ATTACHMENT 3
Technical Specifications
Vital Records Management System
Request for Proposal Number 120277 O3

Bidder Name: _____

Important Scoring Dynamic: Attachment 3 – Technical Specifications shall be subject to a "Pass" or "Fail" assessment. Bidder to review Section (I)(P)(2) of the Request for Proposal (RFP) document for understanding the methodology that will be applied. The items highlighted in <mark>gold</mark> and notated with an asterisk (*) within this document represent the capability and/or requirement that will be subject to the "Pass" or "Fail" assessment, as these are "must" requirements.

Instructions: Bidders shall review the tables below to understand the structure of this document and how to effectively complete this attachment for inclusion with the RFP submission. See section (VII) of the Request for Proposal for instructions on how to include with your Technical Response. Failure to include this completed attachment shall result in the bidder's Solicitation Response as being deemed a "Non-Responsive Solicitation Response". DO NOT ALTER THE FORMAT OR ANY OF THE EXISTING CONTENT WITHIN THIS DOCUMENT. Bidder may increase the size of the response box to provide the necessary information. If the response includes other attachments, bidder to indicate that information in the response box. Such attachments must be included with the completed "Attachment 3 – Technical Response".

This document is comprised of four (4) separate categories that are expressed in the table directly below. Each category is identified by the following initial characters:

Category	Description
ARCH	Architecture Capabilities and/or Requirements
SPC	Security and Compliance Capabilities and/or Requirements
DM	Database/Data Management Capabilities and/or Requirements
OM	Operations Management Capabilities and/or Requirements

Each category above contains multiple sub-categories. The table directly below describes the functionality of each column:

Column Description	Bidder Responsibility
Req #	The unique identifier for the item as assigned by the State of Nebraska.
Capability and/or Requirement	The description of the item to which the Bidder shall respond.

CAPABILITIES AND/OR REQUIREMENTS

How to complete the Capabilities and/or Requirements: Bidders shall provide information in each respective "Response" box provided. Each individual response shall include the information as indicated. Such responses shall include specific details, characteristics and key aspects to demonstrate the bidder's proposed solution and how it meets the conformance specification outlined in relation to the project. Use the format provided to complete this attachment in its entirety. Do not alter the color coding, content, or format of this attachment.

Architecture Capabilities and/or Requirements

Req #	Capabilities and/or Requirements
ARCH-1	Describe the bidder solution to addressing the following architectural details: **Technology Architecture**: Describe the software components, including third-party software products, open-source libraries, and utilities that complete the platform for running a service or supporting an application. This section should document any technical requirements for accessing the software, including but not limited to client desktop installs, etc. Further, the section should clearly outline any State required infrastructure, such as setting up VPN, SFTP, etc., to implement or operate the system. **Network Architecture**: Describe the means of communication, the method of sending and receiving information, between the assets in the Technology Architecture. **Application Architecture**: Describe how the solution components are assembled and interact to meet the business needs. Describe the solution's ability to manage and store documents and attachments. **Data Flow Architecture**: Describe the data flows into and out of the system boundary, include transmission and storage, along with ports, protocols, and services of all inbound and outbound traffic.
Response:	
ARCH-2*	The bidder solution must be a cloud-based hosted environment with all components and data residing in the United States and consisting of ready-made software products that do not require major modifications but support customization to meet the functional specifications as outlined in Attachment 2 – Functional Specifications. Bidder must describe how their approach will meet these requirements.
Response:	
ARCH-3	Describe the bidder solution to address the following: • Type of Software – SaaS, PaaS or, IaaS • Licensing Model- Perpetual or Subscription based licenses • Single or Multi-Tenant architecture
Response:	

Req #	Capabilities and/or Requirements
ARCH-4*	The bidder solution must provide multiple environments concurrently to support functions including production, testing, and training. Bidder must describe how their approach will meet these requirements.
Response:	
ARCH-5*	Review the accessibility requirements described in the following: • Section 508 compliance standards (https://www.section508.gov/manage/laws-and-policies/) • 45 CFR Part 85 (https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-85) • State of Nebraska Accessibility requirements (https://nitc.nebraska.gov/standards/index.html#2). Bidder must confirm that your company has read, understands, and can meet all the capabilities and/or requirements as outlined for each of the items and indicate how your solution will meet such requirements as they relate to the accessibility requirements.
Response:	

