Attachment 2

Technical Requirements Traceability Matrix

Draft EHR 2017

Bidders shall complete a Technical Requirements Traceability Matrix for Electronic Health Record Solution. Bidders are required to describe in detail how their proposed solution meets the conformance specification outlined within each Technical Requirement.

The traceability matrix is used to document and track the project requirements from the proposal through testing to verify that the requirement has been completely fulfilled. The contractor will be responsible for maintaining the contract set of Baseline Requirements. The traceability matrix will form one of the key artifacts required for testing and validation that each requirement has been complied with (i.e., 100% fulfilled).

The traceability matrix must indicate how the bidder intends to comply with the requirement and the effort required to achieve that compliance. It is not sufficient for the bidder to simply state that it intends to meet the requirements of the RFP. DHHS will consider any such response to the requirements in this RFP to be non-responsive. The narrative should provide DHHS with sufficient information to differentiate the bidder’s technical solution from other bidders’ solutions.

The bidder must ensure that the original requirement identifier and requirement description are maintained in the traceability matrix as provided by DHHS. Failure to maintain these elements may be grounds for disqualification.

How to complete the traceability matrix:

Column Description	Bidder Responsibility
Req #	The unique identifier for the requirement as assigned by DHHS, followed by the specific requirement number. This column is dictated by this RFP and must not be modified by the bidder.
Requirement	The statement of the requirement to which the bidder must respond. This column is dictated by the RFP and must not be modified by the bidder.
(1) Comply	The bidder should insert an "X" if the bidder's proposed solution complies with the requirement. The bidder should leave blank if the bidder's proposed solution does not comply with the requirement. If left blank, the bidder must also address the following: • Capability does not currently exist in the proposed system, but it planned in the near future (within the next few months) • Capability not available, is not planned, or requires extensive source-code design and customization to be considered part of the bidder’s standard capability • Requires an extensive integration effort of more than 500 hours
(a) Core	The bidder should insert an "X" if the requirement is met by existing capabilities of the core system or with minor modifications to existing functionality.
(b) Custom	The bidder should insert an "X" if the bidder proposes to custom develop the capability to meet this requirement. Indicate "custom" for those features that require substantial or "from the ground up" development efforts.
(c) 3rd Party	The bidder should insert an "X" if the bidder proposed to meet this requirement using a 3rd party component or product (e.g., a COTS vendor, or other 3rd party). The bidder must describe the product, including product name, its functionality and benefits in their response.

Nebraska DHHS Enterprise Architecture Standards

The Nebraska Department of Health and Human Services (DHHS) is establishing an Enterprise Architecture program that focuses on a holistic approach for engaging with our business partners, designing and implementing IT centric solutions, governance, and a continuous improvement philosophy. The goals of this program include the following:

1. To enable process consolidation and standardization
2. Facilitate a DHHS enterprise roadmap
3. Assist with project scoping and consistent project deliverables
4. Improve agility and adaptability to changes within the DHHS programs
5. Provide agency-based solutions to promote reusability and lower overall costs to DHHS and the State of Nebraska.

As project initiatives become available, DHHS will look for ways to build upon the vision of the enterprise architecture through the procurement of technologies, services, and methods which form a foundation for best practices as it relates to our Enterprise Architecture. To that end, certain technologies, via other initiatives, have been procured. DHHS intends to look for opportunities and explore options to reuse these existing assets within the context of new projects and initiatives, such as the DMA.

Through previous and present project initiatives a number of foundational technologies that support our Enterprise Architecture have been procured and are being implemented. The implementation of these technologies will establish a set of key capabilities to be leveraged, the methods for use, and the processes associated with ongoing governance and support. The remainder of this section will introduce the foundational technologies and key capabilities currently available or planned, and the products used to provide them. Bidders should consider these areas as they prepare their solutions and proposals, as the selected bidder will ultimately need to integrate with, or possibly leverage, the capabilities described.

Information Integration

With the organizations' vision of utilizing independent, best of breed systems and services to provide business functions comes the need to integrate the functions into a unified solution. This requires the ability to integrate at a number of levels, including user interfaces, business processes, functional and technical services, and information. In particular, information integration will need to address how to integrate the information processed within the various operational systems, as well as how to bring that information together in order to support cross system reporting, decision making, and analysis. For these reasons, DHHS has identified information integration as a foundational technology.

