ATTACHMENT A -- EMERGENCY MEDICAL SERVICES
Bidder:_____
PROJECT EXPERIENCE
Number of years as an EMS PCR vendor, if applicable?
Number of state run EMS PCR implementations, if applicable?
Number of new state run EMS PCR implementations over the last 3 years?
What is the bidder's average state run EMS PCR retention?
SCOPE OF WORK SPECIFICATIONS
PROJECT MANAGEMENT
Designated Account Manager for the life of the contract whose role is to ensure business requirements are being fulfilled and be an escalation point for questions and support.
Designated Project Manager to coordinate and schedule implementation, configuration and associated deliverables.
Bidder must provide a general project schedule of each major phase to include timeline, data migration from current vendor, implementation, configuration, testing and training. General project schedule must be attached to bidder response.
Upon contract award, bidder must provide a detailed project schedule that must include, at a minimum:
Business analysis
Establish test and production environments
System setup
System configuration
Data migration and configuration
Testing and acceptance
Training and assistance
GENERAL SYSTEM REQUIREMENTS
Bidder must provide software compliant with the most current NEMSIS data standard and continue to meet future NEMSIS data set standards going forward at no additional cost to DHHS. Bidder must be on the NEMSIS Compliant Software for State Systems vendor list.
Identify a comprehensive list of hardware and software needed by users at DHHS and EMS agencies to allow access and use of the system.
Bidder must provide a solution that is web-based and hosted by the bidder who will be responsible for the database and technical infrastructure.
Allow data collection, analysis and reporting by authorized users via a web-based application using:
Desktops
Laptops

Tablets
iPad
Smart phones
System(s) should be capable of functioning on common browsers.
Operate efficiently with all Internet connections including broadband, wireless and mobile connections.
Allow an unlimited number of users.
The EMS PCR system must be scalable for data storage.
Bidder will supply a live and test environment of the proposed software solution.
Bidder will provide migration of data to newer versions of software as implemented.
EMS PCR SYSTEM FUNCTIONALITY
The system shall allow for the customization of workflows.
Allow for the ability to show or hide data elements based on pre-determined rules (for example supplemental injury fields will not be displayed if no injury is documented).
Allow for users to select from lists of pre-determined answers allowed by NEMSIS or DHHS. Sort order of lists should be controlled by DHHS system administrators.
Ability to prepopulate fields at the EMS agency level.
Allow the DHHS system administrators to control baseline validation, e.g. ability to make a data element required for the entire system.
Allow individual EMS agencies to control additional validation for their EMS agency only.
Required fields must be visually highlighted.
Bidder's software should provide either a score or indicate the completeness of the PCR.
The system should calculate field values whenever possible, e.g., age, Glasgow Coma Score and Revised Trauma Score, allow for multiple stroke scales to be scored at once (e.g. Cincinnati Stroke Scale and RACE Scale).
The system will allow for the live (real-time) data entry or the collection of data offline being cached until connected to the Internet to be uploaded.
Previously entered patient care records should be maintained with the ability to bring past patient data into new incident records (e.g. address, medications, past medical history, demographics, etc.).
Allow for the development of template PCR forms by DHHS that can be copied and modified at the EMS agency level to assist with the facilitation of data entry. PCR forms modified at the EMS agency level will be unique only to that EMS agency.
Allow for changes made to template PCR forms by DHHS to cascade down to copied PCR forms at the EMS agency level.
Does the bidder have template PCR forms available for DHHS system administrator modification.
Allow for the tracking of multiple patients for a single incident.
Users have the ability to save and exit a partial patient care record without completing the record and return to finish at a later time.
Past PCR records can be easily retrieved for review and modification. Search parameters must be customizable.
System should auto save patient care records periodically.

