STATE OF TENNESSEE
Division of TennCare, Office of Program Integrity

REQUEST FOR INFORMATION
FOR
Medicaid Non-Emergency Medical Transportation (NEMT) Credentialing, Auditing, and Complaint Management Solution

RFI # 31865-00709
October 10, 2022

1. STATEMENT OF PURPOSE:

The State of Tennessee, Division of TennCare (TennCare), Office of Contract Management (OCM) issues this Request for Information (RFI) to gain deeper insight into the blockchain solutions available to meet TennCare's needs related to online credentialing, auditing, and complaint management of Tennessee's Medicaid Non-Emergency Medical Transportation (NEMT) benefit. TennCare is seeking information and insight from experienced vendors via this RFI to help identify the industry best practices, approaches, and technologies. This information may aid in organizing requirements for a formal procurement. TennCare appreciates all input and participation in this process.

This RFI is intended to identify technology solutions in the market that meet the following needs:

- Provide a web-based platform that employs blockchain technology to include a credentials repository, an audit tool capable of measuring compliance in real-time, and a complaint intake, referral, and management system for transportation providers, transportation brokers, and MCOs
- Establish a collaborative credentialing network among NEMT transportation providers (TPs), NEMT brokers, managed care organizations (MCOs), and TennCare
- Standardize unique NEMT transportation provider, NEMT transportation broker, managed care organization and TennCare credential taxonomies
- Provide blockchain infrastructure to establish provenance of all credentials, render them immutable, and permanently traceable
- Utilize blockchain technology to establish credential chain-of-custody and primary source verification
- Facilitate web access and secure online transmission of credentials between NEMT transportation providers, NEMT transportation brokers, managed care organizations, and TennCare
- Create an approach for converting historic and future credentials into electronic records

- Provide a platform that offers tools to set and/or change the audit criteria, to perform real-time compliance checks, to automate auditing processes and to receive, triage, escalate, and monitor trends of complaints received against NEMT transportation providers, NEMT transportation brokers, or managed care organizations.
- Ensure credentialing processes and infrastructure support national accreditation standards by the Non-Emergency Medical Transportation Accreditation Commission (NEMTAC)
- Ensure technology tools meet CMS and healthcare security standards
- Provide credentialing, technical, and customer support services to ensure NEMT transportation provider, NEMT transportation broker, managed care organization, and TennCare access to help desk and trouble shooting issues with the platform

This RFI is intended to identify blockchain technology solutions in the market that demonstrate the capacity to meet TennCare's NEMT objectives:

- Reduce administrative burdens across NEMT transportation providers, NEMT transportation brokers, MCOs, and TennCare
- Reduce credentialing costs for NEMT transportation providers, NEMT transportation brokers, MCOs, and TennCare
- Improve speed and thoroughness of audit capabilities
- Promote proactive compliance checks among NEMT transportation providers, NEMT transportation brokers, MCOs, and TennCare
- Promote collaborative credentialing among NEMT transportation providers, NEMT transportation brokers, MCOs, and TennCare
- Adopt tools to intake, triage, refer and/or escalate TennCare member complaints against NEMT transportation providers, NEMT transportation brokers, and MCOs
- Adopt tools to fight fraud, waste, and abuse
- Improve the quality of NEMT services in communities across Tennessee
- Highlight and recognize high-performing NEMT transportation providers, NEMT transportation brokers, and MCOs
- Establish a centralized credentials repository

2. BACKGROUND:

The State of Tennessee's Medicaid program provides health care for approximately 1.4 million Tennesseans. Non-Emergency Medical Transportation (NEMT) is a Medicaid benefit that supports the overall health and wellness of beneficiaries by providing transportation to individuals that require assistance getting to and from healthcare services and other locations where services are provided that support the beneficiary's wellbeing. TennCare maintains partnerships with Amerigroup, BlueCross / BlueShield of Tennessee, and United Healthcare to administer Medicaid NEMT services in the State. These Managed Care Organizations (MCO) utilize Southeastrans and Tennessee Carriers for broker services that include management of over 125 transportation providers (TP) and coordination of service delivery to communities across the State. Together, these organizations constitute a team responsible for safe and effective Medicaid NEMT service delivery in Tennessee. To ensure safe and effective NEMT services, these organizations complete a compliance process designed to set minimum standards and to hold all stakeholders responsible for maintaining high-quality operations.

