations:

- Description of the requested enhancement
- Requirements usually written as user stories
- Test plans
- Acceptance criteria
- Assumptions
- Screen mock-ups and diagrams as needed
- Milestones and related release dates
- Any open questions that require resolution
- A list of items out of scope

Validating End-User Documentation & Business Processes

During UAT, Onpoint provides a test plan that includes validation of both functionality and business processes, using the end user documentation as a guide. Table **8.12.A**, below, is an example of guidelines that would be used for validating documentation and business processes, which includes the page and document as appropriate.

Table 8.12.A. Document & Business Process Validation Guidelines

Category	Role Type	Description	Method
Functionality	Client Admin, Submitter Admin	Credentialed user can log-in to the portal.	Confirm following the "Forgot your password?" link will send a password reset prompt to user's email. Confirm log-in is successful upon resetting password.
	Client Admin	User can view all submissions across different submitters within the portal.	Confirm user can view submissions from both AADPCXX and AADPCXXA using the "Submitter Code" filter on the Submissions page.
	Submitter Admin	User can view only submissions sent by the submitter to whom they are associated.	Confirm user is only able to view submissions from AADPCXXA using the "Submitter Code" filter on the Submissions page.
	Submitter Admin	User can successfully upload a file for each file type in the portal.	Confirm user can upload a file to the portal by following the instructions for uploading a file to the portal in the "User Guide for the Onpoint CDM User Interface" (p.22).

	Client Admin	Client Admin cannot upload a submission to the portal.	Confirm user cannot see an "Uploads" page in the toolbar of the portal when user clicks "Files."
	Client Admin, Submitter Admin	User can view validation results for each submission in the portal.	Confirm user can view list of submissions by first clicking "Files" on the lefthand toolbar of the portal and then clicking "Submissions." Confirm user can view submission-level validation results by clicking into a submission on the "Submissions" page.
	Submitter Admin	User can submit variance requests for a submission's failed validations.	Confirm user can request variances for test files submitted by AADPCXXA following the instructions provided in the "User Guide for the Onpoint CDM User Interface" (pg. 41).
	Client Admin	User cannot submit variance requests for a submission's failed validations.	Confirm user cannot see the "Request Variance" next to a submission's failed validations.
	Client Admin	User has the ability to edit, approve, and reject variances in "Client/Review."	Confirm user can edit, approve, or reject variances in "Client/Review" following the instructions provided in the "User Guide for the Onpoint CDM User Interface" (pg. 51).
	Client Admin, Submitter Admin	User can access all documents in the "Documentation" section of the portal.	Confirm user can download and open all documents uploaded to the "Documentation" section of the portal.
Business Logic	Client Admin, Submitter Admin	Each file type's layout matches the requirements.	Confirm user can view both passed and failed data elements in a Completeness report by using the "Status" filter to select "All" completeness validation results for each file type. Confirm that all data elements outlined in each of the file types are present (except for placeholders) in the submission's Completeness report. Confirm the naming convention for each field matches the data element naming conventions.
	Client Admin, Submitter Admin	The "Expected" threshold listed in the Completeness report matches the agreed upon minimum threshold that a submitter is required to meet for each data element.	Confirm the "Expected" threshold for each data element in a submission's Completeness report aligns with the "Threshold" column provided in the "Data Submission Guide – Client Thresholds" document.

Testing Data Back-up Procedures

Onpoint's Business Continuity Plan and Disaster Recovery Plan are critical components of our business operations and Information Security Program. These plans are updated on an annual basis and as needed in the event of major system changes. The plans serve as guides for the recovery of normal operations following any disaster that affects the delivery of information technology services in accordance with our performance standards and contractual obligations.

The plans cover the recovery of all supporting systems, applications, and data. All client-facing and mission-critical systems are backed up at least daily with a retention policy of at least two weeks. All other systems are backed up daily to weekly, depending on the criticality of the system. Back-up procedures are tested at least annually by restoring a fully functional server or database

from a back-up snapshot to ensure that back-up procedures are adequate and that our team has the ability to quickly execute our back-up procedures in the event of a real system failure.

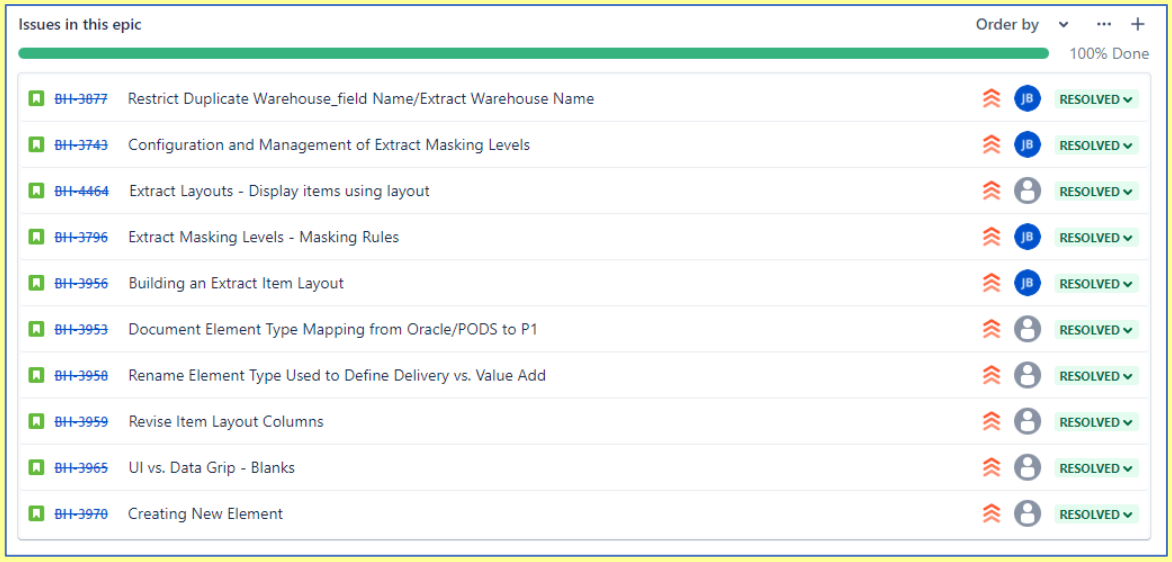
Test Cases / Script Capture & Maintenance

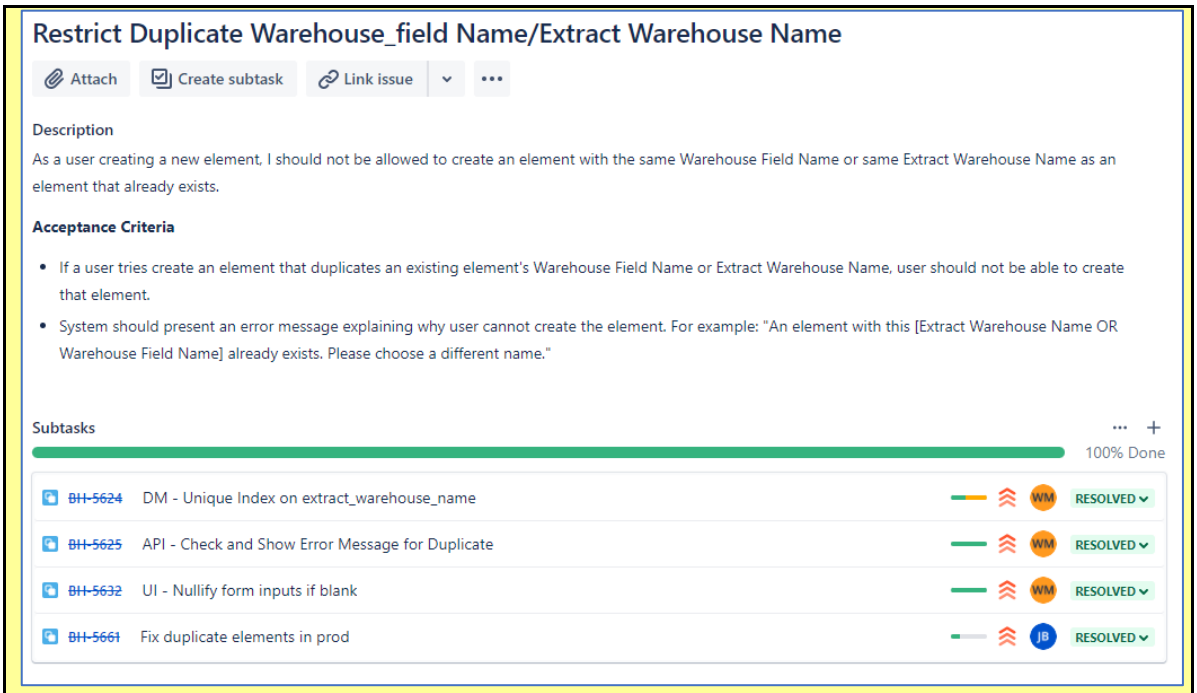
Test cases are first identified within the requirements gathering phase of Onpoint's software development lifecycle and are captured within the Jira tickets created for new functionality. These test cases are used to create automated tests within the development environment, which are automatically executed with each build of the software before code is promoted to the test environment. Onpoint performs multiple levels of testing, including cross module and end-to-end testing within the test environment. Additional test data and testing configurations are stored within persistent databases within this environment.

Requirements Traceability Matrix Example

All requirements for new Onpoint CDM functionality are captured within Atlassian tools. Requirements for larger pieces of functionality are stored within Confluence and Jira "epic" tickets with business requirements and are linked to Jira tickets where tasks are broken down to technical implementation and testing requirements. **Figure 8.12.C** below is an example of a Jira epic and technical requirements for new CDM functionality.

Figure 8.12.C. Jira – Requirement Traceability Example





Automated Testing Tools

As described at the beginning of our response to this question, Onpoint uses Jenkins to run automated unit and regression tests as part of all development cycles. Onpoint's automated user interface testing also leverages Selenium to automate browsers in order to mimic user interactions with the Onpoint CDM portal. Automated security testing is performed using third-party tools offered by Tenable.io®.

Application Testing Roles & Responsibilities

Onpoint's testing methodology ensures that all deliverables stay on schedule and that our performance meets our clients' needs for a high-quality solution. Our testing methodology is centered on automated and manual QA testing, which is conducted rigorously throughout the project. For IDOI deliverables, Onpoint will perform functional and data testing on completed stories and work with IDOI to accept stories as they are completed. Additionally, we will ensure ongoing quality through our schedule of regular status meetings to provide transparency into the prioritization and deployment of IDOI-requested enhancements.

During development, functional testing will be executed at the story level. Items to be tested will be dictated by the acceptance criteria outlined in each user story. The process that we will follow for testing is outlined below:

- Onpoint will work with IDOI to document acceptance criteria for user stories
- IDOI will review acceptance criteria as stories are created
- Implementation of user stories will take place throughout each development sprint
- Onpoint developers will mark a story as finished once implementation is complete
- Onpoint testers will test the story based on acceptance criteria or other QA test-plan criteria such as cross-browser compatibility

- Each user story will be marked as delivered or rejected
- If rejected, the story will be reassigned back to the development team for further work and follow-up.

Recommended Testing Environments

Onpoint uses a four-tier environment – development → test → stage → production – for product development. All system development occurs in the development environment and is migrated to the test environment only after development is complete and all unit tests have passed for the sprint tasks. Once a release passes the testing phase, which includes thorough regression and system testing, it is deployed to stage where internal users, clients, and other external users can perform user acceptance testing. While in stage, performance and load testing are conducted to ensure that the new release meets performance expectations. The stage environment is used only in instances where load testing is necessary or access is needed for individuals outside of the product development team. This step may be skipped if product updates do not require this type of testing. Once this phase is approved, the release is deployed to production.

All development requests – whether standard maintenance, a bug fix, or an enhancement – are entered and prioritized in the product backlog. Any serious software flaw is addressed as a hot fix and deployed as soon as possible. Hardware and other application upgrades and patching follow a similar lifecycle, with all application and hardware changes first deployed to a test environment for thorough evaluation prior to being deployed to production.

8.13 What is your approach to promoting relationships, teamwork, facilitating open and timely communication, and ways staff will foster a collaborative effort among themselves, any subcontractors, and IDOI staff? Include details on managing requests and meeting strategy (frequency, agenda, staff, etc.). The IDOI expects the Administrator to prepare agendas and background for and minutes of meetings. Background for each status meeting must include an updated Work Plan.

Onpoint's project team relies on regular, well-structured meetings to exchange information regarding the status of project milestones and tasks, current activities and upcoming priorities, and general progress related to the Project Management Plan. These meetings typically fall into two categories:

- **Biweekly status meetings** are designed to exchange information with the full project team from both Onpoint and IDOI to provide status updates on open issues and Jira tickets, explore questions, discuss project milestones, identify risks, and solicit important new information related to the project, with agendas provided beforehand for additional input. During implementation, our Health IT Project Manager will provide an updated Work Plan and will take minutes, providing copies of both to the IDOI following the conclusion of each status meeting. All meeting materials, including agendas, notes, and standard and ad hoc progress reports will be maintained for always-available reference using the SharePoint-based Collaboration Zone.
- **Ad hoc meetings and working sessions** are designed to identify and explore an issue or topic of interest more fully and to problem-solve or establish a plan to address the issue or topic. The staff attending these sessions will vary based on the topics covered and the type of subject matter expertise required.

Our Health IT Project Manager will be responsible for preparing agendas for standing meetings as requested by the State. To ensure collaboration and project transparency, Onpoint's team will use a suite of proven and industry-standard tools and resources – regular calls, webinar check-ins, Mavenlink, Jira, Confluence, a SharePoint-powered Collaboration Zone, and on-site meetings.

8.14 Describe your status reporting processes.

What type of status reports are produced and at what frequency?

How are status reports distributed and to whom?

Provide an example of status reports that the State can expect for this project.

We will provide a biweekly status report to all stakeholders based on key indicators to track for Onpoint and IDOI. Tasks and issue timeliness will be displayed visually by green, red, and yellow icons as follows:

- Green – Task is on schedule
- Yellow – Task is at risk; estimated completion date is beyond the planned completion date
- Red – Task is late; planned completion date for the task has passed

The status reports will be disseminated to all relevant stakeholders on a routine schedule prior to each status meetings via email. These stakeholders include the primary IDOI project managers and task leads in addition to all Onpoint team members.

If changes to schedule, scope, or budget are required, Onpoint will discuss required changes and raise potential needs during a status meeting with IDOI. The Onpoint team will meet with IDOI consistently, but if ad hoc meetings or discussions are needed, those will be scheduled with all relevant project team members. While the status report will include information on work accomplished, we also will use the report to track upcoming tasks, decisions needed, risks, issues, and activities. **Figure 8.14.A** displays an example of the key fields and status reporting that will be reviewed with IDOI to ensure consistent communication regarding the project status. The final status report template will be finalized with IDOI to ensure completeness and accuracy.

Figure 8.14.A. Status Report Template (Example)

Subject	Biweekly Status Report	Date	
Compiled By	[PM Name]	Distribution List	

Accomplishment Performance

No.	Topic	Detail
1	What has been accomplished in the past 2 weeks?	•
2	What did not get accomplished in the past 2 weeks?	•
3	What do we expect to accomplish in the next 2 weeks?	•

Milestone Performance

Description	Status	SPI	Baseline Delivery Date	Forecast (F) or Actual (A) Date

GREEN – On target to achieve Milestone Date. Baseline date = Forecast Date.

Yellow – Milestone Target Delivery Date is in danger of not being achieved but a managed solution capable of bringing forward the Forecast date is being applied. Baseline date < Forecast Date

RED – Milestone Target Delivery Date is not going to be achieved or has already passed. No work rounds or solutions capable of bringing forward the forecast dates are available.

SPI = 1 - On plan or on schedule
SPI > 1 - Ahead of schedule
SPI < 1 - Behind schedule

8.15 Provide a detailed description of the training schedule and overall training strategy/plan for State users prior to and during implementation (e.g., on-site, virtual, etc.).

Describe your high-level Training Plan

In what delivery method will application user training be provided (e.g., instructor led on-site, instructor led remote, web-based, Computer Based Training modules, and reference materials) and in what setting (virtual or in-person)?

What training model will be used for application users if instructor-led training is chosen (respondent trained, train-the-trainer, combination)?

How will new application users be trained going forward and what options exist for refresher training?

How will online help be created / maintained as part of the application?

How will the Administrator set up a repository for training materials accessible by application users?