Users with multiple EMS agency affiliations may use a single user ID and password and select the relevant EMS agency affiliation. Users may have different security or access levels at each EMS agency.
Bidder's system should allow for the sharing of patient care records with EMS agencies providing care with or transferring care to another EMS agency for the same patient within the same incident (e.g. BLS EMS agency requests ALS EMS agency intercept).
Allow state and agency level users to create customized questions, data elements with appropriate formats (i.e. mm/dd/yyyy) and labelling without additional programming by the vendor. Custom data elements created at the EMS agency level should not impact the state level data set.
The EMS PCR System must be able to import patient data from all major cardiac monitor manufacturers to include, but not limited to, 12-lead ECG, vitals, capnography waveforms, etc.
Integration with Computer Aided Dispatch systems to allow for the import of times, address, caller complaints, etc.
Allow for the upload of supplemental documentation such as pictures, pdf, word, etc.
System should allow for the capture of electronic signatures that will allow:
Patient, provider and other types of signatures.
Customizable narrative to provide descriptions of the what and why the signature is being collected.
Tracking and sign off of items such as narcotics administered.
Incorporate data entry tools to reduce repetitive entry and allow for users to quickly enter a set of pre-answered data elements (for example incident address is same as patient address or when entering a medication, dose, administration route, outcomes, etc. at once)
Allow for EMS PCR records to lock and not be edited after a set amount of time or other variable determined by the EMS agencies. Records should only be unlocked by specific end user groups.
Allow for the EMS PCR to have a status field that can be changed. For example in progress, completed, needs reviewed, ready for billing, etc.
Allow the EMS PCR system to restrict medications and procedures to a specific license level and allowed by the respective scope of practice.
SECURITY, SECURITY FEATURES, AND CONFIDENTIALITY
EMS PCR System must be securely accessed via internet connection.
EMS PCR System must prevent unauthorized access to the system.
Allow an unlimited number of end user permission groups.
DHHS shall have full administrative rights and access over all system(s) functions.
Meet or exceed Health Insurance Portability and Accountability Act (HIPAA). Bidder will explain how information is stored and the security to protect PHI.
Must include procedures for safeguarding the system from unauthorized modifications.
Bidder shall provide an audit trail for all submissions, access, print, create, read, update, and delete operations performed on submitted data records including user name and date/time. These reports should be compliant with all HIPAA requirements.

Bidder shall describe the end user security protocols including password protocol, end users ability to reset lost or expired passwords, automatic log off procedures, and administrators ability to lockout user(s).
Describe how the product meets HITECH, and other security requirements.
Provide secure system hosting, maintenance and support.

The solution must allow publishing data exports in industry-standard formats (XML, JSON, CSV, Excel) to support data upload into the State Data Warehouse tools and systems including platforms like Snowflake and Tableau where appropriate. The solution must export system queries into other common formats to be used externally (e.g., Excel, CSV).

Data is to be housed on servers that are: Physically secure with procedures for control of security. Backed up on servers in a minimum of two (2) different locations. Provide detailed responses for the process, procedure and communication plan to prevent data loss, disaster recovery of data, or security breaches. Operational 99.8% of the calendar year. Quarterly reports are to be provided that identify operational status during the previous quarter and the process to notify end users the system will be down for planned or unplanned maintenance. Process for security audits.
Bidder will describe the process they will use to report to DHHS any unauthorized access to or security incidents where data may have been compromised within 24 hours.
Ability to adjust or modify EMS agency tree structure, if applicable, to meet business needs of DHHS.
The solution must use a rules engine-like technology where possible to ensure that the business rules are separate from the programming code and the rules can be configured and maintained by businesspeople. The solution system should be configurable as opposed to being hardcoded. The system needs to be data-driven so that business parameters and code lookup tables can be easily updated without changing the application program logic.
Solution must comply with accessibility requirements described in 45 CFR 85 and with State of Nebraska accessibility requirements located at http://www.nitc.state.ne.us/standards/index.html.