Security and Compliance Capabilites and Requirements

Req #	Capabilities and/or Requirements
SPC-1*	Review the standards and policies described in the following: • DHHS Information Technology (IT) Security Policies and Standards (http://dhhs.ne.gov/ITSecurity). • Nebraska Information Technology Commission (NITC) Standards and Guidelines (https://nitc.nebraska.gov/standards/index.html). • Health Insurance Portability and Accountability Act (HIPAA) of 1996. Bidder must confirm that your company has read, understands, and can meet all the capabilities and/or requirements as outlined for each of the items <u>and</u> indicate how your solution will meet such requirements as they relate to the standards and policies described above.
Response:	
SPC-2*	The bidder must agree to conduct an independent, third-party penetration test for the solution in which they are offering within one year prior to the anticipated go-live date, that includes, at a minimum, the Open Web Application Security Project (OWASP) Top 10. Identified risks must be classified by severity and additional information must be provided for any risks identified as medium and above. This must be conducted at no additional charge to the State. Bidder must confirm their intent to conduct this test at the appropriate time and describe how their approach will meet these requirements.
Response:	
SPC-3*	The bidder must agree to conduct an annual independent third-party penetration test of the solution that includes the Open Web Application Security Project (OWASP) Top 10. The report must provide details of the critical, high, and medium findings and associated risks. This must be conducted at no additional charge to the State. Bidder must confirm their intent to conduct this test at the appropriate time and describe how their approach will meet these requirements.
Response:	
SPC-4*	The bidder must agree to conduct an independent, third-party security and privacy controls assessment that aligns with the National Institute for Standards and Technology (NIST) SP 800-53 moderate standard, within one year prior to the go-live date. Identified security gaps must be classified by severity and additional information must be provided for any gap identified as medium and above. This must be conducted at no additional charge to the State. Bidder must confirm their intent to conduct this assessment at the appropriate time and describe how their approach will meet these requirements.
Response:	

Req #	Capabilities and/or Requirements
SPC-5*	The bidder must agree to conduct an annual independent third-party security controls assessment that meets the National Institute for Standards and Technology (NIST) SP 800-53 moderate standard. The report must provide details of the critical, high, and medium findings and associated risks. This must be conducted at no additional charge to the State. Bidder must confirm their intent to conduct this assessment at the appropriate time and describe how their approach will meet these requirements.
Response:	
SPC-6	Describe the bidder solution for the following: • Support for self-service password activities. • Automatic log-off procedures after determined time of session inactivity. • Automatic account disablement after 120 days of inactivity. • Administrators' ability to lockout user(s). • Support and approach for single sign-on • Support and approach for Multi-Factor Authentication • Automatic locking of account after determined number of failed logon attempts.
Response:	
SPC-7*	The bidder solution must use role-based security. Bidder must describe how their approach will meet this requirement.
Response:	
SPC-8	Describe the bidder solution for the following: • How user accounts are assigned and managed. • How the system provides usage reports, such as a listing of all users and their last usage date. • How the system supports authorization at an attribute/field level (e.g., edit, view).
Response:	

Req #	Capabilities and/or Requirements
SPC-9*	Review the State DHHS Information Technology (IT) Audit Standards located at: (https://www.dhhs.ne.gov/ITSecurity). Bidder must confirm that your company has read, understands, and can meet all the capabilities and/or requirements as outlined and indicate how your solution will meet such requirements. As a part of the bidder's response, at minimum, the State desires specific information regarding the following elements: • Detail the data elements that are audited. • Outline the level of audit tracking being maintained. • Provide a sample of their audit reports. • Capabilities for automated audit log evaluation to identify security issues. • How the bidder monitors, identifies, and reports on events impacting the system, such as attacks and other unauthorized use of the system.
Response:	

