**Statement of Work**

State is seeking a cost-effective solution that integrates with internal systems and data sources to enable compliance with the interoperability requirements described in the CMS *Interoperability and Patient Access Final Rule* (CMS-9115-F). The solution must also be flexible enough to support future business requirements and regulatory changes.

**Patient Access API**

1. Minimum Functional Requirements
* Solution must be compliant with the Patient Access API described in the CMS Interoperability and Patient Access Final Rule (CMS-9115-F)
* FHIR API System Requirements
	+ Cloud-hosted or on premise hosted FHIR API server supporting the latest FHIR version required by CMS regulations
* Make available source data for claims, encounter, clinical data (based on USCDI v1+) and drug formulary data using CMS recommended publicly available implementation guides
	+ Data may reside in an existing data store or may be Extracted\Transformed\Loaded to a different data store using approved, secured, and supported technologies
	+ FHIR API will be tested with industry best practices, approved test cases, and testing guidelines provided by CMS
* Data Maintenance Timeframes
	+ Data for drug formulary are updated monthly no later than thirty (30) calendar days
	+ For drug formulary data, no later than one (1) business day after the effective day of any such information or updates to such information
	+ No later than one (1) busines day for adjudicated claims, and no later than one (1) business day after receiving encounter and clinical data
	+ With a date of service on or after January 1, 2016 for active eligible individuals
* Claims and Encounters
	+ Must include all covered services to the extent the CMS recommended Implementation Guides (*CARIN Alliance Blue Button® Framework and Common Payer Consumer Data Set (CPCDS) IG)* reflect them. Ultimately, claims and encounter data for all covered services including behavioral health, long-term supports and services, dental and other claims and encounter data to which the individual has the right to access will be available.
	+ Must include claims data for payment decisions that may be appealed, were appealed, or are in the process of appeal
* Testing and Monitoring
	+ Conduct routine testing and monitoring, and modify as appropriate to ensure API functions properly per the CMS mandated testing script guidelines
	+ Verify an individual or authorized representative can only access claims/encounter data or other protected health information that belongs to that individual
	+ Provide documentation and implementation of best practices regarding API testing tools
	+ Provide traffic throughput metrics to validate expected traffic load
* System will meet 99.9999% uptime and availability requirement
1. Minimum Documentation Requirements
* API Documentation is publicly available and will include:
	+ API syntax, function names, required and optional parameters supported and their data type, return variables and their types/structures, exceptions and exception handling methods and their returns
	+ The software components and configurations an application must use in order to successfully interact with the API and process its response
	+ All applicable technical requirements and attributes necessary for an application (SMART on FHIR or otherwise) to be registered with any authorization server(s) deployed in conjunction with the API
	+ Address client data contained\maintained within documents or other disparate data sets (faxes, pdfs, etc.)
	+ Address how the API will be registered so that applicable SMART on FHIR applications may discover the API
* All documentation related to a successful deployment
* Documented plan for ongoing maintenance and testing
1. Beneficiary Education
* Develop accessible, culturally competent educational materials about privacy and security considerations when selecting applications in the appropriate languages
1. Identity Management and Consent
* Support individual identity verification and authentication via OAuth 2+ and OpenID Connect
* Support SMART on FHIR authorization process
* Provide customer service support for individual questions and trouble-shooting
1. 3rd Party Support for SMART on FHIR Applications
* Registration and on-boarding process for 3rd party applications to connect to the Patient Access API
* See also requirements for API Documentation
* 3rd Party attestation process that obtains information about a 3rd party application’s privacy policy and shares that information with individuals
* Security risk assessment of 3rd-party applications to evaluate and approve access to State’s API
* Ability for State administrators to revoke or discontinue API access
* Customer service support for 3rd party developer questions and trouble-shooting
* Dedicated developer portal or “sandbox” for 3rd-party developers to test with sample data

***Please note the S-TAG Interoperability Workgroup is proposing that some or all of the above activities highlighted in yellow be pursued as a multi-state collaborative.***

**Provider Directory API**

1. Minimum Functional Requirements
* Solution is compliant with the Provider Directory API described in the CMS Interoperability and Patient Access Final Rule (CMS-9115-F)
* FHIR API System Requirements
	+ Cloud-hosted or on premise -hosted FHIR API server supporting the latest version recommended by CMS
	+ Makes available source data for physician and pharmacy network using publicly available and CMS recommended or required Implementation Guides
	+ Provider and pharmacy network data will be updated within 30 calendar days of change
* Solution will meet 99.9999% uptime and availability requirements
1. Provide an overview of your solution architecture and describe how it supports the CMS Final Rule and the requirements outlined in the RFP – specifically the:

a. Patient Access API

b. Provider Directory API

1. Describe up to two (2) case studies with an existing customer that demonstrates your experience with implementing a FHIR-based solution that connects with 3rd-party applications for claims, encounters, and/or clinical data. What are some challenges, best practices and lessons learned that we should consider in our implementation?
2. How much of your solution is owned and performed by your company, and which components or services are subcontracted to another company? If any subcontractors or 3rd-party applications are used to fulfill the requirements of your solution, please identify them by their company and application name, and their contribution to your solution. Describe your experience working with each subcontractor or 3rd-party application.
3. Describe your direct experience with each of the following FHIR interoperability initiatives, including how your solution supports each initiative (if at all) and how your solution builds on that experience?

• CMS Blue Button 2.0

• Da Vinci Project

• CARIN Alliance

• Argonaut Project

1. Describe your overall hosting and deployment options, and what are the pros and cons to each option?
2. For cloud-hosting, what cloud vendor(s) does your solution currently support and where is the data center located?
3. Briefly describe how your solution is built to support future needs and growth, and can scale in a cost-effective way without compromising performance. What is the largest production environment that your solution currently supports – such as total number of lives in your FHIR API solution, size of data managed, supported transactions per second, etc.