Solution must have a Business Continuity and Disaster Recovery (BC/DR) Plan to ensure recovery of all system components in the event of a disaster. The draft version of the BC/DR Plan must: •Be submitted with the proposal; •Be reviewed and approved by DHHS within timeframes agreed in approved work plan. •Be compliant with Federal Guidelines identifying every resource that requires backup and to what extent backup is required. •The BC/DR Plan must, at a minimum, address the following elements: oEstablish the purpose and scope of the BC/DR Plan; oAcknowledge and ensure compliance with applicable HIPAA and HITECH standards; oDescribe the approach and strategy to disaster recovery and business continuity; oDescribe how the plan will meet the MDR specific RTO and RPOs oEstablish roles and responsibilities for managing disaster recovery and business continuity; oIdentify risk areas; oDescribe protocols for managing disaster recovery and business continuity (during and after); oDescribe the approach to ongoing testing and validation of the BC/DR Plan; oDescribe the frequency of updates. At a minimum, the plan must be updated annually, or as needed more frequently.
Solution must provide real time monitoring and alerting for all system components for performance, errors, warnings, and capacity. Also, the Contractor must submit a system performance report with actual system availability and response times to DHHS monthly. Report should calculate based on 24x7 hours less approved maintenance windows. Reports should calculate to the minute. Downtime should be calculated from a full solution level with component calculations optional
Solution must monitor all integrations and interfaces. The solution must identify errors in the integrations (batch, web services, APIs) and immediately notify the required system(s) of the specific errors, where possible.
Solution must comply with all applicable laws and regulations regarding privacy, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), DHHS IT Security Policy, NITC Standards and Guidelines, and the provisions contained in the Business Associate Agreement Provisions – Attachment I.
Solution must document the data sharing and security agreement for any interfaces with external information systems (e.g., solution to outside of the state's authorization boundary). The State recommends the use of CMS Interconnection Security Agreement (ISA)Template https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/Interconnection-Security-Agreement-ISA-Template
Solution must be hosted in an environment that has a Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, has a documented NIST 800-53, or is Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type 2 compliant.

The Solution must provide a comprehensive auditing framework that provides the following features •Maintain a record of all changes made to any item within the system (e.g., data element, business rule, process control, software program), the ID of the person or process that made the change, before and after images of the affected data records, and the date and time the change was made. •Archive and retain audit data based on state retainage requirements •Allow DHHS users to view, filter, and sort the system audit trail, and export audit data in a standardized format (e.g., XML, CSV, ASCII, and RTF). •Provide a configurable option to allow the audit of usage by screen, by data on the screen, and by the user, based on specified timeframes. •provide an audit trail or log which identifies all access to PHI •Retain Audit trail or log data used to identify access to protected health information for a minimum of ten (10) years
The Contractor must describe their maintenance approach for their software product/solution that ensures the following: •All hardware, software, and communication components installed for use by state staff are compatible with the State's currently supported versions of the Microsoft Operating System, Microsoft Office Suite, and the Chrome Browser, and current technologies for data interchange. •The Solution is browser agnostic and must be maintained, updated, and supported with a cadenced and planned schedule. DHHS currently uses Chrome as the browser standard. For provider and client-facing systems, the State of Nebraska requires that the systems support industry-standard browsers such as Chrome, Firefox, Safari, and Microsoft Edge. The Solution should support the current versions of these browsers with minimum backward compatibility for two older browser versions. The Solution roadmap should include plans to maintain compatibility with future browser versions. If a mobile application is offered, it should support both Apple and Android operation systems with at least the current OS plus the prior two versions. •Maintain all hardware and software products required to support the Solution at the most current to -2 version, including patches, fixes, upgrades, and releases for all software, firmware, and operating systems. Any security patches must be maintained at the most current level after thorough testing. •Keep current all software version upgrades within 6 months of release or with approval from State for a modified schedule. •Maintain a product roadmap (updated at a minimum on an annual basis) that provides details regarding planned updates, the timing of product versions/releases, end of support (EOS), and end of life (EOL) for current and past versions. The roadmap should contain information regarding third-party products that the Solution utilizes.