Training Plan Overview

Our approach to training always has been – and will remain – to tailor it to the needs of our clients and their end users. Our support is thorough and comprehensive, relying on a combination of webinars, conference calls, one-on-one calls, and dedicated office hours. Additional details follow:

- **Stakeholder training.** Onpoint's program team for the Indiana APCD will host several trainings and orientation meetings over the course of the implementation for all stakeholders. These trainings will cover a range of topics and include Q&A sessions to ensure that submitters have the support that they need to stay on track. Training topics and meetings will include:

  - Understanding the APCD's data submission guide
  - Setting up for secure SFTP data transfers to Onpoint CDM
  - One-on-one welcome meetings for all registered submitters to review their questions and discuss any possible challenges they feel may limit their ability to meet the required Indiana APCD data thresholds
  - Ongoing and ad hoc submitter meetings – daily, weekly, monthly – to answer questions and keep submitter development efforts moving smoothly and efficiently

- **Onpoint CDM submitter training.** To support the submitter registration process in Onpoint CDM the Operations team will provide ongoing support to registered data submitters, including:
  - Communicating data collection deadlines and validation status
  - Scheduling touchpoint calls and webinars as needed to troubleshoot questions
  - Providing updated documentation related to data submissions
  - Providing training opportunities for data submitters and new Indiana APCD data users
  - Providing training prior to initial file submissions as part of the "Data Submitter Workgroup Meeting: Onpoint CDM Overview" sessions
  - Providing training when revisions to the APCD Program's DSG are published as part of the "Data Submitter Workgroup Meeting: Data Submission Updates" sessions

  Upon project start, Onpoint will conduct a series of Submitter Workgroup Meetings to walk submitters through all key components of the APCD submission process, including a detailed review of Indiana's DSG, file submission methods, data quality requirements, and submission timelines. Among these key trainings is an orientation to Onpoint CDM's online interface, which provides authorized contacts with step-by-step walk-throughs regarding how to monitor the status of their submissions, request variances, access relevant documentation, and review up-to-date quality and variance reporting at any time.

  These trainings are supplemented by scheduled one-on-one check-ins with each participating submitter to better learn about their data submissions and any possible challenges that they may foresee with data submissions. Training sessions also are not restricted to project implementation. Whenever a situation arises that requires action by a payer, Onpoint will work with them to address their questions and ensure that IDOI's data collection remains on track.

- **Analytic Environment training.** During the onboarding process, users of the Analytic Environment also receive a series of trainings to orient them and ensure that they have the technical support to connect all available tools to their data sets. Users will receive guided demonstrations of each tool available within IDOI's Analytic Environment and have access to all supporting documentation.

  As part of the data delivery process, Onpoint's client-support and IT teams remain available to provide regular updates, check-ins, and technical support to ensure on-time and satisfactory delivery. In addition, Onpoint provides regularly scheduled user group trainings to inform end users of upcoming enhancements, provide focused trainings on data use cases, offer billing and claims data updates, and explore other topics of interest.

Onpoint will ensure effective ongoing support to IDOI and authorized data users by providing:

- Analytic support resources who have a detailed understanding of Indiana data submissions and extracted data sets
- A help-desk service and ticketing system for the triaging of support questions and requests
- Individualized support and end-user webinars to troubleshoot questions and outline upcoming changes to the APCD data structures or tools within the Analytic Environment
- Useful, up-to-date documentation to support efficient use of the analytic data sets
- Training in the use of Onpoint's Analytic Environment and data schemas
- Training related to any update in functionality to systems and data enhancements

Training Delivery Method & Settings

Onpoint uses an instructor-led approach for training with most of our training offered virtually, and led by a knowledgeable Onpoint subject matter expert. At the request of the State, Onpoint can provide onsite training sessions for end users and IDOI staff. In our experience, data submitters prefer virtual training sessions as their locations and availability tend to vary widely. Reference materials, including copies of training slide decks and training guides, are provided after each training session and remain available via SharePoint. Submitter-focused materials, such as user guides, also can be made available in the Onpoint CDM portal for easy reference.

Ongoing & Refresher Training

Our team prioritizes collaboration and provides steady communications using an array of tools that keep the IDOI team, submitters, and data end users informed and connected every step of the way. Our tools for ongoing and refresher training include regular all-submitter calls and webinars, email updates with helpful tips, notices detailing any upcoming system or rule changes that may impact them, and dedicated Operations staff to address emails, calls, and questions anytime they arise. We provide training with all system updates and hold user group sessions to help our clients ensure that they are kept informed of process improvements, policy changes, and trending topics related to APCDs and other healthcare issues. As our clients' teams grow and change, we are always available and willing to provide additional refresher training sessions.

Online Help Creation & Maintenance

All IDOI users and Analytic Environment users will be able to easily request support from Onpoint's technical support staff. Onpoint provides an online help-desk service and email ticketing system for the triaging of support questions and requests, and we track all requests or issues through Onpoint's Jira-based ticketing system. Jira's functionality is used daily by Onpoint staff to track and manage issues, tasks, and projects and will be rolled out to IDOI and other collaborating contractors to encourage transparency and engagement throughout out project.

Training Material Repository

To facilitate communication among team members, Onpoint uses SharePoint-powered Collaboration Zones for hosting client-facing training materials as well as a document repository within the secure Onpoint CDM portal for submitter-facing training materials. The Collaboration

Zone also provides a centralized online hub for sharing documents, notes, findings, FAQs, and more.

8.16 Identify any potential concerns, risks, and mitigations to the proposed approach, given that requirements identified in the RFP may change and may need further definition as regulations and operational decisions are finalized.

Based on Onpoint's experience implementing APCDs in other states, possible risks and mitigation strategies that IDOI may wish to consider include the following:

Risk #1: There is a delay in kicking off implementation activities due to scope uncertainty.

Mitigation: Onpoint will work collaboratively with IDOI and your stakeholders to clearly understand and thoroughly document individual needs and interests. We will work quickly and flexibly to address issues and build relationships. Roles will be clear, and processes will be transparent. We will work collaboratively with IDOI to ensure that parameters are well defined from the outset.

Risk #2: Costs become inflated as scope changes are made.

Mitigation: Our Account Management Lead and Health IT Project Manager will work together to manage the contract and ensure adherence to the mutually agreed-upon scope. Communications will be open, our approach will be collaborative and transparent, risks will be proactively identified and managed to avoid delays, and deliverables will be completed as scheduled to ensure costs do not become inflated. Throughout, the project Work Plan will be updated to ensure that all parties remain aligned on the APCD's scope and objectives. All ad hoc and change requests will be followed up with a timeline, scope summary, and a cost estimate (if relevant) and will require approval by IDOI to begin the work,

Risk #3: Poor communication results from the use of inadequate tools and technologies.

Mitigation: Onpoint utilizes a combination of email, ticketing platforms such as Jira, collaborative workspace environments such as SharePoint, and video conferencing applications. Our Health IT Project Manager will ensure that all parties are familiar with our proposed project management tools and will provide additional training as needed. A clear, comprehensive Communication Management Plan also will be developed in collaboration with IDOI to ensure that communication remains effective throughout the contract.

8.17 What is your approach to staying informed and taking early advantage of any federal guidelines, clarifications, technical advancements, and other federal and State sharing opportunities during the life cycle of the project?

As an innovator in a rapidly changing field, Onpoint understands the need to constantly grow and stay informed as our healthcare market changes. All Onpoint employees regularly attend development opportunities through technical training, higher education, in-house training sessions by industry experts, and team cross-trainings. Our staff is required to attend annual trainings in HIPAA, security and privacy, and other critical topic areas. Staff also participate in a variety of

webinars and conferences, such as the National Academy for State Health Policy Annual Conference, Health Datapalooza, and the National Health Policy Annual Conference.

Onpoint serves on the board of the National Association of Health Data Organizations (NAHDO) and has been involved in guiding the development of the national APCD Common Data Layout (APCD-CDL™), including recent advocacy for needed improvements to facilitate the integration of alternative payment models and government payer-specific elements. Our approach to solutioning and program design is informed by our collaboration with such organizations as well as by decades of work with APCD data. We regularly review and update our platforms based on changing guidelines, shifting industry standards, and by scrutinizing incoming data and evolving analytic uses to ensure that lessons learned for any client are leveraged to enhance the data across all clients.

8.18 Provide a timeline that covers the first four (4) years of the project, based on a monthly scale.

Figure 8.18.A, below, provides a high-level timeline that covers the first four (4) years of the project based on a monthly scale:

8.18.A. Indiana APCD Four-Year Project Timeline

8.19 Describe your proposed change management process.

All change requestors will input their change requests to the Health IT Project Manager in writing. As described in our response to Question #8.8 above, our Health IT Project Manager will be responsible for triaging all written change requests and will enter each one into the designated project management tool for tracking and reporting to the Change Control Board (CCB) for further evaluation. When considering newly identify change requests, the Health IT Project Manager will analyze the possible impact of the change request on project objectives, including scope, schedule, and cost, and will present this information to the CCB. The CCB will then decide if the change request should be approved, rejected, partially approved, or postponed to a later date. All stakeholders will be notified of the change request decision, and approved changes will be routed for implementation planning and documentation, flowing through the appropriate request status updating.

8.20 In the event one of your team members is not meeting the State's expectations, describe the processes to replace the team member.

Onpoint is committed to effectively retaining and redeploying all institutional knowledge of IDOI's specific and unique requirements should a qualified personnel change be requested by the State. If a key staff member does not meet the State's expectations or is unable to perform their duties, Onpoint will conduct a personnel evaluation interview with IDOI to understand how staffing could be improved and what specific skills the State is seeking in a replacement team member. Onpoint will then provide a staff profile for our suggested replacement team member, which IDOI will be able to review and approve. Once a suitable new candidate has been identified, Onpoint will ensure that all client-specific knowledge is transferred, that the transition is seamless, and that deliverables remain on track. All changes to staffing will be noted in the Resource Management Plan.

9. Maintenance, Support and Enhancements

9.1 Describe your overall support strategy for post go-live support and ongoing user support services.

Identify those services that will be available to the State's users, including your user support and training, query assistance, data navigation, report creation, and notifications about changes to the system.

Who will provide the support?

How are help desk operators trained?

How will your company monitor the entire solution, including the application layer, network, and data center?

Describe your escalation process. If there's a problem, what escalation procedures do you have? Are there tiered layers? What happens at each stage?

What will the maintenance windows be?

Describe how you will fulfill each of the system maintenance activities listed in Section 9.1 – Maintenance and Support.

Identify those services that will be available to the State's users, including your user support and training, query assistance, data navigation, report creation, and notifications about changes to the system.

Onpoint is recognized by our clients for our ongoing support of end users, including regular client-specific and cross-client user group webinars, updated documentation with each data release, regularly scheduled "office hours" with analysts to explore query optimization and data mart reporting, and accessibility of staff to address questions whenever they arise.

Users provisioned with an Analytic Environment account will be provided with hands-on support and training by Onpoint's technical staff to ensure that they are able to securely and efficiently access the data sets and tools provisioned for them. Users also will be able to easily request support from Onpoint's technical support staff using our Jira-based help-desk ticketing system. As new users are identified, Onpoint will provision them with new workspaces and the agreed-upon tools consistent with our proposed solution.

Notifications regarding system changes are provided through both user-group meetings and via email to all approved users of the Analytic Environment.

Who will provide the support?

Onpoint's assigned primary and supporting analysts for the Indiana APCD will provide key support for the State's end users, pulling in team members from our full analytics team and other departments whenever needed.

How are help desk operators trained?

Onpoint's help desk is staffed not by arbitrary operators but instead by our experienced IT and Data Operations staff members to ensure that questions are reviewed by staff with deep

experience in the data and infrastructure. All incoming questions and tickets are triaged to the appropriate team based on the question or issue.

How will your company monitor the entire solution, including the application layer, network, and data center?

Onpoint's IT staff and developers use a variety of tools and dashboards to monitor Onpoint's cloud infrastructure. Our team is notified in real-time by alarms of events that may impact the performance or security of Onpoint's solution. For example, our staff receive notifications if critical servers malfunction, if storage or memory are at capacity, or if unauthorized users attempt to log into the virtual private network (VPN).

Describe your escalation process. If there's a problem, what escalation procedures do you have? Are there tiered layers? What happens at each stage?

Onpoint's dedicated, experienced, and responsive project managers will be the state of Indiana's first line of response and are skilled at fielding feedback, questions, and triaging technical support queries. Should the State feel that additional support is needed to resolve a problem, the issue can be escalated to Monique Cote, Onpoint's Client Services Manager, as well as to Joanna Duncan, Onpoint's Chief Operating Officer. While Onpoint's project team for the Indiana APCD will have designated key resources, Onpoint's full bench of team members routinely works together to support each of our APCD clients to resolve identified issues and is recognized for being both resourceful and accessible.

What will the maintenance windows be?

Onpoint performs regularly scheduled maintenance on a monthly basis. Regular maintenance periods are conducted Friday evenings during off-peak periods, with email notifications provided to end users that may be impacted (e.g., submitters, credentialed users of the Analytic Environment). Onpoint will notify the State if critical updates or patches need to be made outside of this regularly scheduled period.

Describe how you will fulfill each of the system maintenance activities listed in Section 9.1 – Maintenance and Support.

- **System maintenance.** Onpoint's IT team performs regularly scheduled maintenance on a monthly basis.
- **System performance monitoring and reporting.** Onpoint's IT staff and developers use a variety of tools and dashboards to monitor and report on Onpoint's infrastructure hosted in the Amazon Web Services (AWS) cloud.
- **Incident management.** Onpoint has an Incident Response Plan that is used to guide how our team will respond to any incidents. Onpoint also will factor into our response any Indiana-specific contractual or security obligations.
- **Help desk services.** Onpoint will provide a support process that leverages our Jira help desk. The timing of responses and resolutions are tracked within this software and readily available for reporting.

9.2 What is your approach for monitoring and reporting performance of the system during operations? Include metrics that will be tracked, frequency of reporting, and how these metrics can be accessed.

Various monitoring tools are employed within Onpoint's infrastructure, including support for the Analytic Environment. [redacted] Onpoint will work with IDOI to determine the key metrics of interest to IDOI and develop a reporting format and frequency appropriate for the agreed-upon metrics.

9.3 How do you propose to provide regular submission reports to the IDOI, and at what intervals? What information would be included (the number of records processed; the number of records requiring correction; scores for timeliness, completeness, uniqueness, and validity; etc.)?

Onpoint provides regular submission reports during scheduled status updates that summarize key metrics on a twice-monthly basis. These regular submission reports span all submitters but also focus especially on the status of submitters comprising 80% – 90% of covered lives and cover a variety of metrics that include the following:

- Number of submitted files
- Number of files that have passed the validation phase and are approved for processing
- Submitters that have not started submitting or are delayed
- Variance requests in review and pending approval

9.4 What is your plan to provide access to real-time data submission status information to the IDOI that includes the status of each supplier's submissions and files? How frequently do you propose to provide status reports that document any communication regarding missed deadlines, rejected files, or other compliance issues?

All file submissions are processed by Onpoint CDM using a systematic workflow and validation process, providing credentialed users with access to a real-time view of their files' workflow, including updates regarding each file's status, data completeness, and any applied variances. Submitters, Onpoint staff, and our clients are able to view detailed data quality feedback within Onpoint CDM and receive automated emails that summarize each file's status at each stage of processing.

Onpoint's data collection and integration solution, Onpoint CDM, provides credentialed users with up-to-date dashboards and reports on a wide range of metrics related to their APCD file submissions. Using the secure portal, IDOI staff and data suppliers can follow each file submission as it moves through the processing queue to access key details related to file progress. Onpoint CDM also offers a series of dynamic dashboards that enable Onpoint staff and our clients to monitor key performance indicators (KPIs) such as the number of submissions in review by file

type, the number of variances requiring review (with drill-down), and a summary of overdue submissions.

In addition, all credentialed users also have access to real-time, detailed reports regarding the status of their submitted files as they are vetted for quality at each of the three key automated validation stop gates: (1) proper formatting and file integrity, (2) data completeness and validity, and (3) data quality. Reports for each of these stages are available in the Onpoint CDM portal with multiple filtering options for the quick and intuitive relay of current file status and summary statistics by payer, file type, acceptance/replacement stage, and reporting period. Users can select any file to view additional information, including record counts (with breakouts for valid, invalid, and null records), expected and achieved completeness thresholds, as well as a detailed list of any failed data quality validations.

Onpoint CDM's user interface has been designed deliberately to foster transparency and provide credentialed users with a quick, convenient, and effective dashboard that provides visuals on KPIs and a snapshot of a user's outstanding "to-do" items that need to be addressed. In addition, a suite of detailed reports is available to clients and submitters to monitor their individual file submissions, the status of submitter registrations, and other submission and program reports necessary to monitoring program success. The dashboards and associated reports are continuously refreshed and available 24/7 to credentialed users (**Figure 9.4.A**).

Figure 9.4.A. Onpoint CDM Submission Status Dashboard (Demonstration Client)

Status of Submitter Registration & Training

Onpoint CDM's landing page includes a dashboard that also displays real-time KPIs related to the registration process. Examples include the number of outstanding registrations and a summary of registrations within each status category (**Figure 9.4.B**). While each submitter can view registration KPIs related only to their own organization, clients are able to view registration KPIs across their entire APCD program, summarizing registration metrics and statuses across submitters.

Figure 9.4.B. Dashboard Widget: Onpoint CDM Registration Response Status (Example)

Status of Submitter Variances

As file submissions progress through Onpoint CDM's formatting, validation, and quality stages and into the variance process, multiple dashboards and reports provide the stage and status of each submission. These reports highlight the specific status of each submission (e.g., fail, pass, in progress, in review) as it passes through the data pipeline.

