Attachment A – Revision One
QIDS Technical Requirements Traceability Matrix

Request for Proposal Number 6317 Z1

Bidders are instructed to complete a Technical Requirements Traceability Matrix for QIDS. Bidders are required to describe in detail how the 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 awarded bidder 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 should 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.

 Bidder must include in the response whether the requirement is met as a core component (The requirement is met by existing capabilities of the core system or with minor modifications or configuration to existing functionality), custom, (The bidder proposes to custom develop the capability to meet this requirement for those features that require substantial or "from the ground up" development effort.) or with a 3rd party provider (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 should describe the product, including product name, its functionality and benefits in their response.)

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
DAC	Data Conversion

General Technical Requirements

This section presents the overall technical requirements that apply to the software. Describe in the response how the proposed solution meets the requirement.

Req #	Requirement
TEC-1	Provide a description and diagram of the proposed technical architecture. Include all database/web/networking hardware, software, tools, etc. Indicate where the solution is hosted. Indicate if any components are needed on the client and/or loaded on servers, etc.
Response:	
TEC-2	Describe how the proposed solution is responsive to mobile technology and works with mobile devices such as smart phones or tablets.
Response:	
TEC-3	Describe any third party components that are proposed as part of the solution, i.e. using Crystal Reports as a reporting tool. Please ensure any costs for these required tools are included.

Req #	Requirement
	Response:
TEC-4	Describe how the solution is designed so that business rule parameters and code lookup tables can be easily updated without changing the overall application program logic.
	Response:
TEC-5	Describe the software licensing model of the solution, including any required third party licensing. In all cases, DHHS prefers a concurrent licensing model or a site licensing model as opposed to "seat" or per user licensing.
	Response:
TEC-6	Describe the upgrade and maintenance process for the proposed solution. DHHS requires minimum downtime and impact to the users.
	Response:
TEC-7	Describe any impact on customizations made to the solution for upgrades and maintenance processes. DHHS requires minimum downtime and impact to the users.
	Response:
TEC-8	Describe any redundancy built into the proposed solution to limit any downtime in the proposed solution.
	Response:
TEC-9	Describe how the proposed solution has the ability to share data securely, including importing and exporting of data to/from other application software tools, such as a Microsoft Excel file, XML, comma separated value (csv) file, etc.
	Response:
TEC-10	Describe how the proposed solution has the ability to archive data per the department's required record retention schedules. Describe the method and ability to adjust to changes.
	Response:

Req #	Requirement
TEC-11	Describe how the proposed solution has the ability to provide audit information on all data accessed or changed within the system.
Response:	
TEC-12	Describe how the proposed solution allows multiple users to use the software applications and database concurrently. An initial minimum of 2000 users are estimated.
Response:	
TEC-13	Describe how the proposed solution is scalable and flexible enough to accommodate any changes required by the State and/or federal statute, mandate, decision or policy. Describe any capabilities that allow the DHHS staff the ability to modify data fields.
Response:	
TEC-14	If an electronic document management system is needed, provide a description of the proposed document system and how it is able to support multiple objects such as pictures, documents, PDF file, etc.
Response:	
TEC-15	Describe how the proposed solution has the ability to generate reports and ad hoc queries without performance impact to user access or system response time.
Response:	
TEC-16	Describe how the system stores multiple objects such as pictures, documents, PDF files, etc.
Response:	

Standards Requirements

DHHS currently operates the agency's computer system in compliance with many technology and operational standards. These standards originate from internal development, industry best practices and governmental mandates. Describe how all applications provided by the bidder operate in compliance with these standards and practices.