The solution must operate and must meet the following SLA's •The solution must be available 99.5% of the time during State business days. •The solution must notify in advance, within one (1) business day, DHHS and other contractors when the system will be unavailable due to maintenance. •The solution must return to operations (RTO) within 1 business day following an incident (e.g., disaster, power loss, etc.). •The solution must provide for a two (2) hour recovery point objective (RPO) for manual updates, and as necessary to support the RTO requirement. •The off-site system must be operational within twenty-four (24) hours following a service disruption. •The System online access should have a response time of less than 2 seconds for queries and less than 5 seconds for inserts and updates.
The contractor must perform an annual disaster recovery test demonstrating the efficacy of the BC/DR plan and provide an after-action report (AAR) of the test results to DHHS. The report must detail, the scope of the test, what was a success, what failed, what can be improved, and a plan to address those items. Full data restore capability must be demonstrated with no loss of data. The contractor must comply with and assist DHHS in updating and testing existing Security and Disaster Recovery/Business Resumption Plans.
Solution must provide real time monitoring and alerting for all system components for performance, errors, warnings, and capacity. Also, the Contractor must submit a system performance report with actual system availability and response times to DHHS monthly. Report should calculate based on 24x7 hours less approved maintenance windows. Reports should calculate to the minute. Downtime should be calculated from a full solution level with component calculations optional.
The solution integration framework must be standards-based and must meet the following •All data exchanges including inbound and outbound interfaces shall align with the MITA framework and comply with industry standards where applicable (e.g., National Information Exchange Model (NIEM), National Institute of Standards and Technology (NIST), HIPAA-compliance standards, Health level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR)). (164) •The solution must support the use of XML/JSON standards to ensure interoperability. (159) •The solution must comply with the state's existing data interface standard(s) for automated electronic intrastate interchanges and interoperability. •The solution must support multiple web services standards, including web services, specifications, and adapters (WSDL, WS-*, SOAP, REST, UDDI, ODATA), support standard databases such as MS SQL, SQL Server, Oracle and support integration transfer protocols such as FTPS, SFTP, HTTPS, MSMQ).
Solution must monitor all integrations and interfaces. The solution must identify errors in the integrations (batch, web services, APIs) and immediately notify the required system(s) of the specific errors, where possible.

The solution must provide a comprehensive framework for exchanging data with other modules and systems and should meet the following
•The Solution must provide multiple mechanisms of integrating with the existing and planned Nebraska DHHS systems
•The architecture must enable the system to exchange data efficiently, effectively, and appropriately with other participants in the DHHS enterprise
•The solution must have the capability to implement RESTFUL API and/or SOAP-based web services for real-time integration with both State and external systems. The State prefers API first based integration approach for future planned systems.
•When using APIs, the solution must support using the State API Gateway when interfacing within the agency and with intrastate agencies
•The solution must support the update of data integration points with the Nebraska DHHS Systems as DHHS systems are upgraded or replaced
•The solution must use technology-neutral interfaces that localize and minimize the impact of new technology insertion or replacement.

The Contractor must design, develop, and maintain interfaces that support integration with other systems. Each Application Program Interface (API) or batch interface and components that will interface with the other modules and the Systems Integration Services will be documented using the State-provided ICD template. The Interface Control Document (ICD) which will include data layout documentation, data mapping crosswalk, inbound/outbound capability, and frequency of all interfaces. As new interfaces are required, ICDs for those will be created and shared with, and reviewed and approved by DHHS.

Solution must support the use of existing data interface layouts to minimize disruption to existing systems and operations. Solution must support transferring data files using secure protocols such as SFTP. The Solution however must also support data transfer using REST APIs (Application Programming Interfaces) and implement industry standards for interfaces where existing data exchanges to do not exist.

The Department prefers cloud-based hosting for the solution. The delivery of the solution/services should be seamless with the hosting solution providing the flexibility to integrate other solutions for security and regulatory purposes in the future and be cost-effective and scalable.

Contractor must implement, host, and manage access to the following system environments according to federal and state standards (e.g., interoperability, privacy, security, etc.):
•Development
•Test
•Training
•Production

Solution must utilize these environments to allow components to be added or replaced quickly and non-disruptively.