Onpoint CDM's dashboard also includes a widget that highlights the number of outstanding variances that need to be addressed by the user. The widget provides easy click-through access to the list of outstanding variances to expedite the workflow and keep files moving efficiently. Onpoint CDM's Variance Module offers users the opportunity to request exceptions to the client's required thresholds for completeness and validation quality. The widget also summarizes the number of outstanding variances and to which party they are currently assigned. For clients and Onpoint staff, this widget can be further filtered to focus on specific time periods or submitters (**Figure 9.4.C**).

Figure 9.4.C. Dashboard Widget – Variance Management (Cross-Payer View)

Once a variance has been requested, Onpoint CDM allows users to track and monitor the status of their requests. The variance approval workflow can be tailored based on specific program needs. For example, variances can be configured so that they are automatically approved (not a recommended approach), are automatically approved only when the achieved threshold is within a specific percentage of the required threshold, or are approved only following manual review. Variances also can be configured to trigger review by Onpoint or both Onpoint and IDOI. Users can track the status of each requested variance within Onpoint CDM. Requested variances that are not automatically approved by the system are placed in a "Review" status until approved or rejected, with 24/7 status reporting available to submitters, the state, and Onpoint staff alike. Onpoint provides final approval of variances for many of our clients, however, the approval protocol can be fine-tuned based on IDOI's interests.

Approved variances, which can be tuned by submitter, file type, field, and duration, are documented in Onpoint CDM and are available at all times to the submitter and the client to ensure both understanding and transparency of the available data.

Status of Submitter Compliance with Due Dates & Data Validations

As noted above, Onpoint CDM's secure, online portal provides all credentialed users with access to real-time reporting regarding the stage and status of submitted files. The landing page dashboard includes a widget that summarizes the percent of submissions by status and file type that can be filtered by time period and, for clients, by submitter (**Figure 9.4.D**).

Figure 9.4.D. Submission Status Dashboard Widget (Client View)

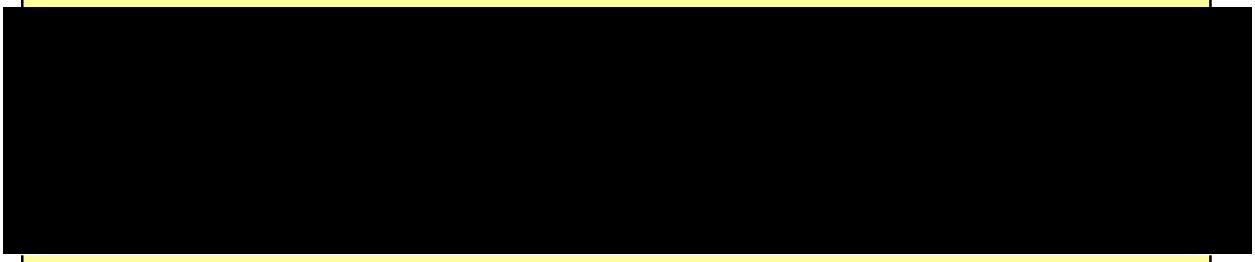
During regular bi-weekly status meetings, a key focus point is those submitters at risk of being non-compliant with their submissions. Onpoint will collaborate with IDOI regarding escalation policies regarding overdue files and compliance issues, The following is our typical cadence regarding non-compliance related to data submission guidelines:

- Week 1: Email reminder of non-compliance
- Week 2: Email reminder with a delivery/read receipt
- Week 3: Meeting with documented minutes/notes, including follow-up steps provided to all attendees by the end of the next business day
- Week 4: Follow-up conference call for updates
- Week 5: IDOI to provide additional guidance

Ongoing Data Submission Status Reporting

Onpoint CDM also includes a detailed submission status report that provides submitters with a summary of the status of each of their organization's submissions across all reporting periods. IDOI and Onpoint staff have an even-broader view: The ability to look across all submitters and all reporting periods to fully monitor the status of all APCD submissions, with icons detailing overdue ( ), rejected/pending ( ), and accepted ( ) submissions (**Figure 9.4.E**).

Figure 9.4.E. Onpoint CDM's Submission Status Dashboard (Cross-Payer View)



9.5 What is your proposed method for maintaining documentation and providing certification of targeted file deletion/destruction at the request of the IDOI? This may include data submitted in error as well as any other data that needs to be destroyed both within and outside the normal data lifecycle.

Physical media controlled by Onpoint are wiped and destroyed in accordance with NIST 800-88. Similarly, media storage devices used to store data by AWS are treated as sensitive throughout their life cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88.

When Onpoint deletes an object (e.g., a submitted file, extract table) in our Amazon S3 storage, removal of the mapping from the public name to the object starts immediately and is generally processed across the distributed system within several seconds. Once the mapping is removed, there is no remote access to the deleted object. The underlying storage area is then reclaimed for use by the system.

Onpoint documents this data destruction in our Jira ticketing system, embedding screenshots of the Amazon S3 deletion process. Onpoint can then issue a Certificate of Destruction when needed.

9.6 Provide a detailed description of the backup and recovery processes used to protect mission-critical data. Additionally, please provide your formal Disaster Recovery / Business Continuity Plan. In your answer, please address the following:

a. What types of redundancy are in place (entire data center, application code, database, etc.)? Is redundancy with a remote location? Provide details.
b. Describe the high-level disaster recovery activities to be used to restore the application and the associated timeline and ownership of those activities.
c. What, if any, impact will the State experience as a result of utilizing the application at the disaster recovery site until the primary site can be restored?
d. What is the maximum application downtime the State can expect once a disaster recovery is initiated?
e. How often is a disaster recovery exercise performed for testing purposes and how will the State participate?
f. When was the previous disaster recovery exercise performed? Describe the high-level results.
g. What priority can the State expect if a disaster recovery is initiated?
h. What is your plan for and associated timeframes related to lost data recreation?

i. Describe how the data warehouse will recover work-in-progress in the event of a system failure.

Table 9.6.A, below, includes details regarding Onpoint's standard back-up processes, with all systems and data located in AWS data centers in the continental United States.

Table 9.6.A. Details Regarding Onpoint's Standard Back-up Processes

Item	Service Used	Back-up Method & Frequency
1. Accepted file submissions from data submitters	[redacted]	
2. Data extracts, tables, data marts, or reporting created by Onpoint for the client		
3. The client's database in the Analytic Environment		
4. Any user-generated files, data, or reporting stored in an Onpoint-specified location in the Analytic Environment		

The overriding objective of Onpoint's disaster recovery planning is continuity of services. In order to minimize downtime that might result from natural disaster, operational error, negligence, or unintentional consequence, the information systems infrastructure design incorporates numerous preventive and recovery controls to keep systems running optimally and preventing unnecessary downtime. For example:

- All of Onpoint's critical systems are in a cloud-hosted data center that features:
  - Multiple internet connections
  - Redundant telecommunications in the form of IP-based phones and cellular devices
  - Hot-failover generators to provide power during an extended outage
  - Advanced fire detection and suppression equipment
  - Climate controls and monitoring by redundant systems
  - Key-card access that is logged and monitored via CCTV

[redacted]

What types of redundancy are in place (entire data center, application code, database, etc.)? Is redundancy with a remote location?

All of Onpoint's systems are built in the AWS cloud with redundancy across multiple availability zones, which provides for our 99% or greater uptime capabilities. Snapshots of configurations, systems, storage volumes, and databases are taken daily and stored in a high-resilience storage area that is replicated across multiple AWS data centers. AWS infrastructure meets the Uptime Institute's Tier III+ guidelines, has been granted FedRAMP provisional Authority-To-Operate (JAB P-ATO), and has been granted Defense Information Systems Agency (DISA) provisional authorization for Impact Level 2.

Describe the high-level disaster recovery activities to be used to restore the application and the associated timeline and ownership of those activities.

Onpoint's Disaster Recovery Plan covers the recovery of all supporting systems, applications, and data. All client-facing and mission-critical systems are backed up at least daily with a retention policy of at least two weeks. All other systems are backed up hourly, daily, or weekly, depending on the criticality of the system and contract requirements. Architecting our systems in the Amazon Web Services (AWS) cloud gives Onpoint the flexibility and resources to achieve our service-level agreements. By relying on AWS, a market-leading cloud technology provider, to provide the infrastructure for our proposed solution, system failures are exceptionally rare, recovery is typically much faster than 24 hours, and any activities related to recovery are likely to be imperceptible to end users.

What, if any, impact will the State experience as a result of utilizing the application at the disaster recovery site until the primary site can be restored?

When redundant cloud systems are used or when applications are restored from back-up versions, the impact to the State experience should be minimal.

What is the maximum application downtime the State can expect once a disaster recovery is initiated?

Application downtime is rare and Onpoint's engagements typically include uptime requirements of 99% or better.

How often is a disaster recovery exercise performed for testing purposes and how will the State participate?

Onpoint conducts disaster recovery exercises on an annual basis using table-top scenario walkthroughs, sample recovery steps, and evaluations of actual outages and recovery actions. All testing and any resulting modifications to the Disaster Recovery Plan are documented and logged. The plans are designed to serve as a guide for the recovery of normal operations following any disaster that affects the delivery of information technology services in accordance with our performance standards and contractual obligations. While clients do not participate in these exercises, a summary of our annual testing can be provided to the State if requested.

When was the previous disaster recovery exercise performed? Describe the high-level results.

In our last exercise in November, our IT team was able to restore a randomly selected server and database from back-up snapshots and test to ensure their usability within 24 hours.

What priority can the State expect if a disaster recovery is initiated?

An active disaster recovery would be the highest priority task of our technical team, and we would dedicate the resources to ensure that we meet our service-level agreements to minimize any impact to the State's program. As Onpoint CDM is a SaaS solution, the State would share the same, highest priority as all of our APCD clients.

What is your plan for and associated timeframes related to lost data recreation?

As noted above in **Table 9.6.A**, Onpoint's systems are architected to meet a recovery time objective (RTO) of twenty-four (24) hours and a recovery point objective (RPO) of twenty-four (24) hours.

Describe how the data warehouse will recover work-in-progress in the event of a system failure.

In the event of system failure, the database can be restored using back-up snapshots of the database, which are less than 24 hours old. The data warehouse is architected so that failures of this type are exceptionally rare. As an additional back-up, all production data can be recreated from original raw data if needed.

If selected for contract award, full copies of Onpoint's Disaster Recovery Plan and Business Continuity Plan can be made available for IDOI's review. An excerpt of Onpoint's Disaster Recovery Plan has been included with this proposal as the following exhibit: "Onpoint - IN RFP 22-70302 - Business Exhibit 2.3.12.A - Disaster Recovery Plan (Excerpt).pdf".

9.7 Describe what planned outages are required, including maintenance, backup cycles, production changes and infrastructure upgrades. How do you ensure there is minimal downtime during normal working hours? What guarantees do you offer for uptime?

As noted above, Onpoint performs regularly scheduled maintenance on a monthly basis. Regular maintenance periods are conducted Friday evenings during off-peak periods, with email notifications provided each time to credentialed data submitters and users of the Analytic Environment.

All Onpoint systems are architected to achieve a 99% or greater uptime service-level commitment. Currently installed fail-safes include the following:

- All application servers have redundancy in multiple AWS availability zones. Should one server or zone fail, the application will failover to another server/availability zone. Elastic load balancers are utilized to manage high-availability services and load balancing.
- Back-ups are automated to the maximum extent possible under AWS to reduce the potential for error and ensure compliance with our plans.

- Onpoint's processing systems, including Onpoint CDM, have multiple node architectures to eliminate the possibility of a single point of failure.
- Multiple back-up copies of systems, configurations, and data are stored in multiple physical locations.

9.8 What is your overall release management strategy and process?

Onpoint CDM has twice monthly releases, in sync with our development team sprint schedule. Release scope is decided at the beginning of each sprint and may include any features that are expected to be completed testing within that two-week window. All software is unit tested by developers then moves into our QA environment where various tests are performed to ensure proper end-to-end functionality.

Onpoint CDM releases do not typically require downtime unless there are extensive updates to infrastructure. Software is released without interruption of services, and our QA team runs a series of pre-planned tests within production. If any issues with the newly deployed code are identified, code is rolled back to prior version. This activity occurs within a two-hour window.

Data releases to the Analytic Environment are performed in close coordination with clients. Onpoint will release data to a new schema leaving the existing data intact, perform QA, and grant access to a select group of IDOI users to review the release. Once approved, Onpoint will make the new data available to other users within the Analytic Environment.

9.9 How frequently will new versions / patches be released? Will there be a regular release schedule?

Onpoint CDM is a SaaS solution with frequent releases that are invisible to end users. Releases typically occur at the end of an Onpoint development sprint, ending every other Friday, but may occur more frequently if necessary to address high-priority issues. Patching of servers and third-party tools occurs during a monthly maintenance window, with advance notification sent to impacted users so they can plan ahead. Updates to the public-facing reporting website will be tied to data releases, occurring once per quarter.

9.10 Will release notes be available and how far in advance before the release will release notes be disseminated?

Release notes that also function as transmittal reports are part of the documentation package that accompanies every extract deliverable. Release notes include details regarding the nature, timing, scope, impact, and remediation plan for identified data quality issues or deficiencies. A change log updated with each subsequent data release as issues are resolved and remediation completed.

Following completion of each quarterly extract, Onpoint will provide IDOI with a release notes package. The release notes will detail any changes in data structure and field assignments since the preceding extract, identify which submitters' data is included in the extract, detail the completeness of the data using triangulation reporting, indicate any data issues that have been

identified and retained in the data, and offer information about enhancements or data findings relevant to data research and analysis.

Onpoint also provides release notes for Onpoint CDM enhancements targeted at different user groups, such as Onpoint's Operations staff and data submitters.

9.11 Provide an example of release notes that the State can expect.

The following images offer excerpts from a recent set of Excel-based release notes that accompanied the delivery of a standard data extract, providing an overview of the content available (**Figure 9.11.A**), a partial change log (**Figure 9.11.B**), and a triangulation report for the available commercial medical claims data (**Figure 9.11.C**).

Figure 9.11.A. Release Notes Table of Contents (Example)

Figure 9.11.B. Change Log (Excerpt)

Figure 9.11.C. Triangulation Report – Commercial Medical Claims (Excerpt)

Figure 9.11.D, below, offers an example of recent Onpoint CDM release notes.

Figure 9.11.D. Onpoint CDM Release Notes (Example)

9.12 How would the State test and give feedback on releases?

For Onpoint CDM, the Analytic Environment, and public-facing reporting functionality requiring input from IDOI (e.g., functionality or language designed specifically for IDOI), Onpoint would provide access to a UAT environment where key IDOI users will have access to review the functionality prior to general release. These UAT environments will be populated with representative data for testing purposes, production data for public reporting and Analytic Environment testing, or curated test data for Onpoint CDM and public reporting software updates. Onpoint will collect feedback from this core set of users and make changes to the code base to address any significant issues. Once IDOI has approved the new functionality, Onpoint will proceed with the production release.

Feedback may also be given following production release through various methods. In the event of a software bug, IDOI users will have access to Onpoint's Jira-based support tracking system and can report issues to our technical team. Other general feedback may be provided directly to IDOI's primary contact during regularly scheduled project meetings as well as during user groups and other Onpoint-led product surveys.

9.13 What obligation would the State have to implement the new release?

Throughout the contract, IDOI will have access to the latest version of our APCD platform solution, Onpoint CDM, including the latest software methodologies (e.g., consolidation algorithms, data quality validations) and all data and reporting enhancements deployed across our client base. Onpoint delivers APCD services through a unified, cross-client Software as a Service (SaaS) model, which ensures that lessons learned for one client are leveraged to enhance and benefit our services for all clients.

Onpoint will work closely with IDOI during the release process for the public reporting website as well as the release of any new Analytic Environment technology to ensure that the timing of the release meets IDOI's needs.

9.14 What is your process for the State to request enhancements? How would you prioritize such requests? Provide an example of form(s) or document(s) that will be used as part of enhancement requests and change request process.

Any requests – whether from our clients or our internal team – follows Onpoint's standard approach to systems development using the Agile and Scrum Systems Development Lifecycle (SDLC) methodology that extends from requirements discovery through analysis, design, development, testing, and deployment. Daily, our team participates in Scrum sessions that support an iterative, rapid-cycle development process to prioritize, develop, and deploy product updates and enhancements.

Product roadmap and prioritization. Onpoint's product team is responsible for defining and prioritizing Onpoint's product roadmap. Product owners conduct regular and ad hoc client interviews to gather feedback on our existing products and collect enhancement and major feature requests so that we can prioritize based on client impact, applicability to other clients, and industry

trends. These enhancements are continuously rolled out to all of our APCD clients as part of our SaaS model.

Sprints ensure ongoing enhancements. Product releases usually occur at the end of a team "sprint," which typically lasts two weeks and provides for the rapid and continuous enhancement of Onpoint's products and our clients' deliverables. Using this approach, Onpoint's products are continuously iterated with minor releases occurring on a frequent basis. Major releases occur when a new product is released or when a major system component is changed substantially.

Our product owners work with both internal and external stakeholders, including clients, coordinating with our client account managers to capture development requests and prioritize them in the product backlog, which is continuously groomed to ensure that the most important features and user stories rise to the top for the next sprint. Client account managers facilitate client scoping sessions for major feature requests as needed.