One component of this compliance process is credentialing. NEMT credentialing consists of the collection, review, and audit of credentials that represent the qualifications of transportation providers, drivers, and vehicles utilized to render NEMT services. Some examples of credentials include drivers' licenses, driver training certificates, background checks, drug screenings, motor vehicle records, business licenses, vehicle registrations, vehicle inspections, insurance coverage, and sanctions and exclusions checks. Transportations Providers are responsible for compiling credentials that fulfill the requirements outlined in their contracts with brokers. These credentials are submitted to brokers who are responsible for reviewing them for completeness and accuracy. In turn, MCOs and TennCare manage compliance by auditing the credentials maintained by brokers. The credentialing process is repeated on a yearly basis and credentials must be verified and any expiration of credentials or violations of credentialing requirements must be addressed. This process is designed to ensure that the driver, vehicle, and support team for every NEMT ride delivered in Tennessee meets the competency and safety standards deemed necessary to protect beneficiaries and minimize opportunities for fraud, waste, and abuse of Medicaid benefits.

Another component of TennCare's compliance process is auditing. NEMT auditing includes TennCare, its MCOs, and their NEMT Brokers accessing credentials and other NEMT documentation to evaluate if the NEMT transportation providers, NEMT transportation brokers, or MCOs are complying with federal and state NEMT program requirements; or if there are gaps in the credentialing or oversight of NEMT services that should be examined further. Auditing of NEMT services includes but is not limited to the following components:

- Validating that NEMT transportation providers possess valid driver's license, vehicle registration, and insurance
- Validating that NEMT transportation providers were subject to criminal history background and sex offender registry checks
- Validating the authenticity of credentials submitted by NEMT transportation providers to ensure that information is not missing, erroneous, or fraudulent
- Evaluating NEMT transportation broker oversight of its NEMT transportation providers including compliance with NEMT program requirements and demonstrating professional conduct with regards to the TennCare member experience
- Evaluating MCO oversight of the NEMT transportation broker to validate that reported data was accurate, to validate that NEMT transportation brokers are maintaining effective trip logs and medical needs forms related to Medicaid covered services, to validate that there is accountability for missed performance measures, and to ensure that TennCare member complaints are addressed
- Evaluate the MCOs to determine if proper Medicaid payments were made for NEMT services and that the MCO is continuously management NEMT driver performance and credentialing to assure safe and effective Medicaid NEMT service delivery in Tennessee.

Another component of TennCare's compliance process is complaint management which includes complaint intake, triage, referral, and response. NEMT complaint management includes each NEMT transportation broker hosting and maintaining an integrated case management system (CMS), that is typically a web-based platform. The CMS includes the date and time the complaint was submitted, the method of submittal, a detailed description of the nature of the complaint, and whether or not the complainant has selected the option for follow-up conversation. If requested by the complainant, the summary will be anonymous as to the identity of the complainant. The NEMT transportation brokers' system tracks initial complaints and any subsequent follow-up contact with complainants on the same case. The system allows for a designation of a complaint category/case type and assigns specific cases to other users within the system for investigation.

The NEMT transportation broker's complaint management system also typically has auto-case assignment capabilities based on incident types and/or locations so that the system is sending email notifications when cases are assigned. The NEMT transportation broker's complaint management system provides for the storage of the complaint and investigation data in accordance with Tennessee record retention requirements. The NEMT transportation broker's complaint management system facilitates communication between management and complaint intake representatives regarding specific cases, including providing templates and/or scripts for follow-up information and questions to be shared with the complainants by the intake representative. The NEMT transportation broker's complaint management system includes the ability to reflect the status of a particular case, at a minimum allowing the case to be reflected as open, in progress or closed. The NEMT transportation broker's complaint management system allows for the creation and downloading of reports both manually and as scheduled intervals at minimum levels of monthly, quarterly, annually, and year-to-date program activity including the nature of the complaint, the length of time from initial complaint intake to case closed, and the department reference. TennCare is seeking a solution that would be open-system allowing for application programming interface between the NEMT transportation broker's information system and this credentialing, auditing, and complaint management solution or offer the ability for the NEMT transportation broker to use the credentialing, auditing, and complaint management solution for all of its complaint tracking and management needs.