The Contractor must continuously monitor the health of the infrastructure according to the performance expectations outlined in the contract to ensure minimal impact on business operations. The Contractor must report, set alerts and reminders proactively to any degradation of the performance of the infrastructure

Solution must comply with all applicable laws and regulations regarding privacy, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), DHHS IT Security Policy, NITC Standards and Guidelines, and the provisions contained in the Business Associate Agreement Provisions – Attachment C.

Solution must meet and Contractor must document compliance with NIST SP 800-53 and/or NIST SP 800-171, SP 800-53A security and privacy standards, and 508 compliance/VPAT testing through the completion of a System Security Plan (SSP) per Attachment K prior to Go-Live. Contractor must provide a Plan of Action and Milestones (POA&M) for any items not fully compliant. •Compliance is subject to a qualified independent security controls assessment prior to solution implementation. •Security and privacy control requirements may be met by confirmed attestation of compliance (e.g., FedRAMP, SOC. •The Contractor will be responsible for engaging a qualified independent security controls assessment contractor. DHHS shall approve the selection of the security assessment contractor. •Bidder must submit a sample of the SSP with the Technical Proposal.
Solution must document the data sharing and security agreement for any interfaces with external information systems (e.g., solution to outside of the state's authorization boundary). The State recommends the use of CMS Interconnection Security Agreement (ISA)Template https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/Interconnection-Security-Agreement-ISA-Template
Solution must provide an efficient and secure method for viewing and exchanging information with DHHS.
Authorized user(s) must have access to user activity history and other management functions, including but is not limited to log-on approvals/ disapprovals and log search and playback.
Solution must be hosted in an environment that has a Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance, has a documented NIST 800-53, or is Statement on Standards for Attestation Engagements (SSAE-16) SOC 1 Type 2 and SOC 2 Type 2 compliant.

SYSTEM ADMINISTRATION
Have an integrated data validation tool/module to ensure data submitted is accurate and valid. The data validation tool/module must:
Allow the state system administrators to control baseline validation for the entire system.
Allow individual EMS agencies to control additional validation for their EMS agency only.
System should provide an announcement feature or similar functionality so DHHS system administrators can announce system changes.
Allow system administrators to change displayed data element text or list values without impacting the pre-defined data element or value such as NEMSIS data element name or an ICD-10 value.

The Solution must provide a comprehensive auditing framework that provides the following features •Maintain a record of all changes made to any item within the system (e.g., data element, business rule, process control, software program), the ID of the person or process that made the change, before and after images of the affected data records, and the date and time the change was made. •Archive and retain audit data based on state retainage requirements •Allow DHHS users to view, filter, and sort the system audit trail, and export audit data in a standardized format (e.g., XML, CSV, ASCII, and RTF). •Provide a configurable option to allow the audit of usage by screen, by data on the screen, and by the user, based on specified timeframes. •Provide an audit trail or log which identifies all access to PHI Retain Audit trail or log data used to identify access to protected health information for a minimum of ten (10) years
IMPORT AND EXPORT REQUIREMENTS

The solution must allow publishing data exports in industry-standard formats (XML, JSON, CSV, Excel) to support data upload into the State Data Warehouse tools and systems including platforms like Snowflake and Tableau where appropriate. The solution must export system queries into other common formats to be used externally (e.g., Excel, CSV). The solution must provide a comprehensive framework for exchanging data with other modules and systems and should meet the following:

- The Solution must provide multiple mechanisms of integrating with the existing and planned Nebraska DHHS systems
- The architecture must enable the system to exchange data efficiently, effectively, and appropriately with other participants in the DHHS enterprise
- The solution must have the capability to implement RESTFUL API and/or SOAP-based web services for real-time integration with both State and external systems. The State prefers API first based integration approach for future planned systems.
- When using APIs, the solution must support using the State API Gateway when interfacing within the agency and with intrastate agencies
- The solution must support the update of data integration points with the Nebraska DHHS Systems as DHHS systems are upgraded or replaced
- The solution must use technology-neutral interfaces that localize and minimize the impact of new technology insertion or replacement.

