# Technical Requirements

Using the Vendor Response in the right column, please provide a detailed response describing Offeror’s solution to the technical requirement. A Word version of the document is provided for the Offeror’s convenience.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **ID** | **Requirement Description** | **Vendor Response** |
|  |  | **General Technical** |  |
| GT | **1** | ***Solution architecture*** |  |
| GT | 1.01 | The system shall use a modular architecture, adhering to Service Oriented Architecture (SOA) principles, and be comprised of distinct functionality components that can be added on or removed through installation addition or license expansion without requiring significant effort to add, remove or test. These functionality components should be designed to interoperate with other components, including components developed by other companies. |  |
| GT | 1.02 | Modular additions shall not require custom programming effort. Custom programming: software-based functionality developed specifically for Community Healthcore to meet a business or technical requirement where said functionality is not native to an acquired solution's module(s) or component(s). |  |
| GT | 1.03 | The system shall provide the ability for concurrent users to simultaneously view the same record, documentation and/or template and, where applicable, work on the same record including create, read, update and delete transactions recording said transactions yet applying the appropriate hierarchy and rules for effecting these transactions based on user group/class/rights. In the event of an update failure, the system shall notify the staff that their update was not made. |  |
| GT | 1.04 | The system shall be highly re-configurable, providing ability to reposition and rename field labels / data fields, remove or “turn-off” unused fields, maintain data, modify the layout of the user interface, and allow addition of custom-defined fields with minimal or no customization. |  |
| GT | **2** | ***Interface and interoperability*** |  |
| GT | 2.01 | The system shall be built to support data integration with other systems using web services. |  |
| GT | 2.02 | The system shall support the dynamic exchange of data from multiple solutions in real time and batch. |  |
| GT | 2.03 | The system shall support linkage to an external document management solution, unless a complete document management solution is provided by the vendor that can be leveraged for other purposes. |  |
| GT | 2.04 | The Offeror shall work with Community Healthcore to develop optimized interfaces - i.e. interfaces that accomplish the objective of exchanging the requisite data and simultaneously require the least amount of custom programming and maintenance - between the solution and Community Healthcore systems with pertinent source data and/or requiring data from the solution for downstream functions. The complete list of relevant systems will be finalized during the requirements elicitation phase. |  |
| GT | 2.05 | The Offeror shall partner with Community Healthcore in the development of transaction/event code sets, data exchange and reporting standards not specific to HIPAA or other federal efforts and will conform to such standards as stipulated in the plan to implement the standards. |  |
| GT | 2.06 | Where web services are used in the engineering of applications, the Offeror’s systems shall conform to World Wide Web Consortium (W3C) standards such as XML, UDDI, WSDL and SOAP so as to facilitate integration of Offeror systems with Community Healthcore systems. |  |
| GT | 2.07 | Point-to-point integrations shall be avoided to the extent possible. Application integration shall be achieved to the extent possible via a central service model. |  |
| GT | 2.08 | The Offeror shall work with Community Healthcore to develop and implement an Interface transition strategy consistent with any agreed-to phase-in of solution functionality (whether phase-in is based on programs or regions/geography) such that the solution and legacy systems are both properly populated, and the associated programs operating appropriately, during the implementation phase-in. This may involve some interface redundancy in the short term. |  |
| GT | **3** | ***User access modalities including mobility enablement*** |  |
| GT | 3.01 | The system shall allow for access to executive level dashboard reports via mobile/tablet device. |  |
| GT | 3.02 | The system shall allow for secure access to select client and end user functionality via mobile/tablet device without loss/degradation of functionality and also be available in offline mode. |  |
| GT | 3.03 | The system shall support multiple user access modalities including remote access connection (Windows) and web browser |  |
|  |  | **Please list all mobile device platforms and operating systems compatible with your solution and describe any non-standard or additional hardware and/or software required to support mobile devices.** |  |
| GT | **4** | ***Security including identity management and verification and access management*** |  |
| GT | 4.01 | The system shall enable role-based security to allow designated security staff to assign and repeal roles from authorized user accounts as needed. |  |