The information integration capability consists of a collection of sub-capabilities that includes data quality, and data transformation and delivery. These capabilities are intended to be used during the project to support the data conversion process, and post-implementation to support both operational systems integration and the data warehousing environment. During data conversion, the data quality capabilities are used to profile the source data to assess the quality of the data and to identify any anomalies. Based on the data profiling results, data cleansing and transformation rules are developed and performed using the transformation and delivery capabilities. Post-implementation the data transformation and delivery capabilities provides functions such as extraction, transformation and load (ETL) that supports preparation and loading of data into the data warehouse environment. DHHS has chosen the IBM InfoSphere Information Server for Data Integration and IBM InfoSphere Information Server for Data Quality products to support data quality, and data transformation and delivery capabilities.

Metadata Repository

As the organization integrates systems and information, a better understanding of the information contained within those systems is paramount. The Metadata Repository has been identified as the foundational technology to aid DHHS in this area. The Metadata Repository will ultimately provide the organization with a single location where the metadata contained in systems throughout the organization will be collected and catalogued. This will assist in developing a common understanding of the information and establishing consistent data definitions and a common vocabulary. The Metadata repository will also contain the necessary information to support tracking data lineage, which will help the organization build and maintain a strong data governance and stewardship program. The IBM InfoSphere Information Governance Catalog product is being used to provide these capabilities.

Enterprise Service Bus

Whether integrating at the process level or the data level, or via real-time web services or batch file transfer, communications between the systems is critical. The enterprise service bus (ESB) is the foundational technology that provides this capability. The ESB allows the organization to connect an array of independently deployed, heterogeneous software and services, thereby reducing the need to develop complex point-to-point connections. This is accomplished through the use of ESB capabilities such as message routing, protocol conversion, service orchestration, and process choreography to name a few. The ESB establishes a standardized and flexible integration foundation, which will allow the organization to support business changes more quickly. The ESB selected to establish this foundational technology is the IBM Integration Bus (IIB), formerly IBM WebSphere Message Broker.

Service (SOA) Registry and Repository

The Enterprise Architecture identifies the use of a Service Oriented Architecture as a key principle, which means that as the organization moves forward it will have a greater number of service (web and otherwise) to manage. In order to ensure that the organization realizes the benefits of using services it was determined that a service registry and repository needed to be a foundational technology. By implementing the service registry and repository capabilities, the organization will have a greater visibility of the services in the environment, and will be able to better manage and control the services environment. The service registry and repository supports the organizations service lifecycle management and service governance processes. It is used to auto discover and catalog services in the environment, track service versions and availability, and to establish and enforce service policies. This capability is provided by the IBM WebSphere Service Registry and Repository (WSRR) and IBM SOA Policy Gateway products.

Master Data Management

As the organization realizes its vision, the number of disparate systems and services in the environment will grow. With this growth, it is inevitable that these systems will duplicate and store their own version of critical data entities that occur across the organization, entities such as client and provider. These entities contain data known as Master Data, which refers to data elements that should be shared across the systems, data elements such as Social Security Number, address and last name. Master data management (MDM) is the set of processes, policies and standards used to link this critical data together in order to provide a single point of reference. Successful master data management will provide the organization with a trusted view of these critical entities. It is for these reasons that the Enterprise Architecture includes MDM as a foundational technology. As part of a current project initiative, the organization is establishing a Master Client Index (MCI) registry and the corresponding governance processes. The MCI will be used to synchronize client data across all systems, and to provide other systems with the ability to cross-reference clients across the systems. The plan is to build a Master Provider (MPI) Index registry as part of future project initiatives. The Master Data Management foundational technology and associated registries will be realized using the IBM InfoSphere Master Data Management Individual Hub for Non-Financial Services and IBM InfoSphere Master Data Management Patient Hub products.