Req #	Requirement
STN-1	Describe what industry standard browsers are supported by the solution. If the system requires additional components, describe the technical details of those components. Please describe how solution may be accessed across the state via web-based portal.
Response:	
STN-2	If the proposed solution requires any DHHS data to be stored off-site (including data "in the cloud") describe how the data is stored in federally compliant data centers residing within the continental United States of America, and if needed, follows HIPAA standards.
Response:	
STN-3	Describe how the proposed solution maintains that all data contained within the system is the property of DHHS, and that DHHS will retain the exclusive rights of use now and in perpetuity.
Response:	
STN-4	Describe how the proposed solution complies with accessibility requirements described in 45 CFR 85 and with State of Nebraska accessibility requirements located at https://nitc.nebraska.gov/standards/2-101.pdf
Response:	
STN-5	Describe how the proposed solution complies 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	Describe how the proposed solution conforms 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/.

Req #	Requirement
Response:	
STN-7	Describe how the proposed solution is consistent with all HIPAA and other statutory, regulatory and policy requirements as defined and adopted by DHHS. Refer to http://dhhsemployees/sites/ls/HIPAA/Policies/Forms/AllItems.aspx for policies and standards.
Response:	
STN-8	If the solution requires client software to be installed, describe how the proposed solution assures that all software used for the solution can be distributed, installed and configured in an unattended "silent" manner.
Response:	
STN-9	Current DHHS policies prevent users from making administrative changes and downloading software locally to a State-owned PC. Describe how the proposed solution supports this policy.
Response:	
STN-10	Current DHHS policies recommend not storing any data locally in the event that a user's desktop PC needs to be reimaged (which deletes locally stored data). Describe how the proposed solution supports this policy.
Response:	
STN-11	Describe the solution's report design tools and output formats.
Response:	
STN-12	Describe how the proposed solution maintains licensed software, including all third-party software, no more than two supported versions behind the latest release, and updated with latest security patches.
Response:	
STN-13	Describe how the proposed solution ensures that all access to any State-hosted device is provided using agency-provided methodology.
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
ERR-1	Describe the proposed Error Handling functionality.
Response:	
ERR-2	Describe how the proposed solution provides 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	Describe how the proposed solution ensures all errors are written and categorized to an error log. Describe how the bidder's proposed solution allows for a user to view, filter, sort, and search the error log.
Response:	
ERR-4	Describe how the proposed solution allows for user-defined alerts of errors, including those to external communication mechanisms (e.g., e-mail and text messaging).
Response:	
ERR-5	Describe how the proposed solution provides for the generation of standard and customizable error reports.
Response:	
ERR-6	Describe how the proposed solution includes a comprehensive list of error messages with unique message identifiers.
Response:	
ERR-7	Describe how the proposed solution displays errors to the user/operator in real-time whenever an error is encountered.

Req #	Requirement
	Response:
ERR-8	Describe how the proposed solution has 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.

Req #	Requirement
DBM-1	Describe the proposed Database architecture. Indicate what database software (DBMS) is used by the proposed application.
	Response:
DBM-2	Describe the proposed Database Warehouse solution, if applicable.
	Response:
DBM-3	Describe how the proposed solution is built upon an integrated data model, such as a RDBMS, with referential integrity enforced. Describe the integrated data model.
	Response:
DBM-4	Describe how the proposed integrated data model has the capability to support triggers, stored procedures, alerts, user-defined functions and data types, and system-defined functions and data types.
	Response:

Req #	Requirement
DBM-5	Describe how the b proposed RDBMS has native-DBMS support of XML.
Response:	
DBM-6	Describe how the b proposed solution allows changes to be made available immediately on-line.
Response:	
DBM-7	Describe how the proposed solution facilitates data structure changes to accommodate expanding scope, new services, changing requirements and legislative mandates.
Response:	
DBM-8	Describe the proposed standard Software Development Life Cycle (SDLC) for deploying software. Describe bidder's process for planning, creating, testing and deploying bidder's solution.
Response:	
DBM-9	Describe how the proposed solution provides the flexibility to extract and load data into standard non-proprietary software formats.
Response:	
DBM-10	Describe how the proposed solution maintains 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-11	Describe how the proposed software database conforms to the Open Database Connectivity Standard (ODBC).
Response:	

Req #	Requirement
DBM-12	Describe how the proposed solution is compliant with the Structured Query Language.
Response:	
DBM-13	Describe how the proposed solution provides utilities or other tools for administrative Users to evaluate data relationships between tables.
Response:	
DBM-14	Describe how the proposed solution provides 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 proposed solution should provide a comprehensive and easily manageable backup and recovery process that is responsive to DHHS needs.