Database/Data Management Capabilities and/or Requirements

Req #	Capabilities and/or Requirements
DM-1*	The bidder solution must use industry standard cryptographic modules such as those certified to meet FIPS 140-2/-3 for encrypting data at rest and in transit. Bidder must describe how their approach will meet this requirement.
Response:	
DM-2*	The bidder solution must securely dispose of State data from its systems upon request and in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf) and must provide to the State of Nebraska a certificate of data destruction. Bidder must describe how their approach will meet this requirement.
Response:	
DM-3	Describe the bidder's technical approach for supporting data conversion and data migration.
Response:	
DM-4*	The bidder's solution must support data integration. The bidder must confirm and describe how their solution will meet this requirement. In addition to confirmation on the ability to meet the requirement, the response must include the following, at a minimum the following details: :• Ability to import and export data using these file types (XML, JSON, CSV). • Support for integration using industry standards approaches and principles for REST APIs and Webservices. • Support for industry integration data standards for Health Level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR), X-12, HIPAA.
Response:	
DM-5	Describe bidder solution for the following: • Documentation to support testing and collaboration with integrating systems. • Documentation of the system's data dictionary which includes user-defined fields and tables.
Response:	

Req #	Capabilities and/or Requirements
DM-6*	Review the data retention requirements described in the following: • 45 CFR Part 164.316 (https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316) • DHHS Vital Records retention schedule is to retain information permanently. Bidder must confirm that your company has read, understands, and can meet all the capabilities and/or requirements as outlined for each of the items <u>and</u> indicate how your solution will meet such requirements as they relate to the data retention requirements.
Response:	

Operations Management Capabilities and/or Requirements

Req #	Capabilities and/or Requirement

OM-1	Describe the Business Continuity and Disaster Recovery (BCDR) plan for the solution they are offering. Bidder's response must describe, at a minimum, their plan to include the following information:
	• Procedures for data backup, restoration, communication to the State of Nebraska, and emergency mode operations in the event of:
	    a. Hardware or Software Failures.
	    b. Human Error.
	    c. Natural Disaster; and/or
	    d. Other unforeseeable emergencies.

Response:	
OM-2*	The bidder must agree to conduct a full disaster recovery test for the solution in which they are offering prior to the anticipated go-live date. The most recent test must be within one year prior to the go-live date. This must be conducted at no additional charge to the State. Bidder must confirm their intent to conduct this test at the appropriate time and describe how their approach will meet these requirements.
Response:	
OM-3*	The bidder must agree to conduct an annual disaster recovery test for the solution and submit the annual results to the designated individual for the State of Nebraska. This must be conducted at no additional charge to the State. Bidder must confirm their intent to conduct this test at the appropriate time and describe how their approach will meet these requirements.
Response:	

Req #	Capabilities and/or Requirement
OM-4	Describe the bidder solution for ability to meet the following: • Compliance with the Recovery Time Objective (RTO) of within twelve (12) hours when the system outage is declared as a disaster. • Compliance with the Recovery Point Objective (RPO) of fifteen (15) minutes of data lost before the disaster event.
Response:	
OM-5	Describe the bidder solution for the following: • Overall testing strategy and support for the following testing types: unit testing, system testing, integration testing, regression testing, user acceptance testing (UAT), parallel testing, performance and load testing, manual and automated and/or scripted testing, and end-to-end integration testing. • Approach to planning and preparing the test/staging environment. • Approach to conducting each test level. • Approach for testing nonfunctional requirements (security, performance, etc.) • Approach to test documentation (e.g., test cases, test scripts, test case matrices added as the design configuration progresses). • Approach to quality control/quality assurance. • Approach to test results reporting, traceability, and metrics.
Response:	
OM-6	Describe the bidder solution for software maintenance processes that address the following: • Approach to managing software versions to ensure bidder support. • Approach to Change Management, including defects and enhancements. • Approach to testing and release management. • Approach to maintaining integrations with external and internal trading partners.
Response:	
OM-7	Describe the incident management process that will be used to report business and security incidents (such as any unauthorized access to, or incidents where, data may have been compromised).
Response:	
OM-8*	The bidder's solution must be responsive to mobile technology devices such as smartphones or tablets. Bidder must describe how their approach will meet this requirement.
Response:	

Req #	Capabilities and/or Requirement
OM-9*	The bidder's solution must provide Scalability and High Availability Architecture. The bidder must confirm and describe how their solution will meet this requirement. In addition to confirmation on the ability to meet the requirement, the response must include the following, at a minimum the following details: • The system architecture must support scaling with increased load. • The system must provide high availability to support minimum disruptions to the business operations. • The system must handle notifications when a component or interface endpoint is unavailable. • The system must handle performance functionality and monitoring tools. • The system must handle recovery of failed transactions because of a component failure. • The system must be available online 24 hours a day and 7 days a week, 99.9% of the time each month excluding scheduled downtime.
Response:	