Reporting and Business Intelligence

As part of current and planned project initiatives, the organization will be building out data warehousing environments. In order to reap the full benefit of these environments, the organization needs to include Reporting and Business Intelligence (BI) capabilities, so they have been designated foundational technologies within the Enterprise Architecture. The Reporting and BI capabilities include support for creating and distributing standard production reports to support operational business reporting requirements, and the ability for users to develop and run reports and queries to support ad-hoc requests. In addition, these capabilities will include the ability to perform complex queries and data analysis to support decision making and business planning. The organization has chosen the IBM Cognos Business Intelligence Analytics product suite to provide these capabilities.

Data Masking, Redaction and De-Identification

Protecting the security and privacy of sensitive information is of the utmost importance to the organization, which is why it is a key principle within the Enterprise Architecture. The use of production data for non-production purposes is becoming more common, in fact, current and future project initiatives plan to use it to support data profiling, to create production-like test data, and to create de-identified data to be shared with internal and external agencies for analysis. Therefore, the organization has established an Architectural Guideline to ensure that production data is sanitized before using it for any non-production purpose, and has classified Data Masking, Redaction and De-Identification as a foundational technology. IBM's InfoSphere Optim Data Privacy Enterprise Edition is the delivery vehicle for the capabilities.

TECHNICAL REQUIREMENTS

The following requirements describe what is needed to support DHHS technical project operations.

Each requirement is identified by the following first three characters:

TEC	General Technical Requirements
STN	Standards Requirements
ERR	Error Handling Requirements
DBM	Database/Data Management Requirements
BKP	Backup and System Recovery Requirements
SEC	Security Requirements
DOC	System and User Documentation
TRN	Training
PTT	Production, Test and Training Requirements
INT	Interfaces/Imports/Exports Requirements
PER	System Performance Requirements

General Technical Requirements

This section presents the overall technical requirements that apply to the software.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-1	The bidder must provide a description of their proposed technical architecture (Oracle, Java, .net, PowerBuilder, etc.). Indicate what components are loaded on the client, what components are loaded on the server, etc. Include hardware, software, networking, tools, etc. required.				
Response:					
TEC-2	The bidder must ensure that third party business partners are seamlessly integrated into the proposed solution. Describe any third party components that are proposed as part of the solution.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-3	Wherever practical and appropriate, the application must be designed so that business rule parameters and code lookup tables can be easily updated without changing the overall application program logic.				
Response:					
TEC-4	The bidder must describe their software licensing model. In all cases, DHHS prefers a concurrent licensing model or a site licensing model as opposed to "seat" or per user licensing.				
Response:					
TEC-5	The software must be designed such that routine upgrades and maintenance minimize downtime and impact to the users.				
Response:					
TEC-6	The system must have the ability to share data securely, including importing and exporting of data to/from other application software tools.				
Response:					
TEC-7	The system must have the ability to archive data per the department's required record retention schedules.				
Response:					
TEC-8	The system must have the ability to provide audit information on all data accessed or changed within the system.				
Response:					

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TEC-9	Describe how your system allows multiple users to use the software applications and database concurrently.				
Response:					
TEC-10	The solution shall be scalable and flexible enough to accommodate any changes required by the State and/or federal statute, mandate, decision or policy.				
Response:					
TEC-11	If an electronic document management system is needed, the bidder must provide a description of the proposed document system. The proposed solution must leverage an integrated system supported by DHHS to support the storage and retrieval of document images.				
Response:					
TEC-12	The system must have the ability to generate reports without performance impact to user access or system response time.				
Response:					
TEC-13	If used, describe how the system stores multiple objects such as pictures, documents, PDF files, etc.				
Response:					

Standards Requirements

DHHS currently operates its computer system in compliance with many technology and operational standards. These standards originate from internal development, industry best practices and governmental mandates. All applications provided by the bidder must operate in compliance with these standards and practices.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
STN-1	Web-based system applications must be accessible through industry standard browsers used by the Department. If the system requires additional components, technical details of those components must be provided.				
Response:					
STN-2	All DHHS data stored off-site (including data "in the cloud") must be stored in federally compliant data centers residing within the continental United States of America.				
Response:					
STN-3	The system must maintain that all data contained within the system is the property of DHHS, who shall retain the exclusive rights of use now and in perpetuity.				
Response:					
STN-4	The software must comply with accessibility requirements described in 45 CFR 85 and with State of Nebraska accessibility requirements located at http://nitc.nebraska.gov/standards/2-101.html				
Response:					