TennCare's Office of Contract Management (OCM) sits within TennCare's Division of Managed Care Operations and is responsible for the compliance oversight of TennCare's NEMT benefit. OCM collaborates with the MCOs and the NEMT transportation brokers to protect the financial integrity and high-quality service delivery of TennCare's NEMT program. OCM has current processes in place to facilitate the oversight of the NEMT benefit, but OCM does not possess electronic credentialing, sophisticated analytics, or aggregator complaint case management tools to enable the enhancements and improvements TennCare is seeking. OCM's objective is to provide TennCare's NEMT program with solutions that can drive improvements in proper NEMT utilization, improved member experience, and cost-effective use of the TennCare's NEMT benefit.

3. COMMUNICATIONS:

3.1. Please submit your response to this RFI via email to:

Matt Brimm, Director of Contracts
Division of TennCare
310 Great Circle Road, TN 37243
(615) 687-5811
matt.brimm@tn.gov

3.2. Please reference **RFI #31865-00709** within all communications related to this RFI.

4. RFI SCHEDULE OF EVENTS:

EVENT		TIME (Central Time Zone)	DATE
1.	RFI Issued		10/10/2022

2.	RFI Responses Due	3:00pm	11/04/2022

5. GENERAL INFORMATION:

5.1. Please note that responding to this RFI is not a prerequisite for responding to any future solicitations related to this project and a response to this RFI will <u>not</u> create any contract rights. Responses to this RFI will become property of the State.

5.2. The information gathered during this RFI is part of an ongoing procurement. In order to prevent an unfair advantage among potential respondents, the RFI responses will not be available until after the completion of evaluation of any responses, proposals, or bids resulting from a Request for Qualifications (RFQ), Request for Proposals (RFP), Invitation to Bid (ITB) or other procurement method. In the event that the state chooses not to go further in the procurement process and responses are never evaluated, the responses to the procurement, including the responses to the RFI, will be considered confidential by the State.

5.3. The State will <u>not</u> pay for any costs associated with responding to this RFI.

6. INSTRUCTIONS FOR RESPONDING

6.1. Sections **7 through 12** below indicate the information specified to be included in your response. All components should be addressed according to the instructions within this section and any item-specific instructions, e.g., page limitations, as noted below.

6.2. Respondents are **<u>not</u>** expected to insert responses directly into the RFI template. Please provide your response under separate cover in accordance with the details noted in the sections below.

6.3. Please clearly label each question/item in your response according to the exact numbering system used in the requirements tables below.

6.4. To better enable an efficient and effective review process, please respond as succinctly as reasonably possible to satisfy the questions/requirements.

RFI #31865-00709 **TECHNICAL INFORMATIONAL FORM**
7. RESPONDENT LEGAL ENTITY NAME
8. RESPONDENT CONTACT PERSON: Name Title/Role Address Phone Number Email
9. EXPLANATION OF VENDOR SOLUTION AND RELEVANT EXPERIENCE **Please limit your section 9 response to five (5) pages* 9.1. Please provide a summary statement regarding how your solution for a non-emergency medical transportation (NEMT) online credentialing, auditing, and complaint managment system that employs blockchain technology can help TennCare achieve the goals

articulated within section **1. STATEMENT OF PURPOSE**.

