ATTACHMENT D: QUESTIONNAIRE FORM

This form is broken into five sections: Section 1. Functional Requirements; Section 2. Non-Functional Requirements; Section 3. RCW Requirements; Section 4. Data Conversion; 5. Pricing. It is requested that vendors respond to all questions in the expandable space provided. If a question requires Vendor to submit additional documents, please attach them to this document and label them clearly as part of your response to this Attachment D. Vendors are encouraged to include further information as attachments about features of their solution not identified below.

Section 1. Functional Requirements – this section identifies the basic system behavior that DOH expects.		Describe how your solution meets the requirement.
Healthcare Practitioner Portal - Healthcare Practitioners need to be able to log into the system and complete the following functions listed below.		
FR-1	Allows healthcare practitioners to complete an electronic medical Marijuana authorization that retail stores can query in order to issue recognition cards.	
FR-2	Allows healthcare practitioners, with a valid Drug Enforcement Agency (DEA) registration number, to review any authorized patient card.	
FR-3	Allows healthcare practitioners, without a valid DEA registration number, to review only patient cards they have authorized.	
FR-4	Allows healthcare practitioners to revoke an authorization that they have authorized.	
Retail Store Portal - Retail stores need to be able to log into the system and complete the following functions listed below.		
FR-5	Allows retail stores to issue, renew, and manage recognition cards.	

FR-6	Allows retail store to view store specific configurable reports. E.g., number of cards the store has created card statistics by consultant, card statistics by patient vs designated provider, retail tax exemption audit report.	
FR-7	Allows retail stores to view invoices on a dashboard.	
FR-8	Allows stores to pay invoices electronically from the system. The state's current banking contract must be used.	
FR-9	Allows stores to review and confirm store users on a quarterly basis. If a store does not complete the quarterly confirmation, the store is inactivated, store users are unlinked from the store and are prevented from using the system.	
Patient and Designated Provider Portal - Patients and designated providers need to be able to log into the system and view or complete the following functions listed below.		
FR-10	Allows a patient or designated provider to access an electronic recognition card and/or authorization form(s) from a mobile device or other electronic computing device.	
FR-11	Allows a patient to inactivate their card or designated provider card.	
FR-12	Allows a designated provider to inactivate their card.	
FR-13	Allows a designated provider to view past patients they have been a designated provider for.	
FR-14	Allows a patient to view their own past designated providers.	
FR-15	Provides card expiration reminder notifications via text and email.	
Administrative Portal - DOH staff need to be able to log into the system and view, query, access or complete the following functions listed below:		
FR-16	Allows DOH staff to manage stores and users.	
FR-17	Allows DOH staff to post messages to end user dashboards, which may include patients, store owners, consultants, budtenders, and healthcare practitioners.	

FR-18	Allows DOH staff to send email messages through the system to user(s) or user groups, which may include patients, store owners, consultants, budtenders, and healthcare practitioners.	
FR-19	Provides audit records to DOH administrators that show who accessed the system, what records were accessed, date/time stamp, what type of activity was performed and what data elements were modified.	
FR-20	Provides reporting functionality. Describe all reports available. Include how reports can be sorted, filtered, rearranged, etc.	
Card Tracking - The system must be able to track and complete the functions listed below.		
FR-21	Assigns a randomly generated and unique ID to a patient without using personal identifiable information.	
FR-22	Tracks all cards issued to a patient and can report on number of unique patients, regardless of how many cards have been issued to a patient without using personal identifiable information.	
FR-23	Tracks card expiration dates and automatically inactivates when expired, unless revoked earlier by healthcare professional, patient or designated provider.	
FR-24	Once patient or designated provider registration is expired or in an inactive status, the record status is changed accordingly. Expired or inactive records are unsearchable by external end user unless under renewal action.	
Invoicing - The system should be able to offer invoicing services as listed below.		
FR-25	Provides Invoice Management and Tracking.	
FR-26	Automatically creates invoices and displays to stores through the dashboard.	
Interfaces - The system must allow for interfacing and data file exchanges with partner agencies as outlined below.		
FR-27	Ability to exchange data files with partner agencies.	