Sprints begin with planning sessions during which the product owners review the backlog with the team and facilitate the group's discussion to determine the next sprint's scope. Prior to sprint planning, development requests are reviewed to determine requirements, the high-level design approach, and the feasibility for incorporating into the product.

Onpoint uses a four-tier environment – development → test → stage → production – for product development. All system development occurs in the development environment and is migrated to the test environment only after development is complete and all unit tests have passed for the sprint tasks. Once a release passes the testing phase, which includes thorough regression and system testing, it is deployed to stage where internal users, clients, and other external users can perform user acceptance testing. While in stage, performance and load testing are conducted to ensure that the new release meets performance expectations. The stage environment is used only in instances where load testing is necessary or access is needed for individuals outside of the product development team. This step may be skipped if product updates do not require this type of testing. Once this phase is approved, the release is deployed to production.

Jira: Our online workspace. In order to support systems development and testing efforts, Onpoint uses Jira as an issue-tracking and Agile project-management tool. Jira allows our team to create and estimate stories/requirements, build a sprint backlog, identify team commitments and velocity, visualize team activity, and report on team progress. Jira's issue-tracking tools, which we supplement with its sister product, Confluence, provide reporting and requirements documentation and capture a wide variety of tickets and their key components, including:

- **Stories.** In the Agile Scrum methodology, a "story" is a feature or enhancement requested by the product owner on behalf of clients, the development team, or another participant that would produce business value for the organization and its users upon implementation. Stories define major planning and development activities.
- **Acceptance criteria.** Acceptance criteria are added to individual stories to provide additional detail and establish a common definition of completion. For client requests, the user stories and acceptance criteria are reviewed and approved by the client prior to initiating development.
- **Tasks.** Tasks are used to keep track of activities that need to occur, but which are not directly related to planning/building the new system or functionality. Tasks are often administrative activities (e.g., conducting a call with an API service provider, updating a financial report, adding content to the system, etc.).

- **QA tests.** The team uses Jira to track individual QA tests. Each test is associated with an individual story and verifies that the changes made to the system to implement the intended functionality as defined by the story and its acceptance criteria were completed.
- **Testing of software and systems.** Onpoint performs testing throughout the various stages of our system development lifecycle. We use Jira to track all development tasks whether they are enhancements or bug fixes. As part of any Jira development task, a quality assurance analyst develops a test plan to ensure that the development task meets its expected objectives. Developers working on the task write unit tests in conformance with the test plan; these tests are then executed and must be passed before code is incorporated into the main code branch.

Confluence: Our documentation tool. Onpoint uses Confluence to document product requirements, technical designs, test plans, development and support processes, and release notes. For product requirements, Onpoint uses a Confluence template that includes gathering information in the following areas to ensure that both clients and Onpoint have agreement on requests, requirements, and solution expectations:

- Description of the requested enhancement
- Requirements usually written as user stories
- Test plans
- Acceptance criteria
- Assumptions
- Screen mock-ups and diagrams as needed
- Milestones and related release dates
- Any open questions that require resolution
- A list of items out of scope

See **Figure 9.14.A** for an example of one of Onpoint's Confluence-based templates used to gather requirements and track progress through team links to Jira.

Figure 9.14.A. Confluence-Based Requirements Template (Example)

Testing methodology and bug fixes. Onpoint's testing methodology ensures that all deliverables stay on schedule and that our performance meets our clients' needs for a high-quality solution. Our testing methodology is centered on automated and manual QA testing, which is conducted rigorously throughout the project. For IDOI deliverables, Onpoint will perform functional and data testing on completed stories and work with IDOI to accept stories as they are completed. Additionally, we will ensure ongoing quality through our schedule of regular status meetings to provide transparency into the prioritization and deployment of IDOI-requested enhancements.

9.15 Is there an emergency change / enhancement process? Describe the process and associated timing.

Should a software bug or defect be identified in Onpoint's production environment requiring an emergency change, our development team will address the issue rapidly, documenting and communicating any impact to clients' systems access or data.

Onpoint's clients can contact Onpoint either their designated project lead or submit a Jira ticket directly for any emergency changes, bug fixes, or enhancements, allowing the team to handle triaging and status tracking.

Any serious flaw in the software causing an emergency change is addressed as a hot fix and remediated as soon as possible.

9.16 Will training be updated and rolled out as needed for new versions? Describe the process.

Across our APCD client base, Onpoint will continue to enhance the processes and features embedded within our Onpoint CDM data integration platform, and those enhancements will be provided to IDOI on an ongoing basis.

With each new version and enhancement that impacts the experience of end users, Onpoint updates our support documentation and offers training webinars to ensure that clients, data submitters, and other end users always have the most up-to-date specifications and guidance.

9.17 What authority will the State have to stop a production release if testing reveals an issue that the State deems critical?

Onpoint will work closely with the state during UAT periods to identify any issues that the State deems critical and prioritize issue resolution based on this criticality assessment. If the State believes an issue is critical enough to stop the release, Onpoint will resolve the issue before releasing to production. Onpoint will provide estimates for resolution timelines to help inform this decision-making process.

9.18 How are updates to testing and training materials integrated into the release management process?

With every release, updates are made to all associated documentation (e.g., data submission guide, Onpoint CDM user guides, data dictionaries). Depending on the release's impact for end users, training webinars are held to ensure that end users are informed of the enhancements. For updates to the Onpoint CDM data submission portal, data collection rules, and data quality validations, training webinars are held for data submitters to ensure that they always have the most up-to-date specifications and guidance. For enhancements that impact data users, trainings are provided either during Onpoint's quarterly user group sessions for cross-client enhancements or during client-specific user group sessions for state-specific enhancements.

9.19 Please acknowledge your understanding of the warranty period outlined in Section 9 of the Scope of Work. Explain your approach to providing a warranty on delivered solutions.

Onpoint acknowledges and understands the warranty period outlined in Section 9.4 of the Scope of Work.

9.20 What is your approach for transitioning to another vendor at the end of the contract period, should the contract not be renewed?

In the case of a transition of APCD services, Onpoint will work collaboratively with IDOI to ensure a smooth transition that adheres to an approved and well-documented Transition Plan developed in coordination with IDOI. The Transition Plan will document the processes, checklists, and mutual cooperation to be provided by both Onpoint and IDOI to provide for smooth, ongoing operation of the APCD during a transition.

Onpoint's project team will ensure that the Transition Plan spans all key activities and functions of the APCD Platform and covers critical transition tasks, including:

- The identification and inventorying of the State's information assets, including both source and integrated/enhanced data as well as detailed documentation of database content and file structures
- Analysis and reporting on the electronic storage requirements of the APCD data as well as the delivery of the data to the State or its designated vendor
- Listing and availability of key Onpoint staff with up-to-date contact information to consult with IDOI and/or a new contractor
- Documented destruction of all data provided by submitters and the State to Onpoint related to the APCD contract in accordance with the State's policies and timelines regarding such destruction
- Discussion of third-party software licensing arrangements and transfer protocols, including any necessary documentation
- Continued operations assistance in maintaining timely collection and processing of data for an extended contract period until the State or its designee is in place to ensure a smooth transition

9.21 Respondents are encouraged to suggest other enhancements or services that the IDOI may be interested in. All proposed enhancements or services must also have an associated supplement to the Cost Proposal Template (as a separate attachment; not as part of this Technical Proposal response) to reflect any added expense/income associated with the change.

Onpoint has proposed a robust, feature-rich solution that includes many industry-leading analytic enhancements to support the State's APCD. During the contract, should the State identify additional data enhancements or services of interest, Onpoint will work with the State to develop a detailed and cost-effective scope of work and budget.

10. Analytics

10.1 Describe an approach for collaborative work with the IDOI to develop an Analytics Plan.

Onpoint understands the importance of collaborating with IDOI to ensure that the Analytics Plan will successfully address the State's analytic needs. During the first two months after project kick-off, Onpoint will work closely with IDOI's leadership to translate IDOI's vision for the Analytic

Environment into an Analytics Plan. Our work with IDOI will be marked by open communication, attention to detail, transparency in business processes, and reliable execution.

Our recommended approach would be to work with IDOI's leadership to convene a series of Indiana APCD stakeholder meetings that identify and confirm overarching strategic goals for the APCD program, identify primary use cases for the Analytic Environment that will meet the needs of a diverse group of users, review the data governance framework and guidelines (including release regulations) and associated user access restrictions, assess the needs of end users from a training and support perspective, and address the analytic tools and technology requirements for the Analytic Environment. As part of this process, Onpoint will bring forward our own experience and feedback from other APCD clients to meet or exceed the performance requirements described for this task.

Proposed milestones for this task are detailed in the following sections.

Establishing the Project Team & Roles

For the APCD analytics project plan to be successful, establishing a project team that includes members of both the IDOI and the Onpoint team will be an important early milestone to confirm roles and responsibilities and begin building the relationships for a successful initiative. Based on our experience working with other state APCD programs, IDOI's APCD Program Manager will be a key resource along with some level of administrative and analytical support staff allocated to the program. The early focus will be to plan for the implementation of key milestones for the development of the Analytic Environment. These will include timelines for each extract to be transferred to the Analytic Environment, data quality processes and reports, logistics (e.g., hosting, user access controls), discussion of data marts and standard analytic reports to be provided/developed, timelines for development and refresh, documentation and training processes, and strategies for data back-up and disposal.

From the very beginning, Onpoint's project team will be supported by a seasoned Account Management Lead with experience with implementing state APCDs, as well as a seasoned Health IT Project Manager to steer the project throughout implementation and production. Our Account Management Lead and Health IT Project Manager will coordinate the efforts of all Onpoint-assigned staff from our systems development, IT support, information security, operations, quality assurance, and analytics teams. These individuals will be backed by a deep bench of technical experts familiar with all-payer claims data management and analytics experience. These team members offer specialized skills and knowledge across the full range of project domains, including Project Management Body of Knowledge (PMBOK®); billing and claims processing; Onpoint's data management processes and systems; analytic enhancements, including third-party tools; health analytics methods and design, including risk adjustment; and reporting systems development and support.

Project Planning

At kick-off and on an ongoing basis, Onpoint's team will collaborate with IDOI to translate program vision and goals into a concrete Analytics Plan. We envision a plan that contains the tactical objectives and timeline to successfully guide project implementation and that is regularly updated to meet IDOI's needs. Onpoint will work in collaboration with IDOI to develop and deliver a comprehensive draft of the plan no later than sixty (60) days following contract execution and will begin implementation following IDOI's approval.

Milestones for Development of the Analytics Plan

Key milestones in developing the Analytics Plan include the following:

1. **Project kick-off.** The kick-off session will include introductions of project staff, review of project vision and goals, agreement on meeting cadence, and discussion of the Communications Plan.
2. **Establishing key staff and roles.** IDOI's APCD Program Manager will be a key resource, working with Onpoint as the State's primary point of contact for any project issues and communications. Onpoint will confirm key staff assigned and their roles.
3. **Onpoint knowledge sharing.** Onpoint will review lessons learned from prior implementations and provide a detailed walk-through of the proposed solution to include Onpoint CDM and the Analytic Environment, including analytic tools and reporting solutions, along with a product roadmap for future releases.
4. **IDOI knowledge sharing.** Onpoint will look to IDOI to relay valuable project history, key stakeholders, program vision and goals, profile the anticipated user community (e.g., organizations, skill levels, tool preferences), likely use cases, analytic projects or priorities already in the pipeline, known risks or dependencies, expected outcomes from the solution, and near-term and aspirational objectives.
5. **Stakeholder engagement.** With IDOI's leadership and as noted above, Onpoint will convene a series of stakeholder meetings to confirm program goals, identify primary use cases, understand the data governance framework and guidelines (including release regulations) and associated user access restrictions, assess user training and support needs, and address the analytic tools and technology requirements for the Analytic Environment.
6. **Technical information sharing.** Onpoint will share technical information on core data integration processes, analytic enhancements, data architecture, Analytic Environment infrastructure and storage capacity, user roles and access guidelines, and configuration options associated analytic enhancements and tools.
7. **Drafting of the Analytics Plan.** Onpoint will draft the initial Analytics Plan based on feedback from milestones 1–6 above.
8. **IDOI review.** IDOI will review the Analytics Plan and provide feedback.
9. **Finalizing the Analytics Plan.** Onpoint and IDOI will finalize the Analytics Plan and approve it for implementation.
10. **Ongoing collaboration.** IDOI would work with the Onpoint team to coordinate delivery of analytic milestones, including configuration and testing of the Analytic Environment, data user trainings, the process for approval and granting access to new users, and other activities.

10.2 Describe in detail how the required functions of the Analytics Plan will be met in their proposed Analytic Environment and the associated timelines.

Onpoint is proposing our Analytic Environment solution, which is a secure, cloud-based analytics environment that offers role-based access to APCD data for clients and their approved users through a customized suite of tools (e.g., Microsoft Office, Tableau Creator, RStudio, DataGrip for SQL queries, Anaconda (Python)) that is optimized for ease of use by end users with varying needs and skill sets. Approved data users can query and interact with their data using a virtual

desktop in a virtual private cloud hosted by Amazon Web Services (AWS). As part of the development of the Analytics Plan, Onpoint will walk through the configuration options, allowing IDOI to tailor the Analytic Environment to best meet the needs of the State.

Onpoint is prepared to meet all requirements outlined by the State in the Scope of Work's Section 10 ("Analytics"), and our detailed approach, mapped to the Analytic Plan's required functions, and associated timelines are included below.

Regular data refresh. Onpoint's Analytic Environment uses a highly performant data model and [redacted] to optimize query turnaround times and data visualization response times. Delivered through a secure environment with strictly enforced role-based access, the Analytic Environment will offer IDOI quarterly data refreshes that include all data enhancements to optimize end users' analyses. Consolidated data extracts, including value-adds, groupers, and the full suite of enhancements, will be refreshed quarterly in the Analytic Environment. These refreshes are delivered using an automated process that follows in-depth data quality validation of the data. During the automated delivery, IDOI will continue to have access to the previously delivered data sets to avoid disruption of ongoing analytics. Once the refresh is ready, IDOI's approved users can move seamlessly to the refreshed data sets or continue to use a previously released version until their projects have been completed.

Point-in-time reporting capabilities. Point-in-time capabilities are a cornerstone of Onpoint's approach to configuration and delivery of data to the Analytic Environment. Onpoint creates reporting snapshots that are maintained over time, allowing the user to monitor how specific metrics are changing. Onpoint will work collaboratively with IDOI to identify those point-in-time metrics that are most important to your end users, noting that the typical snapshots focus on cost, quality, utilization, and member domains that are refreshed on a quarterly basis.

Data review in the Analytic Environment prior to the data being made available to internal and external stakeholders. Our team has been prioritizing data quality for our clients for more than 40 years. While Onpoint's analysts conduct and document rigorous data quality checks upon each data load to the Analytic Environment, we also recognize that some clients wish to conduct their own data quality checks during a UAT period. We pride ourselves on being active and collaborative resources for such work.

Prior to delivering data to the Analytic Environment, Onpoint's analysts perform a series of steps to ensure rigorous quality review. These steps begin once submitted APCD data has successfully passed Onpoint CDM's intake stage and enters the conversion and processing stage for transformation, consolidation, and delivery preparation. This stage includes a robust quality assurance process that analyzes each processing step in a rigorous and methodical fashion.

Dedicated analysts implement a systematic set of checks that represent a blend of automated outlier flagging and analyst-led investigation. These checks verify that data conversion and processing were completed properly and that the application of data enhancements produced reasonable results. Together, these checks ensure that all data extracts are comprehensive, consistent, and aligned with benchmarks and historical trends. The following sections provide additional detail regarding these comprehensiveness, consistency, and alignment checks.

Comprehensiveness checks. All final tables, as well as tables generated after each major step of the conversion and processing stage, are evaluated to ensure that data conform to the specifications defined for the data set and that all data are included as expected. These checks are

performed at the field level, at the table level, and across tables. The comprehensiveness of an extract is confirmed with the following checks:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Consistency checks. In a delivered data extract, it is critical that all tables contain information and values that are consistent with one another as this allows data users to join tables without data loss. Additionally, table structures must be verified so that aggregation yields accurate totals. These checks are conducted on final tables, and any violation of these checks indicates that a processing error may have occurred. The following consistency checks are performed to confirm that delivered data extracts contain tables that are structured properly and are consistent with one another:

- [redacted]
- [redacted]

[redacted]

[redacted]

Alignment checks. A series of alignments checks focus on confirming that the data contained in a delivered data extract are accurate and in alignment with historical trends and benchmarks. [redacted]

[redacted]

Figure 10.2.A. Data Conversion and Processing – PMPM Trending Dashboards (Examples)

The QA process by which these checks are performed is standardized and methodical. Checks are performed according to a set of specific guidelines, and analysts use standard code to perform the checks themselves, investigating any anomalies or outliers as needed. The process is iterative and reflective, with findings from one extract being incorporated into the QA process for future deliveries and other data products when relevant. The process also is flexible, allowing for customization and investigation into the specific nuances of each submitter. Using this proven process, Onpoint will verify that data conversion and processing have completed successfully and that each delivered data extract is comprehensive, can be used as designed, and aligns with expectations and benchmarks.

