Appendix B
Project Requirements
Software as a Solution (SaaS) Product

1 Project Overview

1.1 Background and Purpose

The State of Delaware Department of Health and Social Services (DHSS), Division of Public Health (DPH), seeks to procure and implement the EMSPS Patient Tracking System, which is a statewide, contractor-hosted, web-based solution to support Emergency Medical Services (EMS) data collection, reporting, and patient tracking. EMSPS Patient Tracking System will integrate core functions of the Emergency System for Advanced Registration of Volunteer Health Professionals (ESAR-VHP), the Health Alert Network (HAN), and the EMS data collection and reporting system.

The purpose of the Patient Tracking System is to centralize and standardize EMS service provider data and volunteer credentialing into a statewide platform that supports public health preparedness, emergency response, interoperability with partner systems, and compliance with state and federal requirements, including HIPAA and NEMSIS 3.5 standards.

1.2 Project Lifecycle

DHSS defines the "project" in Appendix B as the totality of work and activities throughout the contract period, which is delineated by a set of project lifecycle phases. The EMSPS Patient Tracking System shall be organized and managed based on five distinct lifecycle phases: Planning Phase, Configuration and Customization Phase, Testing and Deployment Phase, Operations and Support Phase, and Project Transition-Out Phase.

1.2.1 Planning Phase

The Planning Phase includes all mandatory deliverables and activities required to proceed to Configuration and Customization. Deliverables include:

- Schedule and conduct meetings with the project team to discuss and finalize the format and content for each deliverable
- Provide deliverable: Project Schedule
- Provide deliverable: Change Management Plan
- Provide deliverable: Continuity of Operations Plan
- Provide deliverable: Data Conversion Plan
- Provide deliverable: Architecture Network Diagram

1.2.2 Configuration and Customization Phase

This phase includes activities to configure and customize the Patient Tracking system, including integration with ESAR-VHP, HAN, and NEMSIS 3.5. Deliverables include:

- Schedule and conduct meetings with the project team to discuss and finalize the format and content for each deliverable
- Spin-up the cloud instance for the SaaS product
- Configure the product
- Customize the product (e.g., data and image conversion, OKTA SSO integration, etc.)
- Implement the Data Conversion Plan
- Update the Project Schedule
- Provide deliverable: Training Plan
- Provide deliverable: Test Plan
- Provide deliverable: Product Deployment Plan

1.2.3 Testing and Deployment Phase

This phase includes implementing the Test Plan, Training Plan, and Deployment Plan. Deliverables include:

- Schedule and conduct meetings with the project team to discuss and finalize the format and content for each deliverable
- Implement the Test Plan
- Implement the Training Plan
- Implement the Product Deployment Plan
- Update the Project Schedule
- Provide deliverable: User Guide
- Provide deliverable: Data Element Dictionary

1.2.4 Operations and Support Phase

This phase includes implementation of Continuity of Operations and Change Management Plans, ongoing system maintenance, help desk support, and data security monitoring.

- Schedule and conduct meetings with the project team to review operations monitoring and quality control reports, issue tracking, and change control tracking
- Implement the Continuity of Operations Plan
- Implement Change Management Plan
- Initiate Help Desk operations and incident management
- Provide ongoing maintenance and support
- Securely maintain all data and facilities

1.2.5 Project Transition-Out Phase

Upon termination of the contract, the contractor will provide a finalized copy of the Data Element Dictionary, and a copy of the database based on an agreed format and delivery method.

2

Project Team

2.1 DHSS Staff List

Name / Role	Organization / Email	Phone
Britany Huss DHSS Executive Sponsor	Division of Public Health Director of OMES britney.huss@delaware.gov	302-223-2700
Chip Finch DHSS Technical Manager	Delaware Health and Social Services Information Resource Management alfred.finch@delaware.gov	302-255-9256
Donna Doyle DHSS Program Manager	Division of Public Health Deputy Director of OMES Donna.Doyle@delaware.gov	302-223-2700
Michele Jones DHSS Subject Matter Expert	Division of Public Health Management Analyst III michele.jones@delaware.gov	302-857-5915
Amy Fritchman DHSS Subject Matter Expert	Division of Public Health Management Analyst III amy.fritchman@delaware.gov	302-223-2999
Zoriya Kemp DHSS Information Systems Support Specialist	Division of Public Health Bureau of Health Information Systems zoriya.kemp@delaware.gov	302-744-4700