FR-28	Ability for law enforcement officers to confirm the registration of qualifying patients and/or designated providers through the Washington State Patrol ACCESS system using only the card number.	
FR-29	Ability to import the Drug Enforcement Agency data file at least on a quarterly basis.	
Global Requirements - The system must be able to allow for program rules as outlined below.		
FR-30	Prevents duplicate records.	
FR-31	Allows for processing of rules such as, if a designated provider is revoked or cancelled, they cannot become a designated provider for another patient until XX days have passed.	
Section 2. Non-Functional Requirements – this section identifies the system qualities that DOH expects.		Describe how your solution meets the requirement.
Security (Category 4 Externally Hosted) - The system must contain the following security features and capabilities as detailed below.		
NFR-1	Network architectures must be single tenant or logical single tenant and assure disaster resiliency. The architecture must provide logical boundaries that separate Internet available systems, internal application/utility systems, data systems, and user activities. Controls must prevent unauthorized connections to the assets within each segment. The architecture must provide continuous monitoring of both internal and external activity for anomalies and identify, report, and defend against security intrusions before the data is compromised. Automated processes, on-line analysis, notification, and actions are expected. Infrastructure must have three separate and fully independent environments/virtual instances: Development, Quality Assurance (QA) and Production.	

NFR-2	The vendor must ensure data center security controls meet or exceed those expected by the Federal Information Security Management Act (FISMA) for moderate to high impact systems as described in FIPS 199 and 200, and in the most current release of National Institute of Standards and Technology (NIST) Special Publications SP800- 53.	
NFR-59	The vendor must be able to show the data center and all failover facilities are FedRAMP (or FISMA) certified for moderate to high impact systems and that a recent SOC2 type 2 audit was conducted for the specific data center facility where the service is deployed, and all failover facilities. The audit must address security, integrity, availability, and confidentiality.	
NFR-3	The vendor will upon request provide the DOH CISO proof of the FedRAMP (or FISMA) certification and copies of the audit results, including all management comments and plans to correct deficiencies.	
NFR-4	The vendor will certify that all data collected, processed, routed, and/or stored by or through the service, or third-party service providers, remains at all times within the United States.	

NFR-5	The vendor will ensure systematic collection, monitoring, alerting, maintenance, retention, and disposal of security event logs and application audit trails. At a minimum: the logs and audit trails are written to an area inaccessible to system users and are protected from editing. At a minimum the logs and audit trails will provide historical details on all transactions within the system that are necessary to reconstruct activities. Type of event, date, time, account identification and machine identifiers are recorded and collected for each logged transaction. Audit and log files can be analyzed by type in order to find emerging issues or trends. The appearance of severe issues triggers an immediate notification to appropriate system administrators. Logs are secured against unauthorized changes. At a minimum, logs must be retained for a period of 6 months. DOH expects practices that are consistent with the current version of SP800-92 for moderate to high impact systems.	
NFR-6	The vendor will have implemented systematic and accountable processes for managing exposures to system and application vulnerabilities and for prevention of malware infections. The processes must assure the infrastructure is hardened against malicious code and maintained at the most current security patch levels. These practices must meet or exceed those described in NIST SP800-40 and SP 800-83.	
NFR-7	The vendor shall conduct system and application vulnerability assessments at least monthly, and penetration tests at least quarterly. These tests and assessments must be conducted by an independent accredited firm at least annually. The vendor shall provide the results of these assessments and tests, to the DOH CISO upon request.	

NFR-8	The vendor will have successfully implemented application authentication controls that provide a high level of confidence in the identity of individuals and meet or exceed those described in the most recent version of NIST SP 800-63 for information requiring assurance level 3 or higher.	
NFR-9	The vendor will ensure the system/service supports single sign on for state government employees, and external users by integrating the system's authentication mechanisms with the STATE Enterprise Active Directory and the STATE Secure Authentication Gateways (post listeners are typically used for processing the gateway host headers). Knowledge and experience with SAML 2.0 are required.	
NFR-10	The vendor will ensure all system and service accounts use Enterprise Active Directory or a similar centralized authentication and authorization mechanism. If authentication methods such as SQL authentication are required, by the system, the vendor must provide documentation showing how the credentials are secured during all transmissions, using encrypted sessions such as TLS or IPSec, and in storage using a secure hash method validated by the National Institute of Standards and Technology (NIST).	
NFR-11	The vendor will have implemented security controls that require encrypted sessions and strong multi-factor authentication for anyone able to remotely access the infrastructure (e.g., vendor employees and contractors). Authentication mechanisms must meet or exceed those described in the most recent version of NIST SP 800-63 for information requiring assurance level 3 or higher. For system administration purposes one of the factors must be provided by a device separate from the computer gaining access.	