Analysis & Reporting

After the conversion and processing stage has completed and all quality assurance checks outlined above have passed, data are ready to be included in downstream extract, analysis, and reporting. During this stage, data are evaluated for "fitness for use" by examining key reporting elements against relevant benchmarks and historical values as well as by investigating all components and antecedents of key reporting elements. While the checks that are performed are specific to each reporting use case, the process for performing these checks is consistent.

Analysts divide reporting results into relevant stratifications and summary levels (e.g., major payer type, age group), comparing them against results from a prior version of the report if available and against relevant benchmarks. Benchmarks for each key data element (when available) are reviewed individually, are specific to the use case, and are selected as a part of the requirements process for each deliverable; for standard reporting delivered on a scheduled basis, benchmarks are reviewed and updated at least annually. During this process, publicly available

benchmarks (e.g., those published by Quality Compass, Health Care Cost Institute (HCCI), CMS), industry-best practice benchmarks, and internally generated benchmarks are reviewed to identify which most closely align with each key statistic of interest.

For example, in reporting that includes rates for quality measures, analysts compare reported measure rates against benchmarks published by the measure steward (e.g., NCQA, CMS), benchmarks made available in the research literature, and historical measure rate benchmarks. This comparison process is conducted at the most granular level of detail that is afforded by available benchmarks. Measure rate benchmarks, for example, often are published at the major payer level (i.e., commercial, Medicaid, Medicare) and, at times, by age group. The quality assurance process leverages this granularity to ensure that all reported measure rates are compared to a benchmark that most closely represents the population captured in the reported rate. Investigation is conducted for any measure rate that exceeds established benchmarks or previously reported results (or falls outside a benchmark range) by analyzing specific components of each measure (e.g., numerator and denominator), the population of members contributing to each measure, and any differences in measure specifications that may help explain differences between the reported rate and any comparison rates.

Reporting may include results from third-party software (e.g., groupers and classification software). In a similar process to that described above, results are compared against those from previously delivered data sets and reporting periods, when available. In addition, benchmarks published by third-party vendors or available in the research literature are utilized to determine the reasonableness of results. Additionally, the internal consistency within each grouper output table is confirmed along with referential integrity across extract tables to ensure that reported results were generated properly.

Quality assurance dashboards are configured to analyze all components and antecedents of key reporting elements for routine reporting and data set generation. For example, Onpoint has created enhanced completeness and validation reports to identify anomalies and potential limitations in claims, eligibility, cost, and lab data that are used in annual measures reporting. These reports are generated iteratively as data are collected. These reports display annual and monthly trends in utilization and expenditures with automatic outlier flagging at each level of detail that will be used in final reporting and can be used to communicate with health plans should there be any need to resubmit existing data or alter their approach to future submissions. In this way, Onpoint ensures high-quality upstream data well before final reporting is generated.

Trending Over Time

As described in each section above, historical trends play an important role in identifying outliers and verifying that newly collected data are comprehensive and accurate. Trending of key metrics is embedded into the QA process at multiple stages of the data lifecycle to ensure that final delivered data sets are validated against established trends and to identify outlier data that may warrant closer examination.

During the intake process, in addition to the formatting, completeness, and validation checks performed automatically in Onpoint CDM, Onpoint evaluates submission counts for incoming submissions and compares them to counts from prior submissions. Any submission that deviates notably from prior submissions is flagged for follow-up with submitters and is relayed to data quality analysts for review when generating the extract.

To validate data during the conversion and processing stage, [redacted]

Figure 10.2.B illustrates a pre-built dashboard [redacted]

Figure10.2.B. Trending Over Time – Claim Count Trending with Flagging (Blinded Example)

[redacted]

Additionally, elements used in analysis and reporting also are trended over time. Measure rates and third-party grouper software results are reviewed by reporting period and compared to prior reporting periods and available benchmarks, with notable changes investigated to ensure that they are reflective of truly changing conditions on the ground (e.g., shifts in utilization, changes in population characteristics) or updates to measure or grouper specifications.

Overall industry trends also are incorporated into the quality assurance process, examining whether trends in the final data extracts reflect industry-wide patterns or shifts (e.g., a 30% – 50% drop in monthly utilization from March 2020 to April 2020 due to the coronavirus pandemic).

Producing a set of standard data sets with documentation that can be released to qualified users for qualified purposes. Onpoint regularly produces and securely delivers a wide range of standard, ad hoc, and customized analytic data sets for our clients. All data extracts and products include technical documentation and ongoing support from our team to ensure that the standard

tools and processes that we use to define, create, and securely transmit each data set to IDOI's Analytic Environment and end users are understood, tested, and ready for use.

Data sets developed and delivered by Onpoint can be scheduled on a regular or ad hoc basis, with the level of detail in the data carefully tuned to provide a rich data set without exposing unnecessary, sensitive information such as PHI or PII based on the specific data use agreement and use case.

Each data set is accompanied by supporting documentation to help end users understand, validate, and efficiently use the delivered data sets and their analytic enhancements. This documentation includes:

- **Release notes**. With each extract delivery, Onpoint provides a set of comprehensive release notes (sometimes called a "transmittal report") that details any changes in the data structure since the preceding extract, identifies which submitters' data is included, offers information about enhancements or data findings relevant to analysts, and features descriptive information about the specific extract, including the extract's reporting period, exclusions, and versioning. Additional features include triangulation reporting and data profiling updates.
- **Data dictionaries**. Onpoint's data dictionaries provide detailed information regarding each extract's tables, fields, formatting, source-to-target mappings, inter-table linkage, and useful tips for data users regarding specific fields (see **Figure 10.2.C**). Additional tabs in our data dictionaries provide users with code-level detail regarding data enhancements and walkthroughs of common use cases, identifying the tables that should be used and linked to explore such cases most efficiently.

  We also provide easy-to-understand explanations of how to use other included enhancements such as how to use our Member Month table to resolve confusion regarding a member's coordination of benefits when a member had more than one eligibility record reported by various payers in a given month.

  Onpoint's dictionaries are provided in Microsoft Excel format for ease of use, allowing end users to quickly find and filter data within tables to focus on desired information.

Figure 10.2.C. Onpoint's Data Dictionary – Emergency Room Flag (Excerpt)

Field Name	Common Name	Description	Origin	Notes	Additional Information
emergency_room_flag	Emergency Room Flag	This field contains a code that is used to identify specific emergency room (ER) revenue or procedure codes within a claim. Valid values are: N = No Y = Yes	This is a value-added field created by Onpoint.	This field is set only on the specific claim line where an ER-related revenue code, procedure code, or place of service code was found. To find true outpatient ER visits, select claim lines where this field is set to 'Y'.	Records are flagged as 'Y' where: Revenue code = 0450–0459, 0981 Place of service code = 23 (ER) Procedure code = 99281–99289

- **Entity relationship diagrams (ERDs).** The relationships between tables within the data warehouse are integral to effective use and downstream analytics. ERDs supplied to IDOI and their end users will detail the relationships between fields, primary keys, reference

information, and the composition of every key table delivered in the IDOI's data sets. (**Figure 10.2.D**).

Figure 10.2.D. Onpoint's Standard Entity Relationship Diagram (Excerpt)

10.3 Provide a list of preliminary recommended data sets referenced in Scope of Work Sections 6.3 and 10.

List and describe any proposed groupers to be used.

Explain if any data will be required from submitters that is not included in the current version of the APCD-CDL™.

Recommended Data Sets (SOW 10) & Consolidation Services (SOW 6.3)

Onpoint regularly produces a wide range of standard, ad hoc, and customized analytic data sets for our clients, delivered either via SFTP with PGP encryption or through our Analytic Environment with role-based permissions.

Onpoint's extract system has been built for agility and flexibility. Our Product Team regularly creates data sets to address our clients' evolving needs, easily building "items" (tables) and "products" (groups of tables) that can be combined to create a multitude of configurable data extracts. Onpoint's extracts are designed to support intensive analytic queries and common use cases that our clients have encountered when utilizing APCD data to answer high-impact questions.

Whenever new data fields are added to a client's collection or when an existing table requires adjustment to address a specific use case, our team can quickly build, QA, and produce the needed product, selecting from all data fields in Onpoint's master data store. This flexibility gives Onpoint the ability to respond quickly to our clients' needs and custom requests.

As with our standard data sets discussed above, all data sets developed and delivered by Onpoint can be scheduled on a regular or ad hoc basis, with the level of detail in the data carefully tuned to provide a rich data set without exposing unnecessary, sensitive information such as PHI or PII based on the specific data use agreement and use case. Each data set features a highly performant data model to optimize query turnaround times and data visualization response times.

Recommended data sets for IDOI include the following:

- **Comprehensive, consolidated data sets.** Onpoint provides data sets that include the full complement of analytic-ready data elements prepared for the APCD, supplemented with analytic enhancements for use by more-experienced analysts. Onpoint also can provide either the values as submitted, the values after standardization, or a combination of submitted and standardized values based on the specifications provided. The comprehensive, consolidated data set includes claim-level detail and typically is refreshed on a quarterly basis.
- **BI reporting and data marts.** Similarly, the BI reporting solution also will be refreshed within the Analytic Environment on a quarterly basis and will include all optimized data marts and Tableau reporting packages that have been automatically updated. A series of data marts with pre-aggregated facts that are optimized for reporting is provided to easily answer common questions surrounding claims data. While these data marts are valuable to analysts of all skill levels, they are designed specifically to be user friendly for analysts with less experience in using advanced tools. The domains and data marts are engineered to ensure performant queries within Tableau and are the backbone of Onpoint's BI solutions. These data marts also can be leveraged with more-complex query tools (e.g., SQL Workbench, RStudio) and integrated with the comprehensive, consolidated data set. The data marts usually are refreshed on a semi-annual basis.
- **Limited data sets.** A limited data set is a collection of claim-level detail tables that are more constrained in the data released. Examples of the types of restrictions included in these limited data sets include the release of PHI, protected financial information (PFI), and data from governmental payers (e.g., Medicare FFS). These data sets may be further limited by restricting the release of sensitive records (e.g., abortion, HIV, mental health, substance use disorder). These limited data sets often are refreshed on an annual basis and ready to release when requested and approved by the state.
- **Public-use data sets.** Public-use data sets are delivered as user friendly Excel spreadsheets with aggregated records that prevent the identification of individual members, providers, and health plans. These data sets typically are generated to provide summary data that can be released to the public and include the application of multiple methods for de-identification (e.g., Safe Harbor methods, CMS cell size suppression).
- **Custom data sets.** Onpoint also regularly creates custom data sets that are delivered upon a client's request for the client or their authorized data users. These include both ad hoc refreshes and custom extracts designed for highly specific data user needs.

  Custom extracts currently in production by Onpoint for our clients span a wide range of data set types and are designed to support a researcher's specific analysis. Onpoint CDM provides many options for data selection and data exclusions to easily customize data sets as approved by IDOI. Examples of extract customization options include:

  - Selection of payers to include in the data set
  - Selection of reporting periods based on paid and incurred dates. This allows the flexibility of including the same range of incurred and paid dates in an extract or instead selecting one time frame for incurred/service dates and a longer time frame for paid dates to capture claims run-out (e.g., incurred dates 1/1/2019 – 12/31/2021 with paid dates of 1/1/2019 – 3/31/2022). The selection of reporting periods can apply to all payers or be adjusted for specific payers – for example, using three months of run-out for commercial submitters but six months of run-out for Medicaid.

- Selection of specific products or lines of business
- Configuration of data masking at a data element level (e.g., Safe Harbor rules of masking)
- Record-level exclusions can be selected to prohibit the release of sensitive records (e.g., abortion, HIV, mental health, substance use disorder)
- Protected financial information, including data elements (or combination of data elements) such as payer, provider, and dollar amounts can be configured to be masked or withheld from extracts altogether

Data Set Documentation

Onpoint is committed to providing data users of our APCD extracts and reporting solutions with documentation that facilitates ease of use and a comprehensive understanding of the data. This documentation typically is either embedded in the solution, posted to a support site, or delivered as supporting documentation for direct recipients of data extracts.

Each data delivery and reporting refresh is accompanied by a comprehensive data dictionary, an entity relationship diagram (ERD), and release notes. (See our response to Question #10.2, above, for additional detail.)

Groupers

Onpoint's proposed solution for Indiana's APCD includes the following groupers:

- **Episodes of care.** For episodes of care reporting, our solution includes Onpoint's Service-Focused Episodes (SFE) grouper, which was developed in collaboration with state APCD clients and stakeholders in support of public-transparency reporting. Onpoint's SFE grouper generates episode costs by facility or location, facility name, major payer type (i.e., commercial, Medicaid, Medicare), specific payer, major service type (e.g., inpatient surgery, inpatient maternity, outpatient surgery, outpatient diagnostic radiology, and other tests), and a broad array of specific services (e.g., hip replacement, cesarean section, knee replacement, colonoscopy, MRI).

  Unlike commercial off-the-shelf products, Onpoint's SFE grouper has been built specifically to run on and reflect use cases for APCD data and offer clients full transparency. Our grouper software has been used in price transparency reporting and other comparative cost analyses for multiple APCD clients and can be delivered much more cost effectively than commercial counterparts. As part of delivering these episode groupers, we include detailed documentation regarding the methods, including specific diagnoses and procedure codes. By contrast, the business rules for many commercial episode groupers are black-boxed so that analysts using the output cannot explain how they were generated. Onpoint's groupers also are configurable and can be modified to align with the nuances of the Indiana healthcare landscape.

- **Condition and procedure categories.** Onpoint will enhance IDOI's consolidated APCD data with All-Patient Refined Diagnosis Related Groups (APR-DRGs) if licensed by the state. Onpoint is willing to sign a third-party access and confidentiality agreement to access these tools and licenses on behalf of State. APR-DRGs focus on the inpatient population and classify patients according to their reason for admission, severity of illness, and risk of mortality. APR-DRGs are designed to span all patient populations, instead of focusing on a subset (e.g., the Medicare population).

- **Risk assessment and scoring.** Onpoint will 3M Clinical Risk Groups (CRGs) to the Indiana APCD data. This grouper is a clinical classification grouper that assigns a member to one of 1,080 distinct and nine higher-level classifications for the year based on the claims data. The system handles severity and comorbidity. For example, a member might be assigned as having diabetes or might be assigned as having diabetes, congestive heart failure, and chronic obstructive pulmonary disorder (COPD). Numeric risk scores can be assigned to the CRG categories using an assignment methodology reviewed with IDOI for transparency.
- **Ambulatory Payment Classifications.** Onpoint will enhance IDOI's consolidated APCD data with Ambulatory Payment Classifications (APCs) using an open-source version of the software developed and maintained by 3M and available for use without license fees from CMS. APCs are a method that CMS uses to pay hospitals for outpatient services under Medicare. Services are classified into bundled services based on their clinical intensity and resource utilization.

Required Data Not in the Current Version of the APCD-CDL™

The APCD-CDL™ in its current form does not accommodate state-specific fields. Onpoint CDM can support adding non-standard fields of interest to Indiana to the file layouts as needed. The APCD-CDL™ also is very limited in the Medicare- and Medicaid-specific fields (e.g., dual-eligibility status, aid categories) that it accommodates. We can also accommodate an enhanced version of the APCD-CDL™ that would be expanded to include data elements specific to these governmental payers.

10.4 What is your current ability to provide standard reports on a regularly scheduled basis that are available for download?

All reports built within Onpoint's Analytic Environment are updated on a scheduled basis and are always available for download in one of two forms:

1. As static PDFs, with Tableau views provided on separate pages
2. As "packaged workbooks" – a Tableau format that saves both the Tableau views and the underlying data. This format can be shared with others who have access to Tableau software, allowing them to view the dashboards exactly as seen within the Analytic Environment.

IDOI users can export reports and either make them accessible to Tableau users in other environments by sharing the workbook file or by uploading the workbook to a hosted Tableau server instance.

Onpoint will work with IDOI to establish a standard process for exporting reports from Onpoint's Analytic Environment to ensure that the reports and their underlying data contain the appropriate level of summarization for public dissemination.

10.5 Describe your standard reporting packages or capabilities. Provide example reports.

Our proposed reporting solution to be deployed in the Analytic Environment is modeled on a set of domains and data marts (detailed below in **Table 10.5.A.**) and is engineered to address IDOI's interest in a rich and easily accessible solution to reliably explore healthcare costs, utilization, and quality across the Indiana health services market.

Table 10.5.A. Onpoint Reporting Domains & Data Marts

[redacted]

To ensure maximum utility for analysts using Tableau in the Analytic Environment, Onpoint will deliver a BI solution with a suite of standard APCD reports that will be updated during each quarterly data refresh cycle. [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]

The BI solution also provides access to a set of data marts that feature pre-aggregated data and measure results to easily answer common analytic questions. These data marts have been optimized specifically for use with data visualization tools such as Tableau and enable analysts to access and download the underlying data to address the needs of analysts of all skill levels.