9.2. The following items are regarding your relevant experience in providing a non-emergency medical transportation (NEMT) online credentialing, auditing, and complaint management system that employs blockchain technology within the last five (5) years. In response to the requests below, please distinguish between Medicaid and Non-Medicaid experience. Please also distinguish between post-pay analytics and pre-pay analytics in any examples you provide. For your response, please do the following:

9.2.1. List the <u>total number</u> of experiences where your solution for a non-emergency medical transportation (NEMT) online credentialing, auditing, and complaint management system that employs blockchain technology was deployed for the five (5) year period (may include contracts that began prior to 5 years ago, but continued within the last 5 years). Of that total, please elaborate the following the following:

9.2.1.1. Number of instances related to Medicaid versus Non-Medicaid.

9.2.1.2. Number of instances which included an online credentialing solution involving blockchain technology for NEMT.

9.2.1.3. Number of instances which included an online, real-time auditing solution for NEMT.

9.2.1.4. Number of instances which included a case management information system for beneficiary complaint intake, triage, referral, and reporting for NEMT.

9.2.2. Describe three (3) distinct experiences where you delivered NEMT provider credentialing involving blockchain technology, audit services, and complaint management services or are currently delivering these services. For each, please distinguish between Medicaid and Non-Medicaid, as well as which of the requested services are relevant (credentialing using blockchain technoloy, audit services, and/or complaint management services). Please make clear what stage of the project you're in (e.g. pre-implementation, post-implementation, etc.) at the time of this RFI response

9.2.2.1. If delivery is for a government agency, please include the following information:

9.2.2.1.1. State/Federal Agency Name

9.2.2.1.2. Contract Start/End Dates

9.2.2.1.3. Contract Value

9.2.2.1.4. Summary of scope that also specifies non-emergency medical transportation (NEMT) online credentialing, auditing, and complaint monitoring system that employs blockchain technology solutions.

9.2.2.2. If for a commercial entity, please provide similar information to the degree it is contractually appropriate to share. Client names and other identification-related details may be omitted; however, we expect that you can, at minimum, explain the relevance of the scope of work to our objectives.

10. TECHNICAL SPECIFICATIONS AND REQUIREMENTS

**Please limit your section 10 response to seventy-five (75) pages*

10.1. Credentialing Process and Data Considerations

10.1.1. Describe what constitutes a "credential" within your solution.

10.1.2. Describe how your solution digitizes the credential.

10.1.3. Describe how your solution's approach to digitizing the credential is scalable, specifically whether there are discreet data points, artifacts, an ability to upload, and the ability for your solution to receive data feeds from primary sources?

10.1.4. Describe how your solution can distinguish between acceptable documentation (scanned image or received message) versus a credential?

10.1.5. What endorsements are associated with the “credential” within your solution? Are the users of your solution able to select the criteria behind the credential and modify the criteria at will? Or is the criteria behind the credential pre-defined and/or off-the-shelf (OTS)?

10.1.6. Describe how your solution allows users of the solution (e.g. organizations such as TennCare, its Managed Care Organizations, its NEMT Brokers, and Transportation Providers) to move the “credential” between organizations.

10.1.7. Describe your solution’s approach to ownership of the data. How does each user (e.g. organizations such as TennCare, its Managed Care Organizations, its NEMT Brokers, and Transportation Providers) own the data? Who owns copies of the data? Is there a shared function? Is there an interface available between organizations’ systems and your solution? How does your solution handle transition of users (e.g. organizations such as TennCare, its Managed Care Organizations, its NEMT Brokers, and Transportation Providers) and their data within your solution when these users join your solution as new users or leave your solution and need to be deprovisioned due to the users no longer serving as a Managed Care Organization, NEMT Broker, or Transportation Provider with TennCare?

10.1.8. Describe your solution’s approach to centrally storing credentials. Outline your solution’s architecture. Are the credentials stored in the cloud or on physical servers? What is your solution’s data storage capacity and limitations?

10.1.9. Describe your previous experience with establishing a collaborative network of Non-Emergency Medical Transportation (NEMT) providers, including transportation providers, transportation brokers, managed care organizations, and state government agencies.

10.1.10. What are the steps involved and the estimated ramp up time to get NEMT transportation providers, NEMT Brokers, Managed Care Organizations, and state Medicaid Agencies provisioned as users and able to use the solution?