**DATA**

1. Does your solution support FHIR Facade or Repository data model (or both) – i.e., does your solution store a full copy of the source data and make that available, or does it connect to a data source and transform it into FHIR on request? What are the pros and cons to each option?
2. Describe your experience converting claims and encounter data to the FHIR standard. What FHIR implementation guides do you support for claims, encounters, clinical, formulary and provider directory data? Can you supply your testing results to confirm solution conformance to the Da Vinci implementation guides?
3. Does your solution have pre-built or out-of-the-box FHIR adapters for claims and encounter data? If yes, what data formats and standards are supported?
4. Can your solution support FHIR conversion from documents and unstructured data? For example, if clinical data is stored in documents such as PDFs and scanned images – shared by providers as part of the care coordination and prior authorization process.

**IDENTITY AND ACCESS MANAGEMENT**

1. We do not currently have an online member portal that handles identity verification and authentication. Describe how your solution supports the identity verification and authentication process, include login options, and support for two-factor or multi-factor authentication, OAuth, and OpenID Connect.
2. Describe a case study with an existing customer that demonstrates your experience with implementing an identify management process.
3. What customer support do you provide if individuals have questions or problems with the authentication process?
4. Describe your consent management approach and options that are supported, including how individuals are informed and how consent can be obtained, stored and modified (i.e., revoked) by them.
5. What customer support do you provide if individuals have questions or problems with the consent process?
6. Describe a case study with an existing customer that demonstrates your experience with implementing a process for individuals to authorize and manage their consent with 3rd-party applications and their healthcare data. What are some challenges, best practices and lessons learned that we should consider in our implementation?

**THIRD PARTY APP DEVELOPERS**

1. Describe your 3rd-party application registration and onboarding process, including key steps that each 3rd-party application must follow and specific information, tools, discovery, resources and other support available to help a 3rd-party developer connect to and register with the Patient Access API.
2. Does your solution currently connect to and support 3rd-party applications, including consumer-based mobile applications, health plan applications, SMART on FHIR applications, and/ or provider-based applications? If so, list the application name, company name, and the application’s primary function.
3. What customer support do you provide if 3rd-party developers have questions or problems with the Patient Access API or the Provider Directory API?
4. Describe a case study with an existing customer that demonstrates your experience with 3rd-party applications connecting to your solution via FHIR API.

**COMPLIANCE AND SECURITY**

1. Does your solution meet the following (yes/ no):

a. HIPAA compliance

b. SOC 2 Type certification

c. HITRUST certification

1. What are the most common or most significant threats to unauthorized access to the FHIR API Server, and how does your solution specifically prevent or mitigate those security threats?
2. Have you or your direct affiliates had any security breaches in the last five years? If so, please describe.
3. Do you conduct security risk assessments of 3rd-party applications seeking to connect to your solution? If so, describe your assessment process and resources – including assessment tool and criteria to approve/ deny access, and criteria to discontinue access.
4. How does your solution allow administrative users the ability to revoke or discontinue API access?
5. Does your solution or support services include off-shore access to PHI? If so, describe the extent and purpose of such access, and how data security and privacy will be protected.

**IMPLEMENTATION PLAN AND RESOURCES**

1. Describe and include a copy of your proposed implementation plan, including details on

a. key tasks

b. the sequence of those tasks

c. dependencies between tasks, if any

d. responsible parties for each task – vendor, subcontractor, or State

e. estimated time to complete each task

f. key milestones and deliverables

1. What are the expected roles and responsibilities of staff from both your organization and the State related to project management, communication and issue resolution? Specifically list start-up requirements and support that the State will be required to provide for successful project delivery.
2. What are the qualifications and experience of the staff you plan to use for implementation? Provide the name, title and resume of the primary person responsible for ensuring that goals and objectives are met.
3. Do you offer a “Proof of Technology” (POT) option prior to a full implementation – to allow the State to engage with your company to test and confirm the functionality of your solution before committing to a long-term agreement? If so, please describe a POT project.
4. The State is targeting\_\_\_\_\_\_\_\_\_\_\_\_\_ to start implementation with a selected vendor. What is your ability to support this start date? If your company and solution are selected by other States or health plans during this same timeframe, describe your staffing capacity to expand and support us as well as other potential customers?

**TESTING**

1. What is your testing process to ensure:

a. The FHIR API Server is available and connecting properly to 3rd-party applications

b. Individual members can only access data that belongs to that individual only

**TRAINING**

1. Describe your training approach and knowledge transfer to State staff. List all training and/ or educational courses offered and their schedules, including end-user and IT related offerings. Please identify courses that are mandatory, recommended or optional – and which ones are included as part of this proposal.

**ADMINISTRATIVE CAPABILITIES**

1. What administrator dashboard and reporting capabilities are built into the solution – including, but not limited to, viewing API logs and data activity, member consent and business analytics.

**OPERATIONS**

1. After implementation and Go-Live, how will you monitor progress and performance on this account?
2. Describe the workflow process for managing ongoing support and services between your organization and the State. How do you support changes to the solution, including system upgrades and enhancements, and additional regulatory requirements in the future? For example, business requirements may change based on additional regulations, and standards such as FHIR, OAuth, OpenID Connect, and USCDI may be updated.
3. What Service Level Agreements (SLAs) will you provide and how will they be measured and reported. Include an example of your standard SLAs in your contracts, as well as proposed SLAs specific to this proposal. SLAs should include both incentives and penalties for performance thresholds that customer support do you provide if 3rd-party developers have questions or problems with the Patient Access API or the Provider Directory API?