NFR-12	The vendor will ensure the data are encrypted, when transmitted across open untrusted networks (using key lengths of 128 bits or greater), and when at rest, (using key lengths of 256 bits or greater). Algorithm modules validated by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) are required: http://csrc.nist.gov/groups/STM/cavp/validation.html http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm	
NFR-13	The vendor shall ensure application controls provide for sessions that terminate or re-authenticate after an inactivity period of 20 minutes or less.	
NFR-14	The vendor shall ensure administrator and user roles sufficiently restrict privileges and access rights based upon the concepts of least privilege and need to know.	
NFR-15	The vendor will have implemented application/system development practices consistent with the current version of NIST SP800-64 for moderate to high impact systems and assure the software does not contain any of the Open Web Application Security project (OWASP) top 10 vulnerabilities - https://www.owasp.org/index.php/Main_Page.	
NFR-16	The vendor's operational security controls must meet or exceed those described in the most current version of National Institute of Security and Technology (NIST) special publication: SP800-53, (See FedRAMP ModerateBaseline). Where applicable all controls must be consistent with those described for moderate to high impact systems.	
NFR-17	The vendor must be able to show a recent SOC2 type 2 audit of their development and operational practices was conducted, or that a SOC2 type 2 audit will be completed within 6 months after contract execution. This audit must address security, integrity, availability, and confidentiality.	

NFR-60	The vendor must complete ongoing SOC2 type 2 security audits by an accredited auditing firm at least annually. These audits must address security, integrity, availability, and confidentiality. The vendor will provide the results of these audits and plans to correct identified deficiencies to the DOH CISO upon request.	
NFR-18	The vendor must have implemented cyber security incident response practices consistent with NIST SP 800-61. The vendor assures DOH is notified at security@doh.wa.gov within One (1) business day upon the discovery of any suspected or actual security breach. The vendor will provide DOH a copy of their incident response practices prior to contract award. If awarded a contract the vendor will coordinate testing of the incident response plan with the DOH CISO annually.	
NFR-19	The vendor will document, test, and maintain a disaster recovery plan and alternate facility to assure the system/service is recovered within 72 hours of a major disruption or disaster. The recovery plan must assure no more than 24 hours of data are lost.	
Manageability and Maintainability - The system must provide certain maintenance and ongoing management capabilities as listed below.		
NFR-21	The solution must be able to support up to 10% annual growth in overall user base without degradation of performance.	
NFR-22	The solution must provide a release management process in compliance with ITIL best practices. Note: Prospective vendors must demonstrate their release management processes in current deployments.	
NFR-23	The solution must provide a change management process in compliance with ITIL best practices. Note: Prospective vendors must demonstrate their change management processes in current deployments.	

NFR-24	The solution must provide an incident management process in compliance with ITIL best practices.	
NFR-25	The solution must be able to easily incorporate new data, business rules, workflows, and configurations which further enhance the existing functionality.	
NFR-26	The solution must be a fault-tolerant system which will notify the user that an error occurred, log the error, and continue to operate in the presence of error or exception. In the event of a failure in the system, the operating quality should be proportionate to the severity of the failure. The solution should respond 'gracefully'. It is expected that the solution be planned, setup and configured to prevent failure, or crashing, in the event of an unexpected problem or error.	
NFR-27	The solution components must be backward compatible for up to three major versions.	
NFR-28	The solution must be modular with components loosely coupled to reduce the risk that changes in one component will require changes in another component or if one component becomes obsolete the entire system is compromised.	
NFR-29	The solution must be a vendor hosted SaaS solution. Solution's platform/codebase must be effectively managed and maintained by the vendor.	
NFR-30	The solution must be built to allow technical changes to be developed, tested, deployed and productionalized with minimal effort.	
NFR-32	The solution must provide a method for an administrator to configure the solution, in real time, without requesting a formal change request from the vendor. E.g., change data field labels, add, and remove a value from pick lists, add data fields, remove data fields, set a field to required, etc.	
NFR-33	The solution must retain configuration settings during application version upgrades.	