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

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

Req #	Requirement
BKP-1	Describe the proposed Backup and System Recovery plan and readiness. Describe the service level agreement on returning the solution to service from a backup. Describe the proposed backup retention schedules – daily, weekly, monthly, quarterly, etc.
Response:	
BKP-2	Describe the proposed Disaster Recovery Plan. Describe the service level agreement on returning the solution back to operational service.
Response:	
BKP-3	Describe how backups of the proposed solution are able to be scheduled without user intervention and without interruption to the system.
Response:	
BKP-4	Describe how the proposed solution provides testing and validation processes for all of the backup requirements listed previously (BKP-1, BKP-2, and BKP-3).
Response:	

Req #	Requirement
BKP-5	If there is a backup failure or downtime, describe the b proposed method and timing of communication to DHHS.
Response:	

Security and Audit Requirements

Req #	Requirement
SEC-1	Describe the proposed security safeguards integrated into bidder's 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://dhhsemployees/Policy%20Documents/DHHS-IT-2018-001B%20Access%20Control.pdf
Response:	

SEC-2	Describe how the proposed solution complies 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/sites/default/files/nationwide-ps-framework-5.pdf
	    •
	
	Refer to the Nebraska DHHS Information Systems and Technology Security Policies and Standards for more information (http://dhhsemployees/Policy%20Documents/DHHS%20-%20HR%20-%20Information%20Technology%20(IT)%20Security%20Policies%20and%20Standards.pdf).

Response:	
SEC-3	Describe how the proposed solution meets the DHHS requirements for unique user ID access. Including but not limited to: • 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.

Req #	Requirement
	Requirement
Response:	
SEC-4	Describe how the proposed solution meets 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 the proposed solution 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 the proposed solution 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 solution supports the use of multi-factor authentication.

Req #	Requirement
	Requirement
Response:	
SEC-8	Describe any security processes for managing security updates, and integrated components subject to vulnerability, including anti-virus.
Response:	
SEC-9	Describe how the proposed solution provides the ability to maintain a directory of all personnel who currently use or access the system.
Response:	
SEC-10	The 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 the proposed solution will integrate NDS authentication. Refer to the Nebraska Information Technology Commission Security Architecture – Passwords (8-302) for specific requirements: https://nitc.nebraska.gov/standards/8-302.pdf
Response:	

Req #	Requirement
SEC-11	Describe how the proposed solution provides rule-based security and allows restricted access to system features, function, screens, fields, database, etc. Role authentication may occur at the directory level, application level, or database level (depending on database solution). Describe the security administration functions integrated into the proposed system that manage role-based access to system functions, features, and data. Include a description of: • How and where the proposed 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	Describe how the = proposed solution automatically disconnects based upon inactivity, as required by DHHS Policies and Procedures. Describe how the feature is administered and what effect disconnect has on any activity or transaction in process at the time of disconnection. Refer to DHHS Securing Hardware and Software Standard (DHHS-2018-001-A) for specific requirements. http://dhhsemployees/Policy%20Documents/DHHS-IT-2018-001A%20Securing%20Hardware%20and%20Software%20Standard.pdf
Response:	
SEC-13	Describe how the = proposed solution protects Confidential and Highly Restricted Data 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) for specific requirements: http://dhhsemployees/Policy%20Documents/DHHS-IT-2018-001%20Security%20Policy.pdf
Response:	