| GT | 4.02 | The system shall have the functionality to support biometric identification. |  |
| GT | 4.03 | **Please describe your authentication functions including password reset and multifactor authentication support.** |  |
|  |  |  |  |
| GT | 4.04 | The system shall support user single sign on (SSO) with local network and/or SSO with other primary system and inherit system user id and password. Community Healthcore requires multifactor authentication (MFA). |  |
| GT | 4.05 | The system shall support field and data level security. |  |
| GT | 4.06 | The Offeror shall ensure all electronic data transfers and access comply with all applicable state, federal and HIPAA Privacy and Security requirements. |  |
| GT | 4.07 | The system shall allow users to reset passwords if not SSOed with another system. |  |
| GT | 4.08 | The system shall allow the deletion or deactivation and the reactivation of user accounts. |  |
| GT | 4.09 | The system shall encrypt all stored passwords. |  |
| GT | 4.10 | The online user interface for system shall function in a secure, encrypted session. |  |
| GT | 4.11 | The system shall support encryption of data in motion or transit. |  |
| GT | 4.12 | The Offeror’s system shall employ an access management function that restricts access to varying hierarchical levels of system functionality and Information. The access management function shall: • Restrict access to information on a "need-to-know" basis, e.g. users permitted inquiry privileges only will not be permitted to modify information; • Restrict access to specific system functions and Information based on an individual user profile, including inquiry only capabilities; global access to all functions will be restricted to specified staff jointly agreed to by Community Healthcore and the Offeror; and • Restrict attempts to access system functions to a number specified in policy, with a system function that automatically prevents further access attempts and records these occurrences. |  |
| GT | 4.13 | The Offeror shall provide for the physical safeguarding of its data processing facilities and the systems and information housed therein. The Offeror shall enable designated entities to have access to data facilities as required. The physical security provisions shall be in effect for the life of this Contract. |  |
| GT | 4.14 | The Offeror shall restrict perimeter access to equipment sites, processing areas, and storage areas through a card key or other comparable system, as well as provide accountability control to record access attempts, including attempts of unauthorized access. |  |
| GT | 4.15 | The Offeror shall include physical security features designed to safeguard processor site(s) through required provision of fire-retardant capabilities, as well as smoke and electrical alarms, monitored by security personnel. |  |
| GT | 4.16 | The Offeror shall ensure that the operation of all of its systems is performed in accordance with Texas and federal regulations and guidelines related to security and confidentiality of the protected information managed by the Offeror, including but not limited to HIPAA Privacy and Security Rules, the Breach Notification Rules under the HITECH Act, and security incident reporting as required by the SSA, IRS and CMS. |  |
| GT | 4.17 | The Offeror shall ensure compliance with: • 42 CFR Part 431 Subpart F (confidentiality of information concerning applicants and Enrollees of public medical assistance programs); • 42 CFR Part 2 (confidentiality of alcohol and drug abuse records); and • Special confidentiality provisions in state or federal law related to people with HIV/AIDS and mental illness. |  |
| GT | 4.18 | The system shall, at a minimum, provide a mechanism to comply with the most current security requirements and safeguard requirements of the following agencies/entities:  • Health & Human Services (HHS) Center for Medicare & Medicaid Services (CMS) • Administration for Children & Families (ACF)   * Substance Abuse and Mental Health Services Administration (SAMHSA) * Joint Commission * NIST 800-53r4, MARS-E and DOD 8500.2 * Federal Information Security Management Act (FISMA) of 2002 * Health Insurance Portability and Accountability Act (HIPAA) of 1996 * Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 * Privacy Act of 1974 * e-Government Act of 2002 * Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations |  |
| GT | 4.19 | How do you provide proof of security certification(s) compliant with NIST 800-53 R4 and SOC II security standards? Please describe how you comply and the proof of compliance you are willing to provide upon request. |  |
| GT | 4.20 | The system shall adhere to the principle of “Fail Safe” to ensure that the solution does not reveal any sensitive information or leave any access controls open for attacks |  |
| GT | 4.21 | The software used to install and update the system, independent of the mode or method of conveyance, shall be certified free of malevolent software (“malware”). Vendor may self-certify compliance with this standard through procedures that make use of commercial malware scanning software. |  |
| GT | 4.22 | The system, when storing PHI on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), shall support use of a standards based encrypted format using Advanced Encryption Standard (AES) or its successor |  |