10.1.11. It is expected that the solution will be using, at minimum, Transportation Provider data, NEMT Broker data, MCO data, and State Medicaid Agency data. Please confirm whether the solution envisioned for TennCare has been used previously to conduct credentialing across all of these stakeholders?

10.1.12. Does your solution have built in user roles and are mapped to specific sets of application functionality? Please explain the assumed business roles or how roles and responsibilities are defined for a client.

10.1.13. To access relevant TennCare data, a vendor may be granted access to source data within TennCare’s information systems or other data storage applications. Please explain solution capabilities for extracting data files for use in your systems.

10.1.14. Does the solution process and integrate unstructured data, i.e. web data, notes, and/or call center calls? Please briefly summarize any key considerations related to this, including what has been done for previous clients.

10.1.15. Please summarize your deployment options and data hosting capabilities, e.g. on-site, hosted, web portal, or cloud based. Please comment on the readiness of your secure environment, e.g. a cloud environment, where data accessed/provided can be stored throughout the implementation. Please briefly summarize any key considerations and recommendations related to this. Please specify the platform e.g., Amazon Web Services Cloud or Microsoft Azure Cloud.

10.1.16. Does your recommended solution meet security and compliance standards. If so, please describe specific examples of the compliance standards relevant to Managed Care Contractor and State data.

10.1.17. Please summarizes any additional third party certifications or standards met by your solution that may be relevant to the scope of work.

10.2. Blockchain Technology

10.2.1. Blockchain-based systems serve as a verification clearinghouse for documentation of NEMT driver credentials by providing public and/or private entities proof of the veracity of a document or certification. Describe how your solution uses blockchain protocol to give a document a digital signature.

10.2.2. Describe how your solution uses distributed ledger technology (DLT), including how your solution's DLT distributes copies of the ledger to the nodes on a blockchain network, making each one responsible for recording new transactions and participating in a consensus mechanism to agree on updates to the ledger.

10.2.3. Describe how your solution allows any user to verify the digital signature of a document, thererin certifying the document's authenticity.

10.2.4. Describe how your solution uses blockchain technology to preserve the chain-of-custody of the document.

10.2.5. How do you allow a "credential" to be shared within the network (TPs, Brokers, MCO, State) without breaking the chain of custody?

10.2.6. For every credential in your system, how is its origin and every organization that accessed the credential logged? What is the manifest of that information? Is content exchanged between systems or centrally stored?

10.2.7. Describe your platform's use of data exchange including but not limited to third party vendors serving as primary data sources for background checks and sources of screening.

10.2.8. Describe your platform's model for empowering all stakeholders/users in the network to share their data for their own purposes as well as to meet the needs of the state.

10.2.9. Describe your solution's approach to using blockchain technology to promote strong encryption and other security safeguards.

10.2.10. Describe your solution's approach to using blockchain technology to promote a decentralized, peer-to-peer architecture to facilitate blockchain storage.

10.2.11. Describe whether your solution uses a public blockchain (permissionless), private blockchain (permissioned), hybrid blockchain, and/or consortium blockchain approach. Describe how your blockchain approach impacts access control, performance, scalability, security, transparency, auditability, and the ability to upgrade.

10.2.12. Describe your solution's use of blockchain vendors including infrastructure provider(s), application provider(s), and/or service provider(s). Please identify any and all vendors that your solution uses to deliver the blockchain technology and describe their role in supporting your solution.

10.3. Audit and Complaint Management Considerations

10.3.1. Describe whether your system is built specifically for NEMT and or if your system requires an adaptation of an existing credentialing solution (e.g. general provider credentialing solution)?

10.3.2. Describe your NEMT auditing and complaint management experience and if your solution is already configured for NEMT including a NEMT platform or module prior to responding to this RFI.

10.3.3. Describe the major fraud and abuse methods that are used for detection in your solution such as: Statistical Exceptions, Profiling, Business Algorithm Matching, Pre-deceive Analytics, Ranked Listings, Utilization Analysis, and other advanced techniques.