STN-5	The software must comply with digital signature requirements described in the Nebraska Digital Signatures Act. Refer to http://www.sos.ne.gov/rules-and-regs/regsearch/Rules/Secretary_of_State/Title-437.pdf for definition and standards in Nebraska.				
Response:					
STN-6	The solution shall conform to the sub-parts of Section 508 of the Americans with Disabilities Act (ADA), and any other appropriate State or federal disability legislation. Refer to http://www.ada.gov/508/.				
Response:					
STN-7	The system must be consistent with all HIPAA and other statutory, regulatory and policy requirements as defined and adopted by DHHS. Refer to http://dhhs.ne.gov/Pages/fin_ist_policies.aspx for policies and standards.				
Response:					
STN-8	The system should assure that all software used for the solution can be distributed, installed and configured in an unattended "silent" manner.				
Response:					
STN-9	The proposed solution must not require users to be granted administrative rights to their desktop PC's.				
Response:					
STN-10	The proposed solution must not store data on the desktop PC's local drive(s).				
Response:					

STN-11	The proposed solution must ensure that report design tools and output formats are compatible with DHHS desktop software standards at the time of system implementation.				
Response:					
STN-12	The proposed solution must maintain licensed software, including all third-party software, no more than two supported versions behind the latest release and is the version supported by DHHS.				
Response:					
STN-13	The proposed solution must ensure that vendor access to any State-hosted device must be provided using agency-provided methodology.				
Response:					
STN-14	The proposed solutions must have the capability to receive data files from the current Health Record and Pharmacy Systems and convert all current data to be stored in the proposed solution database and to become part of the proposed solution. Describe your process.				
Response:					

Error Handling Requirements

The management of the system requires that all occurrences of errors be logged for review and that critical errors be accompanied by appropriate alerts. Authorized users need to be able to query and review the error log and configure the alerts.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
ERR-1	The bidder must provide a description of their proposed Error Handling functionality.				
Response:					
ERR-2	The system must provide a comprehensive set of edits at the point of data entry to minimize data errors and provide immediate feedback in order for incorrect data to be corrected before further processing (e.g., spell check).				
Response:					
ERR-3	The system must ensure all errors are written and categorized to an error log.				
Response:					
ERR-4	The system must allow for a user to view, filter, sort, and search a comprehensive error log.				
Response:					
ERR-5	The system shall allow for user-defined alerts of errors, including those to external communication mechanisms (e.g., e-mail and text messaging).				
Response:					

ERR-6	The system must provide for the generation of standard and customizable error reports.				
Response:					
ERR-7	The system shall include a comprehensive list of error messages with unique message identifiers.				
Response:					
ERR-8	The system must display errors to the user/operator in real-time whenever an error is encountered.				
Response:					
ERR-9	The system must have the ability to suppress error messages based upon user-defined criteria.				
Response:					

Database/Data Management Requirements

DHHS requires the benefits inherent with a relational database management system (RDBMS). The accessibility, flexibility and maintainability achieved through normalized data structures are essential to achieving the business objectives outlined in this RFP. All components of the new software must be based on a relational database management system.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-1	Bidders must provide a description of their proposed Database architecture. Indicate what database software is supported by your application.				
Response:					
DBM-2	Bidders must provide a description of their proposed Database Warehouse solution, if applicable.				
Response:					
DBM-3	The system must be built upon an integrated data model, using a Relational Database Management System (RDBMS) with referential integrity enforced.				
Response:					
DBM-4	The RDBMS must have the capability to support triggers, stored procedures, alerts, user-defined functions and data types, and system-defined functions and data types.				
Response:					
DBM-5	The RDBMS must have native-DBMS support of XML.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DBM-6	The system must allow committed changes to be made available immediately on-line.				
Response:					
DBM-7	The system must facilitate data structure changes to accommodate expanding scope, new services, changing requirements and legislative mandates.				
Response:					
DBM-8	The system must provide the flexibility to extract and load data into standard non-proprietary software formats.				
Response:					
DBM-9	The system must maintain an automated history of all transactions, including, but not limited to: date and time of change, "before" and "after" data field contents, and operator identifier or source of the update.				
Response:					
DBM-10	The software database must conform to the Open Database Connectivity Standard (ODBC).				
Response:					
DBM-11	The software database must be compliant with the Structured Query Language.				
Response:					