NFR-34	The solution must provide a secure platform in which information is exchanged. Provide a description of technical architecture. Include diagrams of the data flows for both software and hardware components and a block level diagram of client to server communications and security architecture including control points.	
NFR-61	The vendor will provide a test environment for DOH use. Test environment will be kept updated with changes and contain only mock data.	
Integration and Interoperability - The system must have integration features and interoperability as listed below.		
NFR-36	The solution must support Service Oriented Architecture (SOA) and provides the ability to utilize web services and API's for integrations with other systems.	
Data - The system must be able to support data retention and data migration requirements as listed below.		
NFR-39	The solution must support OCIO Open Data Policy 187 (https://ocio.wa.gov/policy/open-data-planning). The solution provides data exports of large-volume, un-manipulated, raw data in a machine-readable format, on a scheduled basis.	
NFR-40	The vendor must provide, and execute, a detailed Data Migration plan with fail safes in place to prevent data loss and data corruption. The plan will be negotiated during planning sessions prior to contract signing.	
NFR-41	The solution must comply with Disposition Authority Number DAN 95-09-57022. Records must be retained for 6 years after file is inactive then destroy. department-of-health-records-retention-schedule-v.1.4-(june-2019).pdf (wa.gov)	
Availability - The system must be available for end users as listed below.		
NFR-43	The solution must be available for use 99.9% of the time, twenty-four hours a day, seven days a week.	
User Experience - The system must offer a certain user experience as detailed below.		
NFR-45	The solution must meet the Accessibility Requirements of WCAG 2.1 level AA, as prescribed by Washington State OCIO Policy 188.10 https://ocio.wa.gov/policy/minimum-accessibility-standard	

NFR-46	The vendor must provide a Voluntary Product Accessibility Template (VPAT) to document compliance with Section 508c Standards. VPAT can be found at https://www.itic.org/policy/accessibility/. The vendor is highly encouraged to provide an application sample that the department can scan for accessibility compliance.	
NFR-47	The solution must provide a single, organized, and intuitive user interface with descriptive labels, valid value selection or text entry input, data validation, and appropriate error messaging for both internal and external users. While separate systems may be implemented, it is expected they would be integrated so that the user will be provided with a seamless work experience.	
NFR-48	The solution must allow users to access and transact with the solution on mobile devices. This includes agency staff using state issued devices (phones, tablets, laptops) to perform their work-related tasks within their permission settings, as well as external customers using their personal mobile devices (phones, tables, laptops) to perform activities within their access restrictions.	
NFR-49	The solution must support common supported versions of marketplace browsers that include Firefox, Chrome, Edge, and Safari.	
Reliability - The system must be able to function under certain circumstances as outlined below.		
NFR-51	The solution must be able to handle multiple concurrent users and continue running at optimal speed for basic navigation, downloads, uploads, and system functions, even at speeds as low as 10 mbps.	
Training, Documentation and Support - The solution must provide training, documentation capabilities and support for all end users as listed below.		
NFR-53	The vendor must provide help desk support for end users and department administrators.	

NFR-54	The vendor must develop training documents and complete training sessions for the following user groups: • MMJ administration staff • Retailers • Healthcare professionals • Law Enforcement • DOH Healthcare Investigators	
NFR-55	The vendor must provide up-to-date and reproducible materials for initial and continued training of DOH staff and all system users.	
NFR-57	The vendor must provide detailed, comprehensive, and perpetually current technical documentation including system administration, operations, procedures; technical specifications and definitions; database definitions, logical data model and record layouts; screen definitions and functions; and the mechanism used to ensure that the standards and documented processes for maintaining the system components are kept current.	
NFR-58	The vendor must provide and maintain an online help feature for all system users.	
Section 3. RCW Requirements – The medical marijuana data registry must meet the following RCW specific requirements.		Describe how your solution meets the requirement.
Any personally identifiable information included in the registry must be nonreversible, pursuant to definitions and standards set forth by the national institute of standards and technology.		
RCW-1	Please describe the ability of the registry solution to encrypt personally identifiable information using a non-reversible hash algorithm validated by the National Institute of Standards and Technology (NIST).	