REPORTING
Provide a data analysis engine or a report generator that will provide standard (no customization) reports, ad hoc custom reporting and:
The ability to analyze data.
Allows approved users to generate statistical information from the aggregate patient care data through an Internet based query tool.
Allows for dynamic and customized analysis without additional programming by the bidder.
Creates charts with identifying labels and appropriate scientific units.
Provides the ability to export reports into PDF®, Excel® and Word® formats.

Provide standard reports including syndromic surveillance reports.
Provide the ability to schedule reports with various time intervals and with changing parameters.
Allow for reports to directly link to a specific EMS PCR report.
Specific Data Analysis requirements:
Provide the user the ability to apply simple mathematical formulas across data elements. For example, researchers need to be able to take two independent data elements and create a new data field that will contain the sum, difference, average, product, mean, median or quotient of the NEMSIS and DHHS defined data fields.
All data fields in the query and analysis section are to be labeled with their appropriate NEMSIS data element. Conversely, the PCR should have hover help or some other means of identifying which NEMSIS data element is being collected. This will allow researchers to easily evaluate and find the proper data elements even if the data fields have been renamed for familiarity with field users.
Provide DHHS a live or near live data repository to be used for reporting. A data dictionary, how data is linked in tables, what the data elements are in each table, and other relevant documentation must be provided.
Provide DHHS with the ability to import data into other DHHS systems.
TRAINING
Provide train-the-trainer instruction and materials, webinar-based training for users and on-line user manuals for instruction on use of the application with information on data elements that are current and reflect all updates.
Provide implementation training.
Provide post go-live training.
HOSPITAL DATA INTERFACE
The system will interface with receiving medical facilities to appropriately receive EMS PCR information through data upload (preferred) or print capability.
Interface allows for the linkage of patient outcome data from the medical facility and EMS agency.
Bidder's system should allow for the sharing of patient care records with the hospital that an EMS agency transports a patient to. When a patient is transferred to a definitive care hospital, patient care records from the initial 911 EMS agency and the transferring EMS agency should be shared with the definitive care hospital.
EMS PCR must be able to interface with and import into the Trauma Registry System selected by DHHS.
SERVICE, SUPPORT AND ENHANCEMENTS REQUIREMENTS
Provide an assigned account manager for the Nebraska implementation.
Provide a system help file available to all users.
Provide help desk support for DHHS staff available during normal business hours. Describe what support options are available (e.g. phone, chat, support ticket, etc.).
Support must be available 24x7x365 for critical system failures or issues.

Provide the process or procedures for response times for all levels of support, escalation process of support, support tracking system, and support severity level determinations.
Provide new versions released only after they have been fully tested and found to be error free and at a time mutually agreeable with DHHS.
Provide for timely system fixes and resolution of issues deemed critical by DHHS, applied or installed after appropriate testing by the bidder and approval of DHHS.
Have regular maintenance schedule policies, to be provided to DHHS, that explain when the system would not be available to Nebraska users.
Improve the system based on DHHS identification of weaknesses, feature enhancements, and needed adjustments and provide a timeline for completion. Provide a description on how DHHS improvements are prioritized related to other client requests.
Describe the process for the archival, use and retrieval for data.
Provide an internal messaging system to allow for communications between DHHS staff and EMS agencies.
Solution must have a Business Continuity and Disaster Recovery (BC/DR) Plan to ensure recovery of all system components in the event of a disaster. The draft version of the BC/DR Plan must: •Be submitted with the proposal; •Be reviewed and approved by DHHS within timeframes agreed in approved work plan. •Be compliant with Federal Guidelines identifying every resource that requires backup and to what extent backup is required. •The BC/DR Plan must, at a minimum, address the following elements: oEstablish the purpose and scope of the BC/DR Plan; oAcknowledge and ensure compliance with applicable HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) standards; oDescribe the approach and strategy to disaster recovery and business continuity; oEstablish roles and responsibilities for managing disaster recovery and business continuity; oIdentify risk areas; oDescribe protocols for managing disaster recovery and business continuity (during and after); oDescribe the approach to ongoing testing and validation of the BC/DR Plan; oDescribe the frequency of updates. At a minimum, the plan must be updated annually, or as needed more frequently.
DATA MIGRATION REQUIREMENTS
Migrate data from the DHHS's current provider identifying the length of time needed for conversion, testing and implementation of the proposed system(s) to full operational use by DHHS and authorized users. The steps are to include:
Defining data to be imported.
Linking/mapping data to fit the new system.
Testing results.
Importing a complete set of data.