DBM-12	The system must provide utilities or other tools for administrative Users to evaluate data relationships between tables.				
Response:					
DBM-13	The system must provide a diagnostic tool or utility to identify contaminated and corrupt files and locate the contamination within the file.				
Response:					

Backup and System Recovery Requirements

DHHS requires the ability to create backup copies of the software and to restore and use those backup copies for the basic protection against system problems and data loss. This requirement refers to all application system files, data files, and database data files. The contractor must provide a comprehensive and easily manageable backup and recovery process that is responsive to DHHS needs.

The bidder must identify and implement a system recovery plan that ensures component failures do not disrupt services. The plan must be completed, implemented, and tested prior to system implementation.

The successful bidder's solution must specify all needed hardware, software, and tools, and the plan must clearly define all roles, responsibilities, processes, and procedures. The solution must be sufficiently flexible to integrate with existing DHHS capabilities and accommodate future changes.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
BKP-1	Bidders must provide a description of their proposed Backup and System Recovery plan. Include all needed hardware, software, and tools, and clearly define all roles, responsibilities, processes and procedures. Bidders must include their backup retention schedules – daily, weekly, monthly, quarterly, etc.				
Response:					
BKP-2	Bidders must provide a description of their proposed Disaster Recovery Plan. Include all needed hardware, software, and tools, and clearly define all roles, responsibilities, processes and procedures.				
Response:					
BKP-3	All backups must be able to be scheduled outside of normal working hours and without user intervention.				
Response:					

BKP-4	Bidders must provide information on their test and validation process for all of the backup requirements listed previously (BKP-1, BKP-2, and BKP-3).				
Response:					

Security and Audit Requirements

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-1	Bidders must provide a description of security safeguards integrated into their application and how these safeguards address DHHS security. Refer to DHHS Information Technology (IT) Access Control Standard (DHHS-2013-001-b) for specific requirements: http://dhhs.ne.gov/IT%20Policies/Information%20Technology%20Access%20Control%20Standard.pdf				
Response:					
SEC-2	As required, the solution shall comply with Federal, State, and division-specific security requirements including but not limited to: • Health Insurance Portability and Accountability Act (HIPAA) of 1996 • Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 • Nebraska Electronic Signature Statute http://www.nebraskalegislature.gov/laws/statutes.php?statute=86-611 • Privacy Act of 1974 • 45 CFR 85 Security standards for PHI • Office of the National Coordinator's Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health information https://www.healthit.gov/policy-researchers-implementers/nationwide-privacy-and-security-framework-electronic-exchange Refer to the Nebraska DHHS Information Systems and Technology Security Policies and Standards for more information (http://dhhs.ne.gov/Pages/fin_ist_policies.aspx).				
Response:					
SEC-3	Describe how your system meets the DHHS requirements for unique user ID access. Include: • Specification on configuration of the unique user ID. • How the unique user ID is assigned and managed. • How the unique user ID is used to log system activity. • How the system handles the creation of duplicate user ID accounts.				
Response:					

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
SEC-4	Describe how the proposed system will meet the DHHS standard for administering passwords: • Initial Password assignment. • Strong Password Requirements. • Password reset process. • Password expiration policy. • Password controls for automatic lockout access to any user or user group after an administrator-defined number of unsuccessful log-on attempts.				
Response:					
SEC-5	Describe how your system meets the requirements for unique system administration access. Include: • Specification on configuration of the unique system administration ID. • How the unique system administration ID is assigned and managed. • How the unique system administration ID is used to log system activity.				
Response:					
SEC-6	Describe how your system meets the requirements for unique database administration access. Include: • Specification on configuration of the unique database administration ID. • How the unique database administration ID is assigned and managed. • How the unique database administration ID is used to log system activity.				
Response:					
SEC-7	Describe how the proposed system shall support the use of Multi-factor authentication.				
Response:					