To illustrate the value and efficiency of Onpoint's APCD data marts, [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

Figure 10.5.A. Sample Standard Report: Facility Service Overview & Associated Costs

Figure 10.5.B. Enrollment Demographics Dashboard (Blinded)

10.6 Describe the level of personalization available to standard reports. Describe what slicers are available to be applied to standard reports for detailed data views.

Onpoint's reporting solution includes a number of standard and customizable reporting dimensions – categories by which measures can be reported or filtered – that will appear in both the standard reports and the analytic data marts. Standard dimensions include reporting period, age band, gender, condition or procedure, payer, insurance product, ZIP code, county, attributed provider, and risk score. Many of these dimensions can be further customized, including geography (e.g., state- and client-specific geographical groupings) and risk score (i.e., Onpoint has the capability to provide several different risk-scoring methodologies, described in further detail in our response to Question #10.17).

While each standard report includes some or all of these dimensions, the exact subset can be customized by IDOI during implementation. Furthermore, all standard reports will be made available for editing by IDOI users, who can further customize them post-implementation.

10.7 Describe how new reporting needs are proactively identified.

In defining future reporting needs, Onpoint will lead initial planning sessions to address any open questions around the vision, purpose, and topic areas of interest and then shift to content and design questions. We work with our clients to identify key measures of interest, desired geographical and other stratifications, and demographic breakouts, for example.

Onpoint will leverage our experience, working collaboratively with IDOI and your stakeholders, to identify, design, and develop user-friendly, well-designed reports that will provide consumers and other stakeholders with useful information regarding healthcare services being delivered in the state.

The requirements-building process will be collaborative in nature and employ Agile principles in order to deliver a product that effectively addresses IDOI's vision and requirements in a timely manner. Related tasks include:

- Collaborating with IDOI and stakeholders to collect requirements that inform the design and content of the BI reports/dashboards
- Developing reporting templates and mock-ups
- Iterating report development as needed to satisfy IDOI's agreed-upon requirements and design standards
- Development and testing of reports and dashboards
- Release of reports and dashboards for IDOI user acceptance testing
- Remediation based on IDOI feedback
- Release of reports and dashboards to production
- Refreshing of the data sets on a regular basis

- Providing technical assistance and documentation to clients and end users
- Collecting stakeholder feedback to inform updates for future releases

New reporting needs for our clients are identified in a variety of ways. Often, reporting needs are identified by our clients, who approach us with questions or topic areas generated by stakeholders and ask us to develop research designs or data sets that will meet their evaluation and health services research needs. Such work may involve the support of state workgroups on specific topic areas (e.g., primary care, surprise billing, cost growth benchmarking), technical guidance, data capabilities, or reporting options. Once we complete a project for one state, we inform others about the work as there often are ways to leverage the code and reporting across clients to efficiently support their work as well. Because we have a diverse set of state clients, we often are able to leverage ideas, coding, and reporting from one client to another for the benefit of all. Standard reporting or new data mart needs also are often identified by our analytics and product teams based on our assessment of the questions that clients are asking and our knowledge of market trends.

10.8 Describe your in-house resources to ensure reports are clinically and statistically valid.

Onpoint's approach to data quality from the intake through extracts to reporting involves comparisons to quality and cost benchmarks and other reasonability checks. Our proposed APCD solution for IDOI incorporates public and third-party benchmark data both to provide comparative context for the data and for quality assurance purposes.

Onpoint uses standard national measures and methods whenever possible to ensure that logic and measures are clinically supported. For example, our quality and utilization reporting is based on certified HEDIS measures and other standard measures like AHRQ's Prevention Quality Indicators. For some clients, we also use AHRQ's Clinical Classification Software (CCS) for procedures. We also use CMS's Chronic Condition Warehouse logic for chronic condition reporting. By relying on measures developed by national experts, we help ensure that our measures are clinically valid.

Additionally, by using our tools across multiple clients, we are receiving regular feedback regarding the quality and validity of methods. As an example, for some of our clients, we use our Performance Reporting Portal to allow providers to validate their data around quality as well as service pricing prior to public reporting or allocation of incentive payments. This review process identifies any potential issues with our logic as providers have strong incentives to review the data and inform us of anything that they believe may be abnormal. For additional information on Onpoint's Performance Reporting Portal please refer to our response to Question #6.54 in Section 6 ("Data Services").

Onpoint also has statisticians on staff and works regularly with statistical consultants. We understand the importance of implementing reliability testing methods for our clients prior to public reporting. For example, we recently worked with California's Integrated Healthcare Association (IHA) to assess the reliability of their Total Cost of Care reporting. Onpoint statisticians evaluated and made suggestions regarding the minimum denominators for reporting, confidence interval cut-points for the measures to be considered reliable, and appropriate truncation level for high-cost members. We also have built and implemented reliability testing and thresholds for Washington's HealthCareCompare website based on data from the WA-APCD. For Washington, Onpoint identified a set of measures within the Washington Common Measures Set

that reliably can be used to predict performance differences between providers (e.g., sufficient sample size, low measurement error). We then developed statistical methods to calculate variance, the ratio of signal to noise in the data, and thresholds that each practice result must meet to be presented reliably on the website.

Our statisticians will work with IDOI to understand the specifications and any statistical modeling required in your reporting to ensure that statistical reliability thresholds are met. We will develop code that meets the specifications to ensure that the data presented in reporting will be statistically reliable.

10.9 Describe the data formats and data languages used in the data warehouse to facilitate data exchange and presentation. Is your data warehouse compatible with all the following formats: HTML, PDF, XML, Excel, comma-separated values (CSV), and PPT?

Onpoint's Analytic Environment includes industry leading data querying, analysis, and visualization tools such as DataGrip (SQL), RStudio (R), Anaconda (Python), and Tableau, which allow users to ingest, edit, combine, and export data in nearly any format. Onpoint's Analytic Environment additionally is equipped by default with the software necessary to create and read web pages, presentations, spreadsheets, and PDFs. Onpoint's BI solution also provides prebuilt dashboards with built-in functionality to export and share important information in the various formats.

10.10 Describe your system's ability to produce interactive dashboards. Would it allow the State's users to drill down for more details on each item? Provide example screenshots.

Onpoint's reporting solutions leverages Tableau Server to provide interactive dashboards that enable filtering and drill-down by dimensions such as geographical region, provider, facility, condition or procedure, and payer. The row-level data sets used to create these dashboards also are provided to users in order to facilitate drill-down and creation of new custom reports.

IDOI users will have access to a host of interactive dashboards, example screenshots of which can be viewed above in our response to this section's Question #10.5.

10.11 Describe the analytics capabilities you provide beyond reporting.

Our analytics team is supporting the largest and most diverse group of APCD users and use cases nationally, which has afforded us the opportunity to invest our data sets with a rich and flexible suite of analytic enhancements, which are recognized by our clients as a differentiator. These enhancements are time-tested, transparent, APCD-specific tools that our clients rely on every day to make efficient and effective use of their delivered data sets. Onpoint's data enhancements include:

Onpoint provides transparent documentation for each of these enhancements to our clients and their data users. Additionally, each data set is accompanied by a detailed data dictionary and release notes that document the data set's control totals, identify any data anomalies (and their resolutions if applicable), highlight relevant differences between previously delivered data sets, and feature user notes for analysts.

As data users ourselves, Onpoint's analytics team is well suited to provide support to clients and their data users. We regularly conduct user group sessions to explain and explore new data enhancements and medical coding topics. We also provide regular direct support to those trying to learn more about how to use the data to conduct analyses.

Our analysts have a full range of analytic skills, including advanced statistical analysis and modeling, methods, and tools. Much of our analytic work is grounded in claims data and, increasingly, requires the linkage of claims data with non-claims data sources – an area of considerable experience for Onpoint. Recent data linkage projects have included the linkage of claims with clinical/EHR, public health registry, health improvement program, survey, incarceration, and social determinants of health data.

Beyond standard reporting, we also conduct analyses delivered in the form of presentations, user-friendly provider and practice profiles, special studies and reports, and research publications. We regularly collaborate with clients and other organizations to publish studies using APCD and other linked sources in peer-reviewed journals as well.

10.12 Describe your ability to provide comparative benchmarks for the State.

As noted above, Onpoint's has ready ability to incorporate public and third-party benchmark data for the State. Onpoint currently captures metadata from the 80 million covered lives that we manage on behalf of our clients, which are submitted by payers nationwide. These metadata allow Onpoint to build and maintain an array of "gold standard" data quality benchmarks that are used to validate both incoming and consolidated APCD data. One example of these "gold standards" includes comparing payer-level costs per member per month to the typical range for the same product type, with the opportunity to stratify in multiple ways (e.g., payer, product, age, gender).

For analytic purposes, Onpoint also licenses well-established, reliable benchmark data from multiple third-party sources, such as NCQA's Quality Compass® data set. We use this internally as a primary benchmarking source for comparative reporting on quality, gaps in care, and utilization (e.g., HbA1c testing for diabetes, well-child visits, inpatient utilization) as we create reporting for our clients. Quality Compass and other national benchmarks also could be incorporated into public reporting if IDOI wishes, though there may be a separate licensing fee for their use.

10.13 Describe your case-mix system's capabilities to map medical claim data into diagnostic categories.

Onpoint's solution will enhance the data and map claims into diagnostic categories using Onpoint tools developed for APCDs and third party groupers. The following data enhancements are included in our solution.

Onpoint's Service-Focused Episodes (SFE) grouper. As noted in our response to Question #10.3, our proposed solution to provide episodes of care for Indiana's APCD reporting includes a fully transparent grouper developed by Onpoint in collaboration with our clients for use in public reporting and other episode-based analyses. [redacted]

Onpoint has direct experience implementing multiple commercial episode groupers and is prepared to support Indiana in making an informed choice should it wish to supplement or replace Onpoint's SFE grouper. We have hands-on experience with the PROMETHEUS episode grouper from Change Healthcare, which we implemented for a regional business coalition; Optum's Episode Treatment Groups (ETGs), which we licensed to support a value-based purchasing initiative; and 3M's Patient-Focused Episodes (PFEs), which we have used for multiple comparative cost analyses. Depending on the use cases that the State intends to support, the considerable, added cost may or may not be worthwhile. Commercially available groupers also vary in their granularity and methods transparency so it will be important to review these trade-offs with Indiana to ensure that your overall needs are best met.

Groupers to aggregate claims into distinct condition and procedure categories. Onpoint will enhance Indiana's consolidated APCD data with All-Patient Refined Diagnostic-Related Groupings (APR-DRGs) using the state's existing license with 3M. DRGs classify hospitalizations into medical and surgical admissions, type of admission, and severity of the hospitalization. This detail allows the users of the output to case-mix adjust for comparisons across hospitals or other groupings (e.g., geographical, payer, medical system).

Onpoint will also provide output from the Ambulatory Payment Classification (APC) grouper, which groups outpatient services into bundled services based on Current Procedural Terminology (CPT) and Healthcare Common Procedure Coding System (HCPCS) codes.

[redacted]

10.14 Describe your case-mix system's capabilities to flag identified diseases and utilization patterns.

Onpoint regularly generates flags that identify a wide array of chronic conditions [redacted]

[redacted]

10.15 Describe your case-mix system's capabilities to track individuals across inpatient and outpatient settings and across databases.

One of the challenges faced by APCD vendors nationwide is providing accurate identity resolution. A signature component of Onpoint CDM is its ability to overcome challenges specific to APCD submissions and successfully generate reliable master patient and provider indexes.

Since health insurers often use multiple proprietary claims and eligibility systems that can differ across even their own products and regions, it often is difficult to track patients when they change health plans due to a change in employers, become Medicaid or Medicare eligible, or experience other life events that affect their insurance. For this reason, it is critical that the master patient index (MPI) has robust algorithms focused on the identifiers available within an APCD to develop person-specific identifiers that allow analysts to track a single member both longitudinally over time and laterally across payers and products. Onpoint's MPI has been designed to deliberately overcome these challenges using a three-phase approach that includes (1) pre-matching analysis and configurations, (2) matching algorithms, and (3) post-matching validations.

Onpoint has implemented MPI solutions for all of our APCD clients, with data collections spanning nearly 20 years, hundreds of data suppliers, and a wide range of file types. The unique identifiers assigned by our MPI solution, which covers more than 80 million patients and subscribers, have been used to successfully perform a broad array of member-level reporting and custom analytics.

Onpoint CDM's member-clustering algorithms use a combination of data elements (e.g., Social Security number, first and last name, date of birth, gender, contract number, payer-supplied member identifier) and are executed hierarchically, with the most rigorous matching requirements occurring first. Onpoint's MPI solution achieves extremely high sensitivity and specificity scores with the submission of well-populated direct identifier fields and is delivered as part of our core solution.

Members in our MPI have the same unique identifier across inpatient and outpatient settings. Members also can be linked to other available databases in the state (e.g., birth certificate, death certificate, clinical registry, program data, hospital discharge) through linkage logic when those data sources are available and contain key identifiers (e.g., first name, last name, date of birth, SSN, ZIP code).

10.16 Describe your case-mix system's capabilities to use predictive modeling to identify lead lists for case management.

Onpoint's analytics team has developed capabilities to use predictive modeling to flag members at risk for specific health outcomes, to create risk-adjusted rates, and to identify control groups for program evaluations (e.g., propensity score matching). We have generated multivariate statistical models that output predicted values since the 1990s. We work collaboratively with our clients to customize models, based on outcomes of interest and the available data types. We also use APCD

claims and non-claims measures in our models. For example, we may link in clinical measures from a clinical registry to enhance the data set or link in data from vital statistics (e.g., incarceration, birth certificate, death certificate, cancer registry). We have published the results of our studies in leading journals. Our model-building process involves a literature search, preparation of the data, testing and validation of the model, and use of the model to predict a future event. Use cases for Onpoint predictive modeling include:

- The identification of patients for future intervention scaled to the specific needs of a client (e.g., which patients should be targeted for a diabetes control intervention)
- The identification of groups of patients who would benefit from future intervention (e.g., are there areas of the state that would benefit from a mobile mental health intervention based on current risk factors of the adolescent population)
- Categorization of groups of patients for comparative analyses
- Identification of the strongest predictors of outcomes
- Evaluation (e.g., propensity score matched control groups)

For case management purposes, it likely would be important to be able to link the results of the predictive model back to a data set with patient-level identifiers (e.g., member ID). One vehicle for providing providers or payers with such data would be Onpoint's Performance Reporting Portal (PRP), a secure environment used by providers and payers across the country to view APCD data on their patients. For additional information on Onpoint's Performance Reporting Portal please refer to our response to Question #6.54 in Section 6 ("Data Services").

10.17 What data inputs influence risk scores? What types of risk scores are available? How often are risk scores updated?

Onpoint also proposes to leverage the state's license with 3M to provide Clinical Risk Groups (CRGs) to support IDOI's need to assess relative risk within a population and to predict concurrent or future healthcare costs. Our staff will work with IDOI to review the different parameter options within CRGs to best meet your needs.

CRGs are used to measure health status and are applicable to all ages and payer types. They classify each member into clinical groups based on diagnoses. Those groups can be used as-is or collapsed into a smaller number of classifications (e.g., healthy, acute or minor chronic, significant chronic, etc.). Risk categories can be used to stratify patients for analytics or can be input into risk-adjustment models. We have proposed to provide risk output quarterly.

While CRGs provide a wealth of information on classification, they do not create a specific risk score per patient. If a single risk sore is needed, Onpoint could use the average allowed amount for each of the 1,000+ CRG categories and then divide by the statewide total average per member to create a score.

If preferred, we also have the capability to run HCCs (Hierarchical Clinical Classifications), free software from CMS and the U.S. Department of Health and Human Services (HHS) to calculate patient risk scores. Another option is for IDOI to receive Johns Hopkins' Adjusted Clinical

Groups (ACGs). ACGs have additional licensing fees, but we could also provide pricing to acquire a license and use this in Indiana as well.

10.18 Describe your ability to create custom population health flags outside of the case-mix system.

Onpoint regularly creates custom population health flags outside of our standard reporting tools and tables for our clients. A few examples of recent projects for which we have created new logic to flag patients with specific conditions include:

- **Behavioral health parity.** Onpoint was contracted to deliver a study on behavioral health parity for Washington's Office of the Insurance Commissioner (OIC), which flagged patients with substance use and mental health disorders and quantified utilization and denied claims for their services.
- **High utilizers for behavioral health.** For Vermont's Medicaid Program, Onpoint delivered a study on children's mental health services, which classified children and adolescents by specific mental health and substance use disorder groupings and developed a definition for "high utilizers" within the state.
- **Seriously ill patients.** In conjunction with the Gordon and Betty Moore Foundation and researchers at the Duke-Margolis Health Policy Center, we identified seriously ill patients and evaluated their medication safety, adverse drug events, and utilization outcomes compared to the non-seriously ill population. The resulting article was published in the *American Journal of Managed Care.*
- **Evaluation of opioid use disorder treatments.** For the state of Vermont's Blueprint for Health, Onpoint conducted multiple evaluations of the state's Hub & Spoke opioid treatment model and developed profiles by treatment site. These analyses involved linkage of the APCD with clinical registry, incarceration, and other data sources as well as the design of new logic to identify patients with opioid use disorder and to appropriately classify treatments.