Req #	Requirement
SEC-14	Describe how the = proposed solution provides System Auditing functions, including but 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-2018-001-F) for specific audit requirements: http://dhhsemployees/Policy%20Documents/DHHS-IT-2018-001F%20IT%20Auditing%20Standard.pdf
Response:	
SEC-15	If the proposed system processes Confidential and Highly restricted Data, describe the auditing functions for all data that is accessed and viewed, regardless of whether the data was changed. Describe the auditing functions which should 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-2018-001-F) for specific audit requirements: http://dhhsemployees/Policy%20Documents/DHHS-IT-2018-001F%20IT%20Auditing%20Standard.pdf
Response:	
SEC-16	If the proposed solution has the ability to override edits, describe how the solution audits all overridden edits and identifies information including, but not limited to, the login ID, date, and time.
Response:	

Req #	Requirement
SEC-17	Describe how the proposed solution produces daily audit trail reports and allows inquiries, showing updates applied to the data.
Response:	
SEC-18	Describe how the proposed solution provides 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	Describe how the proposed solution supports encryption of data at rest or an equivalent alternative protection mechanism. Describe the proposed encryption of data. If data is not encrypted, describe in detail compensating controls.
Response:	
SEC-20	Describe how the proposed solution incorporates any system or network infrastructure into the solution.
Response:	
SEC-21	Describe how the proposed solution adheres 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	Describe how the proposed solution is configurable to prevent corruption or loss of data already entered into the solution in the event of failure.
Response:	
SEC-23	Describe how the proposed solution, upon access, displays a message banner indicating that this application is only to be accessed by those individuals who are authorized to use the system.
Response:	

Req #	Requirement
SEC-24	Describe how the proposed solution, prior to access of any Confidential or Highly Restricted Data, displays 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, describe how the solution displays the banner immediately following authorization.
Response:	
SEC-25	Describe how the proposed solution recognizes 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	Describe how the proposed solution alerts staff authorities identified by DHHS of potential violations of security and privacy safeguards. Incidents that involve or could potentially involve Confidential or Highly Restricted data must be reported immediately as defined in DHHS Policy DHHS-2013-001-E DHHS IT Incident Management Standard.
Response:	
SEC-27	Describe how the proposed solution provides the capability to monitor events on the information system, detects attacks, and provides identification of unauthorized use of the system.
Response:	
SEC-28	Describe how the proposed solution provides 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:	

Req #	Requirement
SEC-29	Describe how the proposed solution provides the capability to identify and report on unauthorized attempts to access information in the system, based on user-defined criteria.
Response:	
SEC-30	Describe how the proposed solution has 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	Describe how the proposed solution supports logging to a common audit engine using the schema and transports specified by DHHS. Describe how the solution exports logs in such a manner as to allow correlation based on time (e.g. Coordinated Universal Time [UTC] synchronization).
Response:	
SEC-32	Describe how the proposed solution supports removal of a user's privileges without deleting the user from the solution to ensure a history of user's identity and actions.
Response:	

System and User Documentation Requirements

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

- User Manuals
- System Documentation
- A complete Data Dictionary

The awarded bidder should 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 should be included in the bidder's response to the RFP. Electronic format is preferred.

Req #	Requirement
DOC-1	Describe how the proposed solution provides 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. Describe how the solution provides context-sensitive on-line help features/functionality.
Response:	
DOC-2	Describe how the proposed solution provides an on-line User Manual with a printable version available. The documentation should include full mock-ups of all screens/windows and provide narratives of the navigation features for each window/screen.
Response:	
DOC-3	Describe how the proposed solution will have on-line Reporting Manual with a printable version available that includes descriptions, definitions, and layouts for each standard report. Include definitions of all selection criteria parameters and each report item/data element, all field calculations defined in detail, and field and report titles.
Response:	
DOC-4	Describe how the proposed solution provides DHHS a comprehensive on-line Installation and Technical System Operation manual with a printable version available.
Response:	