SEC-8	Describe any security processes for managing security updates, and integrated components subject to vulnerability, including anti-virus.				
Response:					
SEC-9	The solution shall provide the ability to maintain a directory of all personnel who currently use or access the system.				
Response:					
SEC-10	State of Nebraska requires authentication and authorization of users through an enterprise directory known as the Nebraska Directory Services (NDS) to access web-based applications. Describe how your system will integrate NDS authentication. Refer to the Nebraska Information Technology Commission Security Architecture – Authentication and Authorization – Identity and Access Management Standard for State Government Agencies (8-302) for specific requirements: http://nitc.nebraska.gov/standards/8-302.html				
Response:					
SEC-11	The system must provide rule-based security and allow restricted access to system features, function, screens, fields, database, etc. Role authentication may occur at the directory level (NDS), application level, or database level (depending on database platform). Describe the security administration functions integrated into your system that manage role-based access to system functions, features, and data. Include a description of: • How and where your system stores security attributes or roles (e.g., LDAP attributes, database tables, a file). • The interface between the LDAP and the application, if roles are assigned in an LDAP directory. • How roles are created and security is applied to the role based on how and where security attributes are stored (if multiple options describe each). • How groups are defined and how roles and security are applied to each group. • How access limits are applied to screens and data on screens by role or group. • How users are created and assigned to one or more roles or groups. • How role and group creation and assignment activity is logged.				
Response:					

SEC-12	The system must be able to automatically lock a workstation after 15 minutes of inactivity, as required by DHHS Policies and Procedures. Describe this feature in the proposed system, including how the feature is administered and what effect automatic logoff has on any activity or transaction in process at the time of logoff. Refer to DHHS Securing Hardware and Software Standard (DHHS-2013-001-A) **3.4 Workstation Security Standards** for specific requirements. http://dhhs.ne.gov/IT%20Policies/Information%20Technology%20Securing%20Hardware%20and%20Software%20Standard.pdf				
Response:					
SEC-13	Confidential and Highly Restricted Data transmitted must be protected from unauthorized access during transmission. Describe transmission safeguards that are integrated into the proposed system to protect data during transmission, including any encryption technology. Refer to DHHS Information Technology (IT) Security Policy (DHHS-2013-001) **6.0 Information Classification** for specific requirements: http://dhhs.ne.gov/IT%20Policies/Information%20Technology%20Security%20Policy.pdf Refer to DHHS Information Technology (IT) Security Policy (DHHS-2013-001) **8.3 Encryption** for specific requirements: http://dhhs.ne.gov/IT%20Policies/Information%20Technology%20Security%20Policy.pdf				
Response:					
SEC-14	Bidders must provide a description of their proposed System Auditing functions. This must include but is not limited to: • The user ID of the person who made the change. • The date and time of the change. • The physical, software/hardware and/or network location of the person while making the change. • The information that was changed. • The outcome of the event. • The data before and after it was changed, and which screens were accessed and used. Refer to DHHS Information Technology (IT) Audit Standard (DHHS-2013-001-F) for specific audit requirements: http://dhhs.ne.gov/IT%20Policies/Information%20Technology%20Audit%20Standard.pdf				
Response:					

SEC-15	If the proposed system processes Confidential and Highly restricted Data, the bidder must provide auditing functions for all data that is accessed and viewed, regardless of whether the data was changed. This must include but is not limited to: • The user ID of the person who viewed the data. • The date and time of the viewed data. • The physical, software/hardware and/or network location of the person viewing the data. • The information that was viewed. Refer to DHHS Information Technology (IT) Audit Standard (DHHS-2013-001-F) for specific audit requirements: http://dhhs.ne.gov/IT%20Policies/Information%20Technology%20Audit%20Standard.pdf				
Response:					
SEC-16	If the system has the ability to override edits, the system must have the ability to audit all overridden edits and identify information including, but not limited to, the login ID, date, and time.				
Response:					
SEC-17	The system must produce daily audit trail reports and allow inquiries, showing updates applied to the data.				
Response:					
SEC-18	The solution should provide an auto archive/purge of the log files to prevent uncontrolled growth of the log and historical records storage using administrator-set parameters.				
Response:					
SEC-19	The solution should support encryption of data at rest for all stored Confidential or Highly Restricted Data or an equivalent alternative protection mechanism. Bidder must describe in detail compensating controls if data is not encrypted at rest.				
Response:					