Any personally identifiable information included in the registry must not be susceptible to linkage by use of data external to the registry.		
RCW-2	Please describe the ability of the solution to prevent the linking of registry data to any other information.	
The registry must incorporate current best differential privacy practices, allowing for maximum accuracy of registry queries while minimizing the chances of identifying the personally identifiable information included therein.		
RCW-3	Please describe how the solution will provide maximum accuracy query results without including personally identifiable information.	
The registry must be upgradable and updated in a timely fashion to keep current with state-of-the-art privacy and security standards and practices.		
RCW-4	Please describe the processes and timelines that assure the registry solution is updated regularly, including security patches, services packs, and new releases for browsers, operating systems, databases, and all other supporting software.	
RCW-5	Please describe your ability to assure the data center facility and the registry solution remain current with Washington state, and federal privacy and security statutes, standards, and guidelines (e.g., chapter 42.56 RCW, chapter 70.02 RCW, FIPS, FISMA, and NIST).	
RCW-6	Please describe the security controls and practices that ensures the registry information is secured against unauthorized access, use, modification or disclosure consistent with federal and industry standards and guidelines for medium to high impact systems (e.g., FIPS, FISMA, NIST, ISO 27001/27002 and OWASP). The response should include data center facility, operational, and administrative controls as well as the system lifecycle development practices.	
RCW-7	Please describe the ability to show compliance with federal and industry standards (e.g., FIPS, FISMA, NIST, ISO 27001/27002, and OWASP), and to complete SOC2 audits. The response should	

	address controls for both Cloud Provider and the registry solution.	
Personally identifiable information of qualifying patients and designated providers included in the medical marijuana registry is confidential and exempt from public disclosure, inspection, or copying under chapter 42.56 RCW.		
RCW-8	Please describe your experience integrating the registry solution's authentication mechanisms with state supported authentication gateways and supporting single sign on.	
RCW-9	Please describe the ability of your solution to support multifactor authentication that provides a high level of confidence in the identity of individuals.	
RCW-10	Does the authentication method meet or exceed the requirements for assurance level 3 or higher as described in the most recent version of NIST SP 800-63?	
RCW-11	Please describe your ability to provide cyber liability insurance for the registry solution. Include limits per claim and annual aggregates.	
Information contained in the medical marijuana registry may be released in aggregate form, with all personally identifying information redacted, for the purpose of statistical analysis and oversight of agency performance and actions.		
RCW-12	Please describe the practices that ensures • prior written authorization is received from the Department of Health before the registry information is released in any form; • only the data specifically authorized by the Department of Health are released; and • the data are released only to individuals or entities specific authorized by the Department.	
Section 4. Data Conversion – If data conversion is to occur, DOH would like to understand the impact of migrating data from the current system to a new system.		Describe how your solution meets the requirement.
Data Conversion		

DC-1	Describe your experience in similar projects with data conversion efforts. How often have you performed this work as part of implementation of a proposed IT solution?	
DC-2	In the event that an RFP results in a new vendor, the new vendor must coordinate work with the existing vendor to convert and/or migrate data into formats and structures required by the proposed solution. Describe how this will done. What information or requirements would you need to accomplish this work?	
Section 5. Pricing – DOH would like to understand costs associated with a new system.		Describe how your solution meets the requirement.
One-Time Costs		
P-1	One-Time Licensing Costs – Describe in detail all one-time licensing costs.	
P-2	Implementation Cost Estimate – Describe in detail costs related to implementation and configuration. Provide hourly rates and level of effort estimates in addition to a total cost estimate.	
P-3	Data Conversion Cost Estimate – Describe in detail costs related to data conversion. Provide hourly rates and level of effort estimates in addition to a total cost estimate.	
P-4	Training Cost Estimate – Describe in detail activities and costs related to training for Retailers, Patients and DOH staff. Provide hourly rates and level of effort estimates in addition to total cost estimate.	
P-5	Testing Cost Estimate – Describe in detail costs related to all phases of testing conducted by vendor and in support of DOH testing. Provide hourly rates and level of effort estimates in addition to a total cost estimate.	

P-6	Implementation Cost Estimate – Describe in detail activities and associated costs related to implementation and configuration. Provide hourly rates and level of effort estimates in addition to a total cost estimate.	
P-7	Customization Cost – Describe how customization costs would be estimated in the event DOH desired the vendor to develop unique business logic not found in the proposed solution.	
On-Going Costs		
P-8	Licensing Costs – Describe in detail all on-going licensing costs.	
P-9	Support Costs – Describe in detail all on-going support costs, including maintenance and operations and help desk services.	
P-10	Professional Services Costs – Describe in detail all fees for professional services.	