2.3 DHSS Roles

2.3.1 Information Resource Management (IRM)

In support of the DHSS and Office of the Secretary - Administration, the mission of Information Resource Management (IRM) is to provide quality, efficient and cost-effective support in the management of technology resources. IRM provides DHSS divisions with information technology planning and management, information technology purchasing, network telecommunications, and help desk services. IRM is represented on the project team as the DHSS Technical Manager.

2.3.2 Department of Technology and Information (DTI)

The Department of Technology and Information (DTI) is the state's central information technology (IT) organization. DTI establishes and enforces the State's IT policy and standards and provides enterprise technology services that enable other organizations to effectively fulfill their missions. DTI does not actively participate in the project team and meetings but is available to IRM as necessary.

2.3.3 DHSS Executive Sponsor

The DHSS Executive Sponsor represents DPH senior management and is responsible for the success of a project and provides sustainability, strategic planning, guidance and resources to the project team and DHSS Project Manager as necessary. The DHSS Executive Sponsor attends the project meetings at their discretion.

2.3.4 DHSS Technical Manager

The DHSS Technical Manager serves as primary coordinator on behalf of IRM; attends project meetings as required, works with the project team to maintain the project plan and schedule; provides DPH and vendor with technical consulting support; facilitates configuration and/or customization required within the state network (e.g., firewall rules, etc.); and manages the work assignments of IRM staff as required (e.g., providing vendor access to or copies of the Patient and needed data and images, etc.).

2.3.5 DHSS Program Manager

The DHSS Program Manager serves as primary business lead for all project phases on behalf of DPH, attends all project meetings; works with the project team to maintain the project plan and schedule; disseminates program information to the vendor as needed (e.g., business requirements, processes, workflows, forms, reports, etc.); and manages work assignments of program staff as required (e.g., review deliverables, perform testing, etc.).

2.3.6 DHSS Subject Matter Expert (SME)

The DHSS Subject Matter Expert (SME) contributes program knowledge and information in all project phases, understands the vendor software from a user perspective, understands program workflows related to patient scheduling, service delivery, imaging, and claims billing; attends project meetings as required, and reports to the DHSS Program Manager.

2.3.7 DHSS Information Systems Support Specialist (ISSS)

The DHSS Information Systems Support Specialist (ISSS) serves as the DPH liaison between program staff and IRM, and between program staff and vendor IT staff. The ISSS participates in all project phases; attends all project meetings; ensures the business requirements are properly communicated to the vendor; assists program staff to understand DTI policies and standards; and assists program staff to understand the created information system processes and data. The ISSS reports to both the DHSS Technical Manager and DHSS Program Manager.

2.4 Contractor Roles

2.4.1 Vendor Project Manager

The contracted Project Manager serves as the chief liaison to the DPH for all project phases, has authority to make day-to-day decisions, facilitates all project deliverables and activities; maintains the project schedule; schedules, hosts and leads all project meetings; authors and distributes agendas, meeting notes and weekly status reports; and ensures contracted staff attend project meetings as required.

2.4.2 Vendor Application Manager

The contracted Application Manager facilitates all SaaS product configuration; documents and communicates systems-related issues and downtime; coordinates with the contractor's Help Desk as necessary; attends all project meetings as required; and contributes knowledge and information to inform the authoring of deliverables (e.g., Project Plan and Schedule, Architecture Network Diagram, Test Plan, etc.). The contracted Application Manager reports to the contracted Project Manager.

2.4.3 Vendor Database Manager

The contracted Database Manager develops and maintains the developed database(s); maintains data storage and retrieval systems; troubleshoots database issues; implements database

recovery procedures and safety protocols; attends all project meetings as required; and contributes knowledge and information to inform the authoring of deliverables (e.g., Project Plan and Schedule, Data Conversion Plan, Interface Control Documents, Data Element Dictionary, etc.). The Database Manager reports to the Project Manager.