Req #	Requirement
DOC-5	Describe how the proposed solution provides 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-6	Describe how the proposed solution provides a data dictionary which includes user-defined fields and tables which can be viewed online and kept updated for each modification.
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
TRN-1	Describe how the proposed solution develops and provides training material to DHHS for initial training and updates to training material for ongoing training on enhancements and changes made to the system. The content of these materials should be consistent with the on-line Help, User Manual, Reporting Manual and Operating Procedures.
Response:	
TRN-2	Describe the proposed solution training plan. This plan should provide both initial and ongoing training. The awarded bidder is encouraged to use a combination of classroom and on-line learning techniques, as appropriate.
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
PTT-1	Describe how the proposed solution supports several environments, i.e., production environment, test environment, and training environment.
Response:	
PTT-2	Describe how the proposed solution supports non-production environments such as testing and training environments. Non-production environments should contain de-identified data and not include Confidential or Highly Restricted data.
Response:	
PTT-3	Describe how the proposed solution provides the ability to refresh any testing or training environment at the request of DHHS. Describe the refresh process and whether the refresh process can be completed using DHHS resources, or whether the process requires professional services from the bidder.
Response:	
PTT-4	Describe the proposed test plan practices for any changes to the solution. Describe user test planning including unit testing, end-to-end testing, stress testing, and readiness testing prior to "go live" date.
Response:	

Interfaces/Imports/Exports Requirements

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

Req #	Requirement
INT-1	Describe the proposed automated approach to managing interfaces.
Response:	
INT-2	Describe how the proposed solution's interfaces secure and protect the data and the associated infrastructure from a confidentiality, integrity and availability perspective.
Response:	
INT-3	Describe how the proposed solution has the capability to notify System Administrators/ system support staff if an interface is not available for any reason.
Response:	
INT-4	Describe how the proposed solution provides necessary APIs and/or Web services to allow DHHS to create interfaces to and from the proposed solution.
Response:	
INT-5	If needed, describe how the proposed solution supports 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	Describe how the proposed solution has the ability to expand data access to additional systems that are consistent with current data standards.
Response:	
INT-7	Describe how the proposed solution conducts end-to-end testing with interface partners both external and internal to ensure requirements are met.

Req #	Requirement
Response:	

System Performance Requirements

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

Req #	Requirement
PER-1	Describe the proposed system performance functionality and monitoring tools.
Response:	
PER-2	Describe the minimum response times for the following functions, even at peak load. For example, expected response time will be within two (2) seconds 95% of the time, and under 10 seconds for 100% of the time. • Record Search Time • Record Retrieval Time • Transaction Response Time • Print Initiation Time • Subsequent Page Display Response Time • Document Availability Note: These response times do not include network latency, which will be measured and reported by DHHS.
Response:	
PER-3	Describe how the proposed solution captures system downtimes, along with the causes of the downtimes where applicable. Describe the bidder's proposed method and timing of communication to DHHS on downtimes.
Response:	
PER-4	Describe how the proposed solution supports 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.

Req #	Requirement
Response:	
PER-5	Describe how the proposed solution is available online 24 hours a day and 7 days a week, 99.9% of the time each month. Describe any known timeframes where the system will be unavailable for use.
Response:	
PER-6	Describe how the proposed solution provides application performance monitoring and management capabilities, including any key performance indicators (KPI) or other metrics to measure and report system performance for the proposed system.
Response:	

Data Conversion Requirements

This section describes requirements related to the proposed system's conversion of historical data.

Req #	Requirement
DAC-1	Describe the process for converting all historical data from the Department's existing systems, spreadsheets, and other supporting applications that are required for ongoing operations of the system and the historical reporting needs of the department.
Response:	
DAC-2	Describe the data conversion plan which includes data element mapping crosswalks, data cleansing, data synchronization for initial and interim conversion activities leading up to the final data conversion, and frequency of interim conversion events and final conversion execution.
Response:	