SEC-20	Bidder should describe in detail any system or network infrastructure incorporated into the solution.				
Response:					
SEC-21	The solution shall adhere to the principle of “Fail Safe” to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.				
Response:					
SEC-22	The solution shall be configurable to prevent corruption or loss of data already entered into the solution in the event of failure.				
Response:					
SEC-23	Upon access, the system should display a message banner indicating that this application is only to be accessed by those individuals who are authorized to use the system.				
Response:					
SEC-24	The solution, prior to access of any Confidential or Highly Restricted Data, shall display a configurable warning or login banner (e.g. "The solution should only be accessed by authorized users"). In the event that a solution does not support pre-login capabilities, the solution shall display the banner immediately following authorization.				
Response:					

SEC-25	The solution should recognize Confidential and Highly Restricted information in screens, reports and views (i.e. PHI and SSN). Restrict distribution and access based upon system security settings and roles. Include warnings on printed and viewed reports.				
Response:					
SEC-26	The solution shall alert staff authorities identified by DHHS of potential violations of security and privacy safeguards.				
Response:					
SEC-27	The solution must provide the capability to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.				
Response:					
SEC-28	The solution should provide a process for archiving and/or destroying data and sanitizing storage media in conformance with DHHS and Division data governance policies and subject to applicable HIPAA, and federal (e.g., Federal Information Processing Standards (FIPS), National Institutes of Standards and Technology (NIST), and State laws.				
Response:					
SEC-29	The solution must provide the capability to identify and report on unauthorized attempts to information in the system, based on user-defined criteria.				
Response:					
SEC-30	Have defined and deployed strong controls (including access and query rights) to prevent any data misuse, such as fraud, marketing or other purposes.				
Response:					

SEC-31	The solution shall support logging to a common audit engine using the schema and transports specified by DHHS. The solution shall be able to export logs in such a manner as to allow correlation based on time (e.g. Coordinated Universal Time [UTC] synchronization).				
Response:					
SEC-32	The solution shall support removal of a user's privileges without deleting the user from the solution to ensure history of user's identity and actions.				
Response:					

System and User Documentation Requirements

DHHS requires the Contractor to develop, electronically store and distribute system documentation to include, at a minimum:

- User Manuals
- System Documentation
- A complete Data Dictionary

The contractor must provide a complete Data Dictionary. The Data Dictionary is to include definitions of all data elements and tables where they reside.

A sample copy of all user manuals in electronic format should be included in the bidder's response to the RFP.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
DOC-1	Bidders must provide a description of their system and user documentation approach and content.				
Response:					
DOC-2	The bidder shall provide an entity-relationship model, class diagram and a table of contents with data dictionary for report creation by the State that is regularly updated and includes table, field, and relationships.				
Response:					
DOC-3	The solution should provide on-line help for all features, functions, and data element fields, as well as descriptions and resolutions for error messages, using help features including indexing, searching, tool tips, and context-sensitive help topics. All selection criteria parameters and each report item/data element must be defined and all field calculations must be defined in detail.				
Response:					

DOC-4	The contractor should ensure that the User Manual remains accessible to users on-line, with a printable version available. The documentation will include full mock-ups of all screens/windows and provide narrative descriptions of the navigation features for each screen/window.				
Response:					
DOC-5	The system will have on-line documentation that includes descriptions, definitions, and layouts for each standard report. All selection criteria parameters and each report item/data element must be defined, all field calculations must be defined in detail, and field and report titles are mandatory.				
Response:					
DOC-6	The system must provide a data dictionary which includes user-defined fields and tables which can be viewed online and is kept updated for each modification.				
Response:					
DOC-7	The contractor shall provide DHHS a comprehensive system operation manual, at the time of installation.				
Response:					
DOC-8	The contractor shall develop, use and provide training material to DHHS for initial and ongoing training. The content of these materials will be consistent with the User Manual, any Operating Procedures and Help text.				
Response:					