2.4.4 Training Manager

The contracted Training Manager develops and maintains training materials; schedules and conducts training sessions; communicates with users; attends all project meetings as required; and contributes knowledge and information to inform the authoring of deliverables (e.g., Project Plan and Schedule, Training Plan, etc.). The Training Manager reports to the Project Manager.

3 Project Deliverables

The following subsections define the requirements and minimum data content for each deliverable. Each deliverable is submitted to DHSS as a standalone document and updated throughout the project per the vendors Change Management Plan. The Project Schedule, and Test Plan, are submitted to DHSS in Microsoft Excel format. All other deliverables are submitted in Portable Document Format (PDF) format. DPH acknowledges that the content and format associated with any deliverable is subject to change based on pre-existing documentation available from the vendor (e.g., Continuity or Operations Plan) or based on agreement reached during a project phase meeting.

3.1 Project Schedule

Vendor shall provide the Project Schedule in Microsoft Excel format and include task number, task description, assigned staff, task dependencies, task start and end dates, task duration, percentage completed, task completion date, and a project calendar depicting all tasks. For the duration of the project, Vendor will deliver to DHSS weekly an updated Project Schedule. Vendor will define tasks at a sufficient level to track the work assignments of Vendor and DHSS staff, which at a minimum includes deliverables, configuration, customization, conversion, training, testing and deployment. During the Operations and Support Phase, the Project Schedule will include issue resolution, change management, system downtime, or any other event or activity that requires tracking.

3.2 Change Management Plan

Vendor shall provide their Change Management Plan in PDF format and describe the change management process, both in terms of configuration and customization, define the method to request change, the process to rank and prioritize change requests (via a Configuration Control Board or equivalent), define the role of DPH, include a sample of any forms and artifacts used in the change management process (e.g., change request form, change approval form, UAT approval form, etc.), and list the project deliverables that will be updated (e.g., Project Schedule, Test Plan, User Guide, Data Element Dictionary, etc.).

3.3 Continuity of Operations Plan

Vendor shall provide their Continuity of Operations Plan in PDF format and describe their backup and recovery process of applications and data; and describe their methods to ensure all professional services are continued following a natural disaster, power outage, or any other event that impacts facilities, staffing, systems, or data. Vendor shall identify any associated vendors, provide documentation of recovery procedures and testing, define the communication method for alerting DPH of a disaster or event requiring the execution of the Continuity of Operations Plan, and define the Service Level Agreement (SLA) time to return to operations following notification to DPH.

3.4 Data Conversion Plan

Vendor shall provide a Data Conversion Plan in PDF format describing the method to transform and import data and images from the current system hosted by the existing vendor. The plan shall include the approach to ensure data quality before and after the data conversion process, describe the manual and/or automated controls and validation methods, and outline the process for data error detection and correction.

The plan shall also include a data conversion specifications table listing all source tables and fields, the corresponding target tables and fields, data value mappings (where applicable), and data transformation rules (where applicable).

3.5 Architecture Network Diagram

Vendor shall provide an Architectural Network Diagram in PDF format depicting the

user's interaction with the login, application and database servers, and interfaces with other systems (e.g., imaging), and include the IP addresses and port requirements.

3.6 Training Plan

Vendor shall provide a Training Plan in PDF format that describes their approach to training, includes a curriculum to demonstrate all core system functionality (e.g., user login; product configuration; online inquiry of patient, service, claim, and image information; reports and dashboards; and web portal), and includes a copy of all training materials or includes links to the training materials if available online.

3.7 Test Plan

Vendor shall provide a Test Plan in Excel format and document the test cases associated with unit and integrated testing. Vendor is required to work with DPH to identify the staff for testing, review the Test Plan with staff before testing begins, and facilitate one or more meetings with staff to execute the Test plan together. Vendor shall include in the Test Plan test cases for all core systems functionality associated with the product (e.g., user login; product configuration; online inquiry of patient, service, claim, and image information; reports and dashboards; and web portal), include DPH-specific configuration where applicable, and include test cases for all customization work (e.g., conversion, OKTA SSO). Vendor will include in the Test Plan a summary for each test case, and a series of test steps for each test case, instructions for executing each test step, the expected outcome, and columns for staff to record the actual outcome, and any testing notes.