The Contractor must describe their maintenance approach for their software product/solution that ensures the following:

- All hardware, software, and communication components installed for use by state staff ar compatible with the State's currently supported versions of the Microsoft Operating System, Microsoft Office Suite, and the Chrome Browser, and current technologies for data interchange.
- The Solution is browser agnostic and must be maintained, updated, and supported with cadenced and planned schedule. DHHS currently uses Chrome as the browser standard. For provider and client-facing systems, the State of Nebraska requires that the systems support industry-standard browsers such as Chrome, Firefox, Safari, and Microsoft Edge. The Solution should support the current versions of these browsers with minimum backward compatibility for two older browser versions. The Solution roadmap should include plans to maintain compatibility with future browser versions. If a mobile application is offered, it should support both Apple and Android operation systems with at least the current OS plus the prior two versions.
- Maintain all hardware and software products required to support the Solution at the mos current to -2 version, including patches, fixes, upgrades, and releases for all software, firmware, and operating systems. Any security patches must be maintained at the most current level after thorough testing.
- Keep current all software version upgrades within 6 months of release or with approva from State for a modified schedule.
- Maintain a product roadmap (updated at a minimum on an annual basis) that provide details regarding planned updates, the timing of product versions/releases, end of support (EOS), and end of life (EOL) for current and past versions. The roadmap should contain information regarding third-party products that the Solution utilizes.

DATA OWNERSHIP REQUIREMENT

All data collected by the system(s) will be owned exclusively by the DHHS and transferrable in a format approved by DHHS to it or its designee upon contract termination/expiration.

END OF CONTRACT REQUIREMENT

The bidder shall be responsible for end of contract activities at the completion of the contract to ensure that the transition from bidder's operations by the successor or DHHS occurs smoothly and without disruption to DHHS. End of contract transition activities will include planning, transfer of data and documentation specifically for Nebraska at no additional cost in an agreed upon timeline. This obligation survives the termination of the contract.

CUSTOM PROGRAMMING

The bidder shall provide hourly pricing for any current and future custom programming needs to meet specific requirements for EMS PCR as requested and mutually agreed upon by the bidder and DHHS.

OPTIONAL - The following are independent and optional only. Include each as optior

Community paramedicine functionality to include but not be limited to development of medical charts, outcome measure, patient visit document, etc. These data fields may not be included in the NEMSIS data set at this time or in the future. Allow for the integration with an electronic health record system.
Critical care paramedic documentation module to assist in the documentation of care and procedures provided at the critical care level. This option should integrate with the EMS PCR. These data fields may not be included in the NEMSIS data set at this time or in the future.
Provide integration solutions to prevent the duplication of data entry for migration of common data elements for the following registry types:
CARES
STEMI
Stroke
Education module or functionality to allow EMS agencies to track and maintain training and education hours provided or attended by each employee.
Quality Improvement module to allow for the comprehensive EMS PCR reviews by physician medical directors.
Inventory module to allow EMS agencies to manage ambulance and medical supply inventory.
Checklist functionality to all EMS agencies to perform daily, weekly, monthly maintenance and inspection checks.
App available for the use on mobile devices.
Provide secure integration solutions to state Health Information Exchange (HIE).
Allow for the ability to purchase and incorporate changes provided by the Contractor.
ADDITIONAL SO
Provide a detail of any additional software features not already covered and if they are included in the cost or at additional cost.

(EMS) PATIENT CARE REPORTING (PCR) REQUIREMENTS

			114658 O3
	EXPLANATION		
YES, INCLUDED	YES, ADDITIONAL COST	NO	EXPLANATION

nal in bidder's response and cost proposal.

FTWARE FEATURES