10.19 Describe how you translate medical coding data into user-friendly descriptions.

Onpoint's data extracts include a comprehensive series of reference tables that provide a crosswalk between medical codes and their descriptions (e.g., short description, long description) to facilitate understanding and utility of the data. Consumer-facing products designed for the general public include both the actual codes as well as summarized descriptions to avoid confusion and help audiences understand the displayed information as intuitively as possible. Additionally, we have experience developing materials for websites like Washington HealthCareCompare that highly prioritize user-friendly descriptions. We have experts on staff within our communications and analytics teams who can bridge that gap.

10.20 Describe the functionality to create and manage cohort groups based on input criteria.

Onpoint's BI tool and data marts make it easy to identify cohorts of patients and examine their cost, utilization, and quality of care. For example, an analyst might want to compare women with diabetes living in one geographical area to those living in another area and identify variation in

quality, cost, hospitalizations, and other outcomes between the areas. Our intuitive data marts and easy-to-navigate data sets make such analyses easy. We aggregate this data on key dimensions and calculates metrics to enable rapid comparisons of different populations across various dimensions such as health plan, product type, and geographical location. Users are able to tune the grouping dimensions directly within these views to focus on data points of interest and analyze trends from multiple angles.

All data [redacted] are accessible within Tableau for users to create custom cross-dimensional analyses. Users are able to build custom reports from the pre-aggregated data marts provided by Onpoint as part of Onpoint's BI Solution or directly from the detail data sets delivered with each quarterly update to the Analytic Environment. Onpoint's solution is designed for flexibility, providing displays that answer common questions while also allowing IDOI and your end users to easily develop custom analyses.

Data from the APCD and BI tool can also be linked to program data or other data sources (e.g., vital statistics, cancer registries, incarceration data, education data, healthcare exchange data, survey data) to identify a cohort and enhance the data with risk factors and outcomes.

10.21 Describe your system's capabilities for data mining for health care fraud and its ability to apply these processes over multiple providers.

Data in the standard APCD includes procedure codes, diagnosis codes, payments, and providers and is well suited to identifying issues around healthcare fraud, billing discrepancies, up-charging, and other such issues that drive up the cost of healthcare. We also have statisticians and data experts on staff and available as consultants who are familiar with data mining procedures on issues like up-coding, duplicate billing, excess utilization, and unit billing errors.

We have not specifically mined the data for fraud, but we have recently engaged in a variety of work with Washington State's Office of the Insurance Commissioner to analyze healthcare claims to identify variations in billing practices that drive up the cost of healthcare. Some recent work in this area includes analysis and reporting to support implementation of Washington State's Balance Billing Protection Act, which became effective in January 2020 and aims to protect consumers from balance (or "surprise") billing for a specific set of services and/or conditions. Among Onpoint's deliverables was a Surprise Billing Data Set using the Washington APCD. We have also worked to evaluate the impact of hospitals buying up physician practices and billing additional facility fees to try to quantify the impact of consolidation in the marketplace. Additionally, we have examined behavioral health at the payer level to identify payers who are denying claims for services that generally should be covered under law.

We also are familiar with fraud in the claims and have professional billers on staff who are aware of appropriate billing practices. In the past, we have seen and verified overbilling/fraud in our analyses. For example, in work that we undertook with Vermont State on opioid use disorder treatment, it was suspected and subsequently found that a lab in the state was overbilling for urinalysis for patients in our study. We were able to verify this in the claims data and make adjustments to our study design to allocate settlement payments. The APCD is a good source of data for these types of analyses.

10.22 What are your reporting system's abilities to include data on social determinants of health (e.g., income, education level, etc.)?

a. What data sources do you incorporate for these measures?

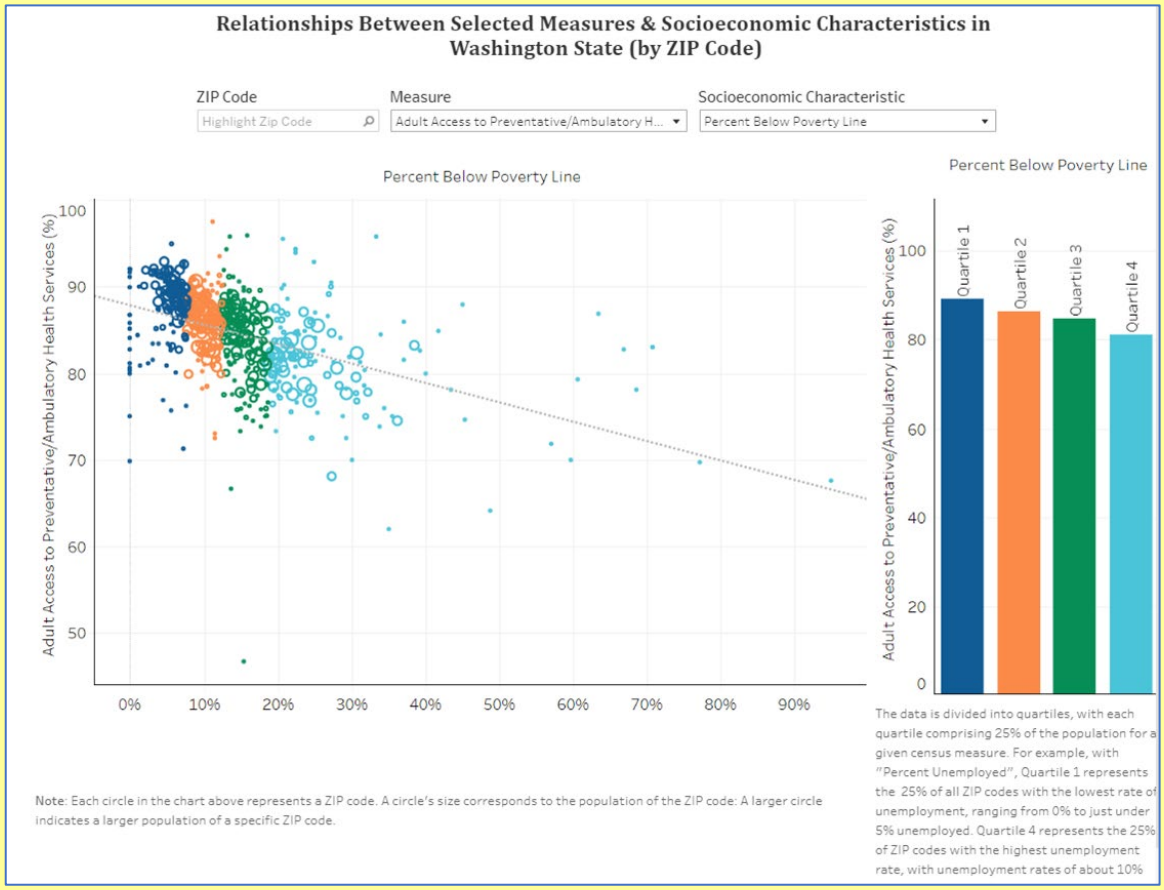
Onpoint's Analytic Services team supports a wide range of regular and ad hoc analyses requested by our clients. These requests often require the linkage of claims data with non-claims data sources such as clinical, public health registry, health improvement program, survey, incarceration, and social determinants of health (SDoH) data.

Onpoint regularly incorporates externally generated measures, including quality of care, patient experience, patient safety, and outcomes from other sources of data such as the Consumer Assessment of Healthcare Providers and Systems (CAHPS) survey, the Behavioral Risk Factor Surveillance System (BRFSS) survey, CMS Hospital Compare, linked birth certificate data, and the American Community Survey (ACS).

A recent example is the population health dashboard that we developed for Washington State, highlighted below in **Figure 10.22.A**. This Tableau-based dashboard allows users to compare ZIP-code level results from a select set of healthcare quality and cost measures, including adult access to preventive care and total cost per member per month, to socioeconomic characteristics, such as the percent of population living below the poverty line.

To visit the dashboard, please click here: https://ofm.wa.gov/washington-data-research/health-care/health-care-access-utilization-and-quality/relationships-between-cost-utilization-and-quality-measures-health-care-data-dashboard

Figure 10.22.A. Washington State Social Determinants of Health Reporting



While race and ethnicity data typically are not well populated in eligibility files, we also have worked on several projects to impute race and ethnicity from claims data using first name, last name, and Census tract data on race and ethnicity. We worked on an imputation model with the University of Connecticut, validating results of the model using sources that included birth certificate and hospital discharge data, which tend to have race and ethnicity fields well populated. We also have worked to test the implementation of RAND's Bayesian Improved Surname Geocoding (BISG) model using the voluntary multi-payer data of our California client, the Integrated Healthcare Association. Our team was able to impute race and ethnicity for nearly all patients. With the current emphasis on social determinants of health in healthcare, improvement of the submitted data on race and ethnicity as well as use of imputation models such as BISG are expected in the future.

Beyond race and ethnicity, Onpoint's Analytics team also has worked on projects to extract social determinants of health from claims data. ICD-10 "Z" codes, for example, directly identify homelessness, poverty, neglect, abuse. While many of these codes are not yet regularly populated, this is changing, and some useful information on social determinants of health is still available and useful. For the Connecticut State, for example, we have used logic to identify children who had Adverse Childhood Experiences (ACEs) based on their claims and the behavioral health claims of their parents/guardians. We also often link claims to outside data sources with better information on income, poverty, incarceration to complete our studies.

10.23 Describe your experience working with health data to provide actionable insights for your clients. Provide sample reports.

Onpoint regularly works with our clients to design analyses to provide actionable insights. Recent examples of Onpoint's APCD-based analytics include:

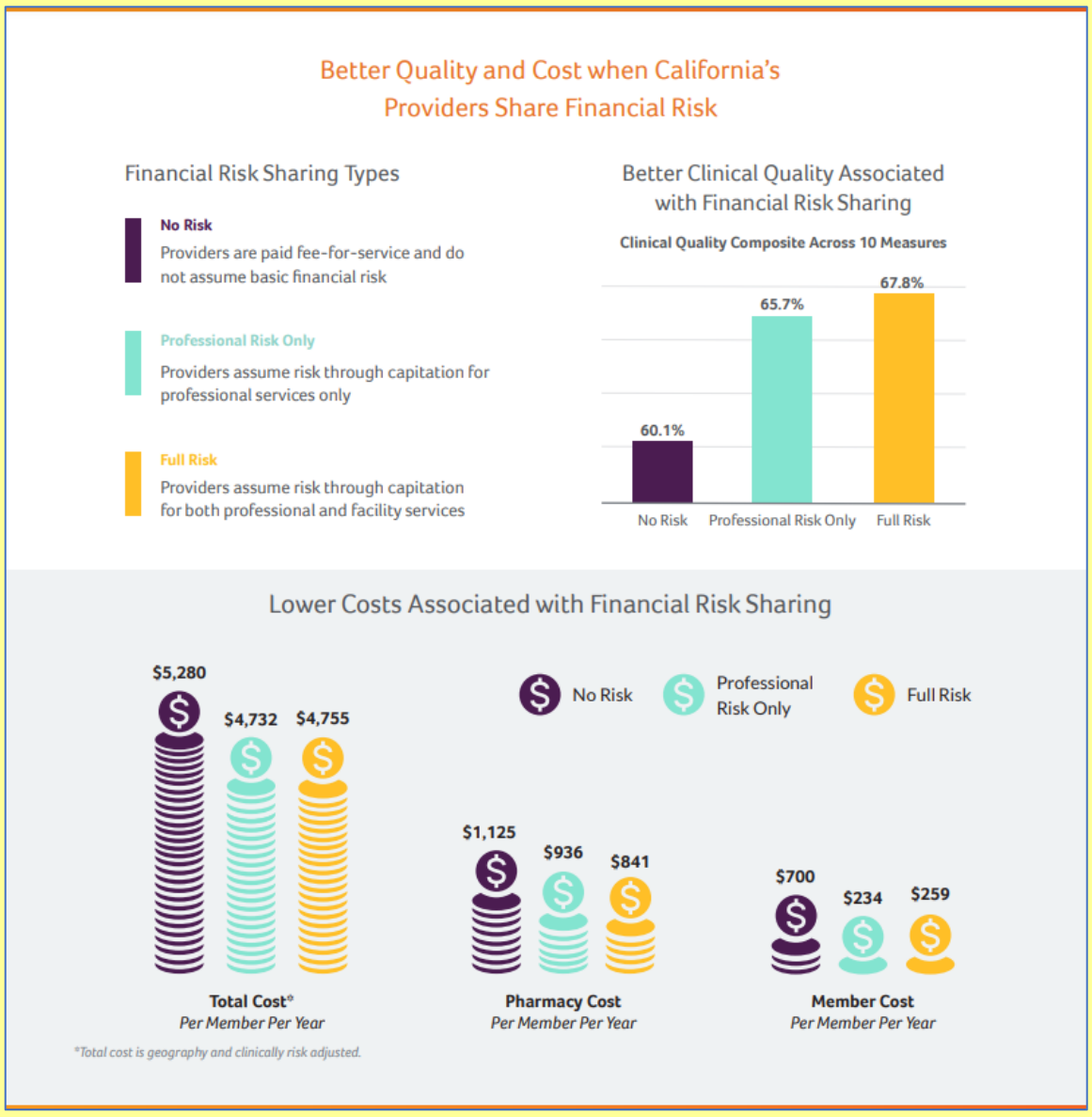
- **Policy-related work in California.** Onpoint and the Integrated Healthcare Association (IHA) have been contracted to perform analysis to support various policy-related work in California. This work includes:
  - **Covered California.** Support for Covered California's policy objective of driving to more integrated, coordinated, accountable, affordable care offerings:
    - » To inform AB 1810 report on affordability, we generated statistics of medical and pharmacy spend, member out-of-pocket costs, and risk scores for every combination of: region, age group, metal tier / actuarial value tier, and plan type.
    - » To inform benchmarks for Qualified Health Plan (QHP) contracting, we conducted an analysis with input from RAND on 15 million commercial lives to measure the variation in primary care spending across payer and product types and regions, as well as provider organizations, ACOs, and health plans; we also ran correlations of primary care spending with clinical quality, utilization, and total cost.
    - » To explore the feasibility of alternative value-based contracting options, in consultation with Elliott Fisher of Dartmouth Institute, we identified informal networks of independently contracted FFS physicians acting like a more formal provider organization by their referral patterns, and assessed the quality, utilization, and cost of the networks based on level of affiliation compared to risk-bearing organizations.
    - » To reveal opportunities for network improvements, we created QHP-specific reports to display performance of contracted provider organizations on clinical quality, total cost, and value and identify organizations in the high cost / low quality quadrant.
  - **Healthy California for All Commission.** To support the first report to the Legislature on the payment landscape in California, we analyzed the percent of costs that are capitation vs. FFS for professional services and facility services for commercial HMO and PPO and Medicare Advantage and original Medicare, by region.
  - **Gordon and Betty Moore Foundation.** In conjunction with researchers at the Duke-Margolis Health Policy Center, we identified seriously ill patients and evaluated their medication safety, adverse drug events, and utilization outcomes compared to the non-seriously ill population. The resulting article was published in the *American Journal of Managed Care.*
- **Multi-payer comparisons of cost, utilization, and quality.** Onpoint provides performance reporting across medical groups and practices in Oregon as an analytics contractor to Comagine Health, the state's voluntary all-payer claims database, for their statewide Oregon Data Collaborative and, more recently, for Oregon's Comprehensive Primary Care Plus (CPC+) initiative. Both programs rely on Onpoint's Performance Reporting Portal (PRP), which offers dynamic reporting, review and reconsideration functionality, and roster management functionality.

Related work includes performance reporting for 18 regions and 5,500 practices participating nationally in CMS's CPC+ alternative payment model as a subcontractor on the CMS Data Feedback and Reporting Tool contract.

Other work includes measurement and reporting for the Minnesota Atlas of Children's Health Care, a study of unwarranted variation in children's healthcare that leverages the state's APCD.

- **Impacts on cost and quality from various plan design characteristics.** IHA's California Cost & Quality Atlas – for which Onpoint calculates and produces results – provides variation reporting by geography, payer and product type, and payment design characteristics. Users can easily apply desired filters in order to compare cost and quality across regions by product type, for ACO vs. traditional PPO and HMO plans, as well as by type of provider risk sharing (**Figure 10.23.A**).

Figure 10.23.A. California Cost & Quality Atlas Financial Risk-Sharing Infographic



- **Support of cost growth benchmarking initiatives.** Onpoint has been supporting Washington's Health Care Cost Growth Benchmarking work through the development of dashboards showing trends in cost by category within the state and analyses of truncation points for high cost outliers.

Other types of health policy decision support using APCD data. Onpoint also recently generated a new and innovative multi-state analysis for the New England States Consortium Systems Organization (NESCSO) that involved Onpoint's integration of data from all six New England states' APCDs to assess the percentage of overall healthcare spending being invested in primary care services based on claims data for 7.2 million commercial, Medicaid, and Medicare members. This report, which was released in January 2021, was aligned with parallel work in California noted above.