3.8 Product Deployment Plan

Vendor shall provide a Product Deployment Plan in PDF format and describe their approach to deployment, describe the method to communicate with DHSS staff; include a readiness checklist for facilities, environments, applications, databases, operations, and Help Desk; describe their method to monitor operations and quality control; and include sample reports associated with operational monitoring and quality control.

3.9 User Guide

Vendor shall provide a User Guide in PDF format and include instructions and screen samples to navigate and use all core system functionality (e.g., user login; product configuration; online inquiry of patient, service, claim, and image information; reports and dashboards; and web portal). Vendor will include a table of contents; organize, and group the content by core functionality; and provide instructions for contacting the Help Desk.

3.10 Data Element Dictionary (DED)

Vendor shall provide a DED in PDF format and document all the table names, table descriptions, field names, field descriptions, field attributes, field positions, field sizes, valid values and primary keys associated with the application database. Vendor shall organize the DED with each table presented alphabetically as a separate section, order the fields for each table by position in the database, and depict the field information in a spreadsheet-like format.

4 Project Requirements

4.1 Offshore Prohibitions

Offshore is defined as not being within the United States or its territories. Offshore storage and transmission of DHSS data is prohibited. Onshore project data and project artifacts including backup and recovery files in any form shall not be accessed by offshore staff and shall not be copied, processed, transmitted, or moved offshore. Vendor is permitted to engage offshore resources including sub-contractors for development and internal lower level (unit & integration) testing only. Vendor is prohibited from using State data in any form even if masked or obfuscated for offshore testing. All aspects of user acceptance testing and production operations will take place onshore.

Associated Link:
Offshore IT Staffing Policy

4.2 Data Classification Policy

Vendor shall abide by the terms and conditions established in the Delaware Data Classification Policy, which defines the roles and responsibilities of a Data Steward based on the data classification. The data classification for this procurement is **State of Delaware Secret**.

Associated Link:
Data Classification Policy

4.3 Cloud Hosting and Data Use Agreements

The contractor shall abide by the terms and conditions established in the Terms and Conditions Governing Cloud Services and the Data Usage Policy, which govern remote hosting/cloud systems and the accessing/storing of State data outside the State network. The Terms and Conditions Governing Cloud Services and Data Usage Agreement includes columns that identify which provisions are mandatory depending on whether the data is Public or Non-Public. The data classification for this procurement is Non-Public. The mandatory clauses are determined by the checkmark in the appropriate Public/Non-Public column in each agreement.

Associated Links:
Terms and Conditions Governing Cloud Services and Data Usage Agreement
Terms and Conditions Governing Cloud Services and Data Usage Policy

The contractor has the option to conditionally accept or reject any clause in the agreement. In such cases, the contractor will list the agreement clause number, state whether the clause is “accepted conditionally” or “rejected,” and describe the reasoning and/or controls in place to ensure compliance with the same or similar requirements. Any exception identified by the contractor will be vetted by the Delaware Department of Technology and Information (DTI) and the Delaware Deputy Attorney General (DAG). Individual clauses may be negotiated and updated by the DTI and DAG, and the negotiated agreement version will be attached to the final contract.

During the Operations and Support Phase, the contractor will renew the Terms and Conditions Governing Cloud Services and Data Usage Agreement every 12 months.

4.3.1 Criminal Background Check

All vendor staff working on this project will be subject to a Criminal Background Check (CBC). Vendor will be solely responsible for the cost the CBC. DHSS will review the CBC results. DHSS at their sole discretion may request that a vendor staff be replaced if their CBC result is unsatisfactory.

4.3.2 Cyber Liability Insurance

All data in transit must be encrypted whether transmitted over a public or private network. If vendor cannot comply with the requirement to encrypt data at rest, then vendor must purchase adequate Cyber Liability Insurance to protect vendor and the State from data breaches and other cyber security issues. The selected vendor will present a valid certificate of cyber liability insurance for attachment to the contract prior to contract signature.