Training Requirements

This section presents the overall training requirements that apply to the software. They are not specific to any technology or platform.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
TRN-1	The bidder must provide a description of their proposed training regimen to allow staff to sufficiently perform all functional requirements, test data conversion and reporting. The contractor is encouraged to use a combination of classroom and on-line learning techniques, as appropriate, to implement Training for DHHS staff.				
Response:					

Production, Test and Training Requirements

DHHS requires three separate environments (Production, Test, and Training) in order to operate and maintain the new software on an ongoing basis:

Test Environment – A test environment is required that mirrors the live production environment, including hardware and software. This test environment will be used to test application changes before they are deployed to production. This step is an important part of quality assurance, where all changes are tested to minimize the risk of adverse reactions in the production environment. While it is necessary to mirror all of the functions of the production environment, it is not necessary to maintain the same load capacity.

Training Environment – A Training environment is also required that allows DHHS to provide hands-on training to users. This environment would allow DHHS to maintain unique data for use in training and conduct training without interference with the test or production environments. This environment will have occasional use.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PTT-1	The system must support several environments, i.e., production environment, test environment, and training environment. Bidders must provide a description of their proposed production, test, and training environments.				
Response:					
PTT-2	Non-production environments such as testing and training environments should contain de-identified data and not include Confidential or Highly Restricted data.				
Response:					
PTT-3	The solution must provide the ability to refresh any testing or training environment at the request of DHHS. Describe your refresh process and whether the refresh process can be completed using DHHS resources, or whether the process requires professional services from the vendor.				
Response:					

Interfaces/Imports/Exports Requirements

The proposed software solution is expected to be able to interface with other computer systems as necessary.

Req #	**Requirement**	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
INT-1	The bidder must provide a description of their automated approach to managing interfaces.				
Response:					
INT-2	The solution's interfaces shall secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective.				
Response:					
INT-3	The solution shall have the capability to notify System Administrators/system support staff if an interface is not available for any reason.				
Response:					
INT-4	The bidder shall provide necessary APIs to allow DHHS to create interfaces to and from the DHHS solution.				
Response:					

INT-5	If needed, the solution must support data exchanges between components in real-time so that data is always synchronous across the entire solution, including any third-party components.				
Response:					
INT-6	The system must have the ability to expand data access to additional systems that are consistent with current data standards.				
Response:					

System Performance Requirements

This section describes requirements related to the proposed systems' on-line performance, response times, and sizing from a system architecture standpoint.

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-1	Bidders must provide a description of their proposed system performance functionality and monitoring tools.				
Response:					
PER-2	The solution should meet the following minimum response times even at peak load. Times will be measured for adherence to the requirements at the State's discretion. • Record Search Time – The response time must be within four (4) seconds 95% of the time and under ten (10) seconds for 100% of the time for record searches. • Record Retrieval Time – The response time must be within four (4) seconds 95% of the time and under ten (10) seconds 100% of the time for record retrievals. • Transaction Response Time – The response time must be within two (2) seconds 95% of the time and under ten (10) seconds for 100% of the time for screen response. • Print Initiation Time – The response time must be within two (2) seconds 95% of the time and under ten (10) seconds 100% of the time-for-print initiations. • Subsequent Page Display Response Time – The movement from viewing one page to viewing the next page within the same document shall not take more than one (1) second 95% of the time and under five (5) seconds for 100% of the time for screen response. • Document Availability – 99.5% of all documents must be available within on average five (5) seconds after imaged. Note: These response times do not include network latency, which will be measured and reported by DHHS.				
Response:					

Req #	Requirement	(1) Comply	(a) Core	(b) Custom	(c) 3rd Party
PER-3	The solution shall capture system down times along with the causes of the downtimes where applicable.				
Response:					
PER-4	Support concurrent users with minimal impact to response time, with the ability to increase the demand on the system by 50% without modification to the software or degradation in performance.				
Response:					
PER-5	The solution shall be available, online 24 hours a day and 7 days a week, 99.9% of the time each month. Planned, approved downtime for maintenance will be excluded from this requirement. Describe any expected timeframes where the system will be unavailable for use.				
Response:					
PER-6	Describe any key performance indicators (KPI) or other metrics to measure and report system performance for the proposed system.				
Response:					
PER-7	The solution shall provide application performance monitoring and management capabilities.				
Response:					