10.24 What recommendations do you have to improve the public health understanding of epidemiological analyses?

Onpoint aims to provide data and tools for our clients to analyze their data. Additionally, we provide analytical support to our clients in the form of special research studies, program evaluations, and ad hoc reporting. Epidemiological analyses can be complicated, and sometimes the meaning can get lost in the details. One of our goals is to provide our clients and their stakeholders with actionable data and insights that can transform public health and healthcare. This starts with clear communication of study results. We recommend straightforward studies wherever possible, use of plain language, and vivid, intuitive visualizations, each of which aid in the communication of results to the public and to less technical stakeholders. We also recommend the use of transparent tools whenever possible, with clear methods instead of black-boxed solutions. We start each project by discussing the objectives with the client: Who is the audience for the results of the study? What end product will be best able to reach them? What presentations or reports will be required? By starting with these questions, we find that we are better able to design the research outputs in a way that will be more readily understood by the audiences.

10.25 What experience do you have conducting epidemiological analyses on similar data?

Onpoint has provided research design expertise, statistical modeling, and data preparation for a wide array of studies using APCD data during recent years. A few examples of our work include:

- **Evaluation of patients receiving Medication Assisted Treatment (MAT) for opioid use disorder (OUD) compared to other treatment**. This study used administrative claims data based on a five-year longitudinal cohort. The study identified 6,700 patients with OUD receiving MAT and 1,186 patients with OUD receiving other treatment that could be tracked in the APCD claims. We linked incarceration data for five years between 2014 and 2018 and examined the overall rate of adverse opioid events during those years.
- **Evaluation of Integrated Community Care Management (ICCM) Program in Vermont.** ICCM patients were matched to a control group using propensity score matching. A difference-in-difference analysis compared ICCM outcomes to outcomes of other patients to examine emergency department use, cost, and hospitalizations between the two groups.

- **Evaluation of spending on primary care and cost and quality.** This analysis used data from nearly 14 million commercially insured adults in California to examine variation in the percent of healthcare dollars spent on primary care for different products (i.e. EPO, HMO, PPO) offered by health plans with quality, utilization, and total cost of care. Correlations between increased spending on primary care and improved outcomes and lower cost were observed.
- **Study of diabetes co-morbidities on total cost of care.** This analysis examined variation in healthcare expenditures vs. a measure of disease control (i.e., most recent glycated hemoglobin [A1C] test results). Multivariable linear regression calculated the relative impact of a series of risk factors on medical expenditures. Poisson regression estimated the relative impact on inpatient hospital admissions. Possible savings were estimated with a reduction in potentially avoidable hospital admissions.

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

11.1 Confirm your understanding of the Billing & Invoicing, Corrective Action, and Payment Withholds structure outlined in the Scope of Work.

Onpoint confirms our understanding of the billing, invoicing, corrective action, and payment withholds structure outlined in the Scope of Work.

11.2 Describe any problems and failures that you encountered in delivering services similar to the services requested in this RFP, how these were resolved, and what were the lessons learned.

Problem encountered: Onpoint was engaged to support the development of an APCD for the state of Tennessee, which never completely got off the ground. The state's data collection regulations were so restrictive from a privacy standpoint that we were unable to build a reliable master patient index (MPI). A reliable MPI is an essential ingredient to any all-payer longitudinal analysis – analyses that allow an analyst to follow a patient over time and across health plans – which is critical to the types of studies that Tennessee, like other APCDs, had in mind when building its APCD.

The limits embedded in the state's collection rule meant that all personally identifiable information (PII) had to be hashed (i.e., irreversibly rendered into meaningless 128-character strings) by payers prior to submission, and included only fields for first name, last name, and gender. An essential element of any MPI, date of birth, had to be transformed into age in months and then entirely removed prior to submission. Onpoint was left with only gender and hashed first and last names, which could not be standardized or cleansed prior to hashing by submitters, making it impossible to create reliable unique patient identifiers. This fundamental flaw in the APCD severely limited its utility and the state was unable to address the limitations of its collection regulations.

Lessons learned: First and foremost, there are essential components of an all-payer claims database that must be in place to ensure utility, including a reliable MPI. While Onpoint was engaged prior to the finalization of Tennessee's collection regulations, we were unable to

effectively convince them that the compromises they were making with privacy interest groups would undermine their ability to meet the state's most fundamental information needs.

This experience taught us the importance of working with APCD clients up front, whenever feasible, to ensure that the essential building blocks are in place for a successful APCD program, including data collection requirements that allow the development of a reliable MPI. We work collaboratively with clients – both during implementation and ongoing – to ensure that program and policy decisions are informed by the technical implications of such decisions, including any impact on the utility and usability of their APCD.

There have been other, less impactful problems that Onpoint has encountered with other APCD programs where mitigation opportunities were available, including those summarized below.

Problem encountered: The Supreme Court's 2016 Gobeille ruling resulted in a significant loss of ERISA self-funded plan data in state-mandated APCD programs. The loss of self-funded commercial claims data has ranged from 25% – 40% in state APCD programs based on Onpoint's review of data submissions received before and after the ruling.

Lessons learned: The strength of the relationships with key stakeholders within a state, including health plans and the business community, is key to capturing self-funded data on a voluntary basis. The best approach, in our experience, is to demonstrate the value of the APCD to these stakeholders. Engaging around this value proposition has the potential of securing voluntary participation in the APCD and expanding the commercial data available for analysis.

Of note is that some public self-funded plans – those covering state and municipal employees and educators, for example – fall outside these ERISA self-funded restrictions and thus are available for collection within the APCD.

Problem encountered: Limitations of cost fields in claims file submissions from health plans that capitate certain services or supplement total fee-for-service payments through other alternative payment models (APMs) must be addressed to accurately measure and report on healthcare costs. As capitation and other APMs expand in many markets, with the objective of shifting risks from health plans to provider organizations, it is important that clear guidance on submission specifications be provided and accompanied by appropriate training for technical staff from health plans that administer capitation and other APMs.

Lessons learned: A supplemental cost file containing member-level cost information has been an effective solution to collect capitated and other APM costs that are not captured in the claims files. National standards are not yet available but are currently under development and should be followed, if possible, by Indiana in its implementation. In addition, data quality validations need to be in place to identify any inadequate or inaccurate reporting of cost fields at the field and file levels.

12. Optional Questions

12.1 Are there any changes to State law that would increase the functionality and effectiveness of the database? If yes, include a recommendation of the statutes and necessary changes.

Onpoint's experience working with states to implement and operate well-functioning APCD programs offers key insights and lessons learned in developing effective statutes and rules, including the following:

- **Establish clear submission requirements.** To ensure complete, timely, and reliable submissions from participating plans, it is important to provide clear requirements regarding the file types to be reported and the timing of those submissions. We currently work with clients that allow for semi-annual or even annual submissions that may vary by file type – a cadence that we have found to be less than optimal for analysts. To keep the APCD's data products and analyses as current as possible, we recommend a monthly cadence for submissions, which enables early detection of data quality issues and, ultimately, more frequent data refreshes.
- **Establish a threshold for participation.** To avoid confusion among health plans, it also is important to establish a clear threshold for mandatory participation. The most common approach is to set a covered lives threshold – that is, a quantity (e.g., 3,000) of in-state residents covered by a health plan licensed in the state. The specific threshold can be determined by evaluating what threshold would be required to capture a certain percentage of the state's fully insured population (typically at least 80%, including Medicaid and Medicare).
- **Identify the universe of required registrants.** While some states require annual registration of only those plans flagged for participation in the APCD, others require all health insurers doing business in the state to register annually even if they do not meet the threshold for mandatory participation. This broader list of insurers typically is identified by the state's Department of Insurance. If a threshold is set for participation, an annual registration process that includes all health insurers doing business in the state would help identify both new insurers and any insurers whose book of business has grown to newly meet the threshold.
- **Include the collection of unencrypted direct identifiers.** Onpoint has implemented APCDs for which we collect either unencrypted direct identifiers or hashed/de-identified member information. We would recommend that IDOI collect unencrypted direct identifiers since doing so enables the development of a much more reliable master patient index within the APCD. Being able to reliably track patients across health plans, providers, and time is fundamental to many population-based analyses.
- **Do not enact an opt-out option.** Our team has implemented an APCD that incorporates an opt-out option, allowing members to visit a website and remove their claims and demographic data from the APCD. This is a typical requirement of a health information exchange but, to our knowledge, has not been incorporated by any other state as a requirement related to its APCD. An opt-out provision requires extensive administrative resources to handle requests either through a website or state agency and introduces unwelcome variability and data loss to the APCD.
- **Establish clear compliance authority.** While most health plans voluntarily comply with participation and submission requirements and schedules, there are times when it is necessary to enforce stricter adherence to the APCD's collection rule. While the state's APCD data vendor can encourage and provide technical assistance as much as reasonably possible, enforced compliance, including the authority to issue fines, is the realm of the state and should be outlined in the regulations governing the APCD. This practice provides "teeth" and ensures that all parties are on the same page regarding requirements, consequences, and any appeals process.

- **Keep layouts and file specifications outside of collection regulations.** Some states have embedded their APCD file layouts and field-by-field thresholds in their regulations. This is not recommended. Locking the layouts into legislation creates significant challenges to adapting file and field specifications as needs change, interests evolve, and new fields and file types become available. A best practice in designing an APCD is to have the ability to be responsive to industry changes, legislative changes like surprise billing, and unplanned events like the COVID-19 pandemic – changes that can be hindered if they require legislative approval and updates to take effect.
- **Establish a clear data governance process, including release regulations.** It will be important to provide a framework for which data elements are available for release and for which purposes. This framework will inform the design of releasable data products. Onpoint has constructed a wide array of data products with a range of variables – unencrypted vs. encrypted identifiers, identified provider information, null vs. full provider payment amounts (i.e., protected financial information), complete vs. truncated ZIP codes and service dates (HIPAA Safe Harbor rules, etc.) – to meet our clients' varying needs. Approving the release of these data products is the purview of the state and most often is done through a data governance/release committee. Often comprised of stakeholders from both state and private sectors, these committees typically review and arbitrate data requests, assess fees, and implement data use agreements and other necessary administrative steps to ensure that data recipients understand any restrictions on their use and release of the data and their analyses.
- **Allow flexibility in the design and distribution of APCD data products.** APCD use cases and users will evolve over time as interests change and new markets emerge. The APCD's collection and release rules should enable the data products to be nimble and adapt to such changes. There may be some data products that would benefit from the inclusion of sensitive data (e.g., reporting patient-level performance measure results to providers), while others (e.g., a public-facing website) would preclude such release. The founding legislation should empower the IDOI to make such decisions based on input from stakeholders and the market.

12.2 Do you have any other comments relevant to the implementation of a robust and transparent database?

As Indiana prepares for the establishment of a robust and transparent APCD solution, beyond the recommendations and background provided above, Onpoint offers the following additional guidance:

- **Transparency in business rules.** The transparency around the technical details underlying Indiana's APCD solution will be an important factor in building trust both in the data itself and in the analytic enhancements that increase the utility of the APCD for end users. Indiana's data administrator should be prepared to provide transparency around the business rules and/or logic associated with the following processes or value-add elements, for example: Data quality validations, claims consolidation, identity resolution, categorizations or groupings, and performance measures. Many vendors "black-box" their business rules and methodologies or rely primarily on commercial grouper output, which can raise questions and concern among analysts and researchers who need to understand how to use the data reliably.

- **Integration of non-claims data.** Choosing a nimble partner and a flexible technology platform is a major component of a successful implementation. As Indiana's APCD matures and new types of data become available, the State may find that your data and analytic needs evolve and that your user base has varying interests. A technical partner with a data integration platform able to infinitely scale and easily integrate new data sources, and one that delivers an end-to-end solution that leverages the most contemporary technology, will most easily address the state's inevitably changing requirements.
- **Value of cross-client collaboration.** Many APCD programs have an interest in cross-state collaboration. Onpoint's large APCD client base allows us to support this interest, including:
  - Sharing lessons learned that can be applied to all APCD clients (e.g., data issues encountered in one state can be applied to all states, data enhancements that improve usability can be shared by all state APCDs, etc.)
  - Engaging with other APCD programs to jointly address areas of interest such as analysis of common policy issues, benchmarking, and standards development (e.g., alternative payment model data, collection standards, compliance, enforcement)
- **Cultivating a vibrant user community.** A vital component of ensuring the state's APCD end users' success is providing the necessary analytic support to allow them to make effective use of the data resources and powerful tools available. A vibrant user community that includes users both within and outside state government is often a marker of a successful data initiative, in our experience. Onpoint has worked actively to support an active user base through:
  - Enabling self-service access to data resources and tools
  - Training in the content and appropriate use of APCD data
  - Training in data querying and visualization tools
  - Providing documentation to support effective data use
  - Dedicating resources to prepare for and facilitate user-group meetings
- **Nonprofit vs. for-profit status of the vendor.** The corporate structure of the state's data administrator is an important consideration from a trust, collaboration, cost structure, and transparency perspective. For this reason, many states place a high priority on selecting a vendor with nonprofit status to implement or maintain their APCD, underscoring the state's interest in having their data managed independently of commercial interests and agenda. Nonprofit organizations are mission-driven, their finances are transparent, and they share the state's focus on supporting the public good, with any organization profits reinvested into furthering that objective.

12.3 Do you recommend collecting data from the following sources? Explain.

Children's Special Health Care Services (CSHCS)

Ryan White Program

Children's Health Insurance Program (CHIP)

Federal Employee Health Benefits Plan (FEHBP)

Indian Health Service (IHS)

Medicare Advantage

Medicare Part D

Medicare Supplement

Veterans Administration (VA)

Among the data sources identified by the State for potential inclusion in the APCD, all could be integrated if they are available. Onpoint supports the idea of expanding the population available in the APCD as much as possible. With more comprehensive data, the APCD will be even more useful and valuable as an analytic resource.

The issue for a number of these sources will be availability. Those sources for which access is controlled by the federal government – the Federal Employees Health Benefits (FEHB) Program, the Indian Health Service (HIS), and the U.S. Department of Veterans Affairs (VA), for example – will be very challenging or impossible to obtain, in our experience. Programs that are administered by Medicaid, such as Children's Special Health Care Services (CSHCS) and Children's Health Insurance Program (CHIP), could easily be incorporated within the Indiana Medicaid enrollment and claim file submissions.

Based on our experience in other APCD markets, Onpoint provides the following feedback and recommendations on the collection each of these data sources:

- **Children's Special Health Care Services (CSHCS).** Onpoint anticipates that CSHCS data would be collected through and/or submitted by the State's Medicaid program. It would offer valuable insight into services utilized by children with serious, chronic medical conditions in Indiana.
- **Ryan White Program**. Onpoint would recommend collecting Ryan White program data as it could offer insight into HIV-impacted populations and related health outcomes, help identify areas in Indiana where intervention and education could be beneficial, help understand comorbidity of HIV with chronic health issues, and help understand the intersection of HIV with other public health emergencies, such as COVID-19. Onpoint has experience securely handling this type of sensitive data.
- **Children's Health Insurance Program (CHIP).** Onpoint anticipates that CHIP data would be collected and submitted to the APCD by the State's Medicaid program, which is the typical approach in other state APCD programs. This population of lower income children and pregnant mothers is an important population for which to understand the utilization, access, and quality of care.
- **Medicare Advantage.** Medicare Advantage data typically is a standard data source for APCDs in other states, is submitted by commercial insurers, and would be important for understanding the quality and cost of services being delivered in Indiana. Medicare Advantage represents a large and growing share of the Medicare population overall. In Indiana, more than 350,000 Hoosiers are enrolled in Medicare Advantage plans.
- **Medicare Part D.** Medicare prescription drug data is typically a standard data source for APCDs in other states, is submitted by commercial insurers, and would be a valuable and important addition in Indiana. An understanding of prescription drug costs and utilization

rates for the more than one million Indiana Medicare beneficiaries who have Part D prescription coverage will be critical for the state of Indiana.

- **Medicare Supplement.** Onpoint would not prioritize collecting Medicare Supplemental plan data as it can complicate many analytic use cases and would be costly to integrate relative to the benefits that it offers. Medicare Supplemental coverage complements Medicare FFS coverage, which already will be captured in the APCD; therefore, the utilization and full cost of healthcare services also already will be captured in the APCD.
- **Federal Employee Health Benefits Plan (FEHBP).** Onpoint's experience in other markets is that the federal government has been unwilling to provide claims data for the Federal Employee Health Benefits Program population to APCD programs. While we would be surprised if the FEHBP would approve release to the Indiana APCD, it certainly would be valuable to have this population represented in the database if available.
- **Indian Health Service (IHS).** Onpoint would recommend collecting Indian Health Service data if Indiana has a mechanism for compelling the IHS to supply the data to the APCD. This data historically has not been provided to APCDs in other states. Onpoint would be interested in working with the State to integrate Indian Health Service data, if available, as IHS data can provide valuable insights into an underserved population that is rarely available in an APCD.
- **Veterans Administration (VA).** Onpoint's experience in other markets is that the federal government has been unwilling to provide claims data for the Veterans Administration population to APCD programs. While we would be surprised if the VA would approve release to the Indiana APCD, it certainly would be valuable to have this population represented in the database.