4.3.3 Subcontractors

Subcontractors are not required to sign the CSA or the DUA; however, the vendor will hold them responsible to the same or more stringent security requirements to ensure that State data is adequately secured.

4.4 HIPAA Regulations

PDDS shall certify compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations and requirements as described in Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162 and 164 along with the updated ARRA and HITECH act provisions, as well as all HIPAA requirements related to privacy, security, electronic transaction and code set standards, and provider enumeration (National Provider Identifier). The proposed solution must meet these cited requirements.

4.5 Business Associate Agreement

Because the data includes Protected Health Information (PII), which is covered by HIPAA regulations, a Business Associate Agreement (BAA) is required to sign a contract. Typically, a contract uses the DHSS or DPH BAA; however, DPH has agreed to use the vendor BAA, which was already vetted and approved by the Delaware Department of Technology and Information (DTI) and the Delaware Deputy Attorney General (DAG).

4.5.1 Subcontractors

Subcontractors are required to sign a BAA.

4.6 PDDS SaaS Agreement

The contract will include the vednor SaaS Agreement, which was already vetted and approved by the Delaware Department of Technology and Information (DTI) and the Delaware Deputy Attorney General (DAG).

4.7 DHSS Data Rights

All data covered by this contract is the sole property of DHSS. De-identified or derived/aggregated DHSS data is not exempted from this requirement. This provision shall survive the life of the contract. PDDS does not acquire any right, title, or interest in DHSS data under this contract. Except as otherwise required by law or authorized by DHSS in writing, no DHSS data shall be retained by vendor for more than 90 days following the date of contract termination. After the 90-day timeframe the following provisions will remain in effect: vendor will immediately delete or destroy this data in accordance with NIST standards and provide written confirmation to DHSS; vendor is expressly prohibited from retaining, transferring, repurposing, or reselling DHSS data except as otherwise authorized by DHSS in writing; vendor retains no ongoing rights to this data except as expressly agreed to by DHSS in the contract.

4.8 UAT and Training Environments

The User Acceptance Testing (UAT) and Training environments must be secured at a level equivalent to the security in place for the production environment. It must be sized and architected such that production-sized files can be copied over into UAT. The architecture must be equivalently configured so that performance and load testing will essentially produce the same results and expectations as testing in the production environment. Depending on the type of data (i.e., top secret/highly confidential, behavioral health) and specific security requirements around this data, there may or may not be an expectation to mask field values in the UAT and Training environments. Copying production data into lower environments may be prohibited especially for role-based training. Lower environments with production data that are secured in the same manner may be exempt from masking requirements as well however this may be subject to DHSS or Federal policies and regulations that override this potential exemption or explicitly disallow production data being copied into lower environments. The division Deputy Attorney General will be consulted on what is allowed/disallowed in non-production environments.

4.9 Data Masking in Non-Production Environments

While securing of production data is of critical importance, migration of that data to lower environments (e.g., development, testing, training) presents its own set of challenges as lower environments typically are not as secure as the production environment. Masking of production data in lower environments usually involves deletion or obfuscation of actual PII-related field values such that they have no meaning as plain text and there is no identifiable method of translation back to the original values. If vendor intends to include production data in a non-production environment, then vendor is required provide a detailed description of their masking approach, and DPH will amend this section of Appendix B. Otherwise, if vendor does not intend to include production data in a non-production environment, then this section of Appendix B will be amended as such by DPH. This section must be amended before a contract can be signed.

4.10 Help Desk

Vendor shall provide help desk services to all users by phone and email, and optionally through the internet using a secured online chat session. Vendor shall operate the Help Desk 24 hours per day and 7 days per week. Vendor will acknowledge all help desk tickets to the user(s) by email within 5 minutes of receipt, and assign the ticket priority (regular, priority) within 15 minutes of receipt. Vendor will resolve priority tickets within an hour of receipt, and regular tickets within 4 hours of receipt. In addition, vendor will provide emails to the user(s) alerting them of the ticket progress (in process, resolved, closed with no action), provide contact information of the staff assigned a ticket in process; and when a ticket is resolved or closed, an explanation of the resolution or closure.