10.3.4. Describe your solution's ability to take a 'rule set' and to modify the rule set and apply it to TPs and Broker and MCO and State audits; within your platform and/or application(s)?

Run the algorithm against these rules

10.3.5. Does your solution possess pre-existing business rules and algorithms for credentialing and audit that are directly applicable to identifying relevant flags within provider and broker data? Please elaborate on the sophistication of existing algorithms. Please elaborate on your experience regarding the need to customize and/or create new algorthims for each implementation, as well as the potential time/effort involved in arriving at the sufficient level of algorithms generally required to begin conducting analytics.

10.3.6. Is the Audit Case Tracking component within your solution specifically created for NEMT or is your package a COTS package or a Commercial package?

10.3.7. Is your audit solution fully integrated across your solution with the credentialing module and complaint management module? If not, please explain the process and key considerations for integration, including variables that impact the timing and cost of integration. Describe your audit solution.

10.3.8. Is the Complaint Management Tracking component within your solution specifically created for NEMT or is your package a COTS package or a Commercial package? Describe your complaint management solution.

10.3.9. Please describe your experience and process for integrating/importing historical case information from existing databases (legacy case management systems); for example, active and open cases, closed, referred and pending cases, and previous documentation/notes.

10.3.10. Does your tool have the ability to auto-populate information from other sources of data? If yes, how will the case management solution pull in data from other sources, e.g., the analytics solution or outside information related to transportation provider identification.

10.3.11. Please describe your process for creating role/rule-based access rights and how access is managed and monitored.

10.3.12. Does the solution allow for users to enter notes and edit as needed throughout the process to ensure accurate documentation? Will there be a behind the scenes audit trail available?

10.3.13. Can the solution auto-generate communications such as reminders, notifications, and letters to other parties?

10.3.14. Can the solution auto-populate letter templates based on information within the solution, when triggered in the workflow? Please elaborate on use of such functions and potential customization requirements.

10.3.15. Does the solution provide workflow capabilities? If so, are there any pre-built workflows? In your experience, how much customization is required to meet each client's need? What are key drivers requiring customization?

10.3.16. Please explain the credentialing workflow and your approach to identifying providers and/or other elements that would enable us to detect improper credentials.

10.3.17. Please explain the audit workflow and your approach to identifying providers and/or other elements that would enable us to detect non-compliance.

10.3.18. Please explain the complaint management workflow and your approach to identifying providers and/or other elements that would enable us to detect trends among member complaints or provider complaints against members.

10.3.19. Does your solution deploy sophisticated data analytics and predictive modeling? Does it leverage tools such as as artificial intelligence, machine learning, link analysis, natural language processing, or geocoding? Are these standard functions in the solution or do they require additional effort/customization? Please briefly summarize any related key considerations. Do you use a partner to achieve data analytics within your solution? If so, who?

10.3.20. Please summarize the standard/out of the box reporting and dashboarding capabilities available to help users in their efforts to credential, audit, and manage complaints.

10.3.21. What are the reporting capabilities of the complaint management system?

10.3.22. Does your solution offer reports that track key performance indicators around credentialing, auditing, and complaint management? Please provide additional context to help understand what information you are capturing for other clients that may be relevant to TenCare's use case.

10.3.23. Does your solution offer the print functionality for hardcopies for reports available within your solution?

10.3.24. Please elaborate on other reports readily available that you believe may be critical and/or add value to our approach based on your experience with other clients.

10.3.25. Please describe how your solution maintains privacy and security of confidential complaint/resolution data, and how the solution addresses relevant industry privacy or security controls and compliance standards (i.e. HIPAA, NIST) related to confidential information (e.g. Role, Workflow, or Policy based access) ?

10.3.26. Please describe how your solution approaches linking complaint incidents, known violations, and approved resolutions to one or many providers, and describe the capabilities for allowing a holistic view of associated provider performance within the complaint management solution?

10.3.27. Does your complaint solution meet compliance standards related to Americans with Disability Act and Section 508 regulations

10.3.28. Does your solution allow for flexible and configurable role assignments with the ability to integrate, remove, or reassign resources into the complaint process to allow for personnel changes during the lifecycle of the complaint?

10.3.29. Does your solution have the ability to support single and multiple levels of sequential management or organizational review cycles? Does your solution allow for the capture of follow-up details within management or organizational review, as well as capture the date that the follow up has occurred, or the date that it will occur

10.3.30. Does the solution provide data validation on mandatory fields prior to submission of complaints or inquires, and does it have the capability to generate concise notifications or error messages for identifying further action needed?

10.3.31. Please describe the search features available in your solution that will allow uses to search on individual, providers, or incident/resolution attributes across time and date ranges

10.3.32. Does your solution provide the ability to support verification activities such as time verification, supporting documentation uploads, and other attribute verification approaches to enhance data quality and consistency?

10.3.33. Please describe if or how the solution supports modification of submitted or uploaded documentation? Do the revisions create an audit history of the document revisions and modifications that can be easily viewed within the tool?

10.3.34. Does your solution allow for analysis of complaint resolutions to identify common themes to assist with operational and/or system improvements?

10.4. Personnel and Support

10.4.1. Does your solution provide continuous ongoing support?

10.4.2. Does your solution provider train-the-trainer and/or direct-end user training and if so, is the training medium televisual and/or in-person?

10.4.3. It is TennCare's intention to train internal staff to use the solution and conduct online credentialing, auditing, and complaint management activites with little to no ongoing effort from the vendor in conducting such activities. Does your solution require resources (e.g., personnel) from your team to run to perform online credentialing, auditing, and/or complaint managenment once your solution is implemented? Please explain potential cost considerations, timeline, and impact.

10.4.4. What is the level of credentialing, auditing, and/or complaint management experience needed in order to run your solution? Please elaborate on your approach to training resources to independently conduct credentialing, auditing, and/or complaint management with the solution.

10.4.5. Have your other clients faced challenges in training their resources to use your solution? Please explain common challenges and potential suggestions for a successful and efficient training model.

10.4.6. Describe the support activities you have provided to other clients.

10.5. Timeline and Approach

10.5.1. Please describe the process for solution implementation, including average timeframes for each key phase/step.

10.5.2. Please elaborate on the key considerations and variables that may impact the timeline and cost.

10.5.3. Do you suggest TennCare dedicate an internal coordinator or TennCare project lead during implementation? Post-implementation? Please explain any staffing recommendations you have from a TennCare personnel standpoint.

10.5.4. What is your approach to providing help desk services, such as desktop support or support for outages. Please describe the issue escalation process and typical service level agreements on resolution of high-level defects. TennCare considers this solution critical to its mission and is particularly interested in the variety of approaches vendors take in supporting their implemented solutions.

11. COST INFORMATION

** Please limit your response to fifteen (15) pages.*

11.1. Describe your normal pricing approach as follows:

11.1.1. Describe your normal pricing structure (one time or ongoing monthly/annual costs; variable costs based on number of users/amount of data/number of members or other variables) for each component of the solution (e.g. credentialing using blockchain techonology vs. auditing vs. complaint management). Specify whether your solution uses an on-premise vs. cloud implementation and the associated costs and pricing approach in your response including cost of data storage, user access of the application and/or platform, and annual maintenance and support post-implementation.

11.1.2. Where, in response to sections 9 and 10 above, you indicated that additional customization would be required, provide general descriptions of how you usually approach pricing customizations. The response should be specific to your solution (including all relevant portions of your solution including credentialing using blockchain techonology vs. auditing vs. complaint management). What key considerations, benefits, and obstacles have you observed in terms of this approach in dealing with other clients, especially if you believe a particular model is more cost effective and efficient?

11.1.3. Describe the typical price range for similar services or goods and elaborate on key considerations, drivers, and components that are priced separately (technology, data, personnel, etc.).

12. ADDITIONAL INFORMATION

**Please limit to five (5) pages.*

12.1. Please provide input on alternative approaches or additional things to consider that might benefit the State and/or our understanding of your solution for (e.g. credentialing using blockchain techonology vs. auditing vs. complaint management).