| GT | 4.23 | The Offeror shall review and analyze the key risks to the important assets and functions provided by the System to certify that the Common Weakness Enumeration (CWE)/SANS Institute Top 25 Most Dangerous Software Errors (http://cwe.mitre.org/top25) have been mitigated and document the mitigation. |  |
| GT | 4.24 | The Offeror shall review the System and certify that the code and any new development meets or exceeds the Open Web Application Security Project (OWASP) Application Development Security Standards outlined on the www.OWASP.org site and document in writing that they have been met. |  |
| GT | 4.25 | The system shall be subject to a Security Impact/Risk Assessment prior to updates being released into production |  |
| GT | 4.26 | All system servers shall have hardened operating systems by eliminating any unnecessary system services, accounts, network services, and limited user access rights throughout all of the environments. |  |
| GT | **5** | ***Performance*** |  |
| GT | 5.01 | The system response time during operations shall be 5 seconds or less for 95 percent of the **search and lookup queries** (does not include ad hoc queries and analytics) as tested in a sufficient number of Community Healthcore sites. Maximum response time will not exceed 15 seconds except for agreed to exclusions. Response time is defined as the time elapsed after depressing an ENTER key (or clicking on a button that triggers the transaction) until the system displays the response back to the user. |  |
| GT | 5.02 | The system shall return a **Dashboard report** within 5 seconds or less, 95% of the time. Dashboard report: online or printed report that provides either a graphical or tabular presentation of the current status and historical trends of the performance of select functions/services based on prescribed metrics. |  |
| GT | 5.03 | The system shall return a **Static Standard** report within 5 seconds or less, 95% of the time. Standard static report: online or printed report that is generated in accordance with a prescribed format and information specifications and requires no user input regarding a data source or query. |  |
| GT | 5.04 | The system shall return a **parameter-based report** within 20 seconds or less. Parameter based report: online or printed report that is generated in accordance with a prescribed format and information specifications that requires no user input regarding a data source or query but does require user input requiring constraints on the information being sought, e.g. specific date and time range(s), population(s) served, program(s)/service(s), office(s)/service center(s). |  |
|  |  | **Please describe your standard Service Level Agreement (SLA) related to system performance (speed, no application latency), system uptime/unplanned downtime, and planned downtime.** |  |
| GT | **6** | ***Capacity, scalability and extensibility*** |  |
| GT | 6.01 | The system shall be scalable and adaptable to meet future growth and expansion/contraction needs such that the system can be expanded on demand and be able to retain its performance levels when adding additional users, functions, and data. |  |
| GT | 6.02 | The system shall possess capacity sufficient to handle the workload projected for the start of the program and will be scalable and flexible, so they can be adapted as needed, within negotiated timeframes, in response to program or enrollment changes. This will be determined as part of solution and operational readiness activities that shall be conducted by Community Healthcore in accordance with a mutually agreed upon protocol. |  |
| GT | 6.03 | The system's interfaces shall be scalable to accommodate changes in scale including changes in user population, transaction volume, throughput and geographical distribution. The System will be capable of making any changes to the interface data elements/layouts easily, and to test those changes. |  |
|  |  |  |  |
| GT | **7** | ***Usability*** |  |
| GT | 7.01 | The Offeror shall be able to demonstrate that its client and end user portals have undergone extensive usability testing with at least three independent groups and that the results of said testing have been incorporated into the design of the client and user portal - navigation, user interface/screen design, menu design, user prompts, ease to populate fields/provide information. |  |
| GT | 7.02 | The system shall allow users to complete all functions and navigate all fields by both keyboard and mouse. |  |
| GT | 7.03 | The system shall allow users to adjust screen and printed fonts both in size and color and adjust background colors and screen contrast (functionality should be similar to Microsoft Office applications). |  |
| GT | 7.04 | The system shall support undo and redo or provide onscreen confirmation/acceptance to the user to confirm a change that is permanent and cannot be "undone". |  |
| GT | 7.05 | The system shall allow users to create shortcuts (e.g. onscreen short cuts, hot-keys, etc.) for frequent actions. |  |
| GT | 7.06 | The system shall provide users with clearly marked "backouts/exits" for instances when a user mistakenly chooses a system function; such "exits" shall be simple and require minimal steps. |  |
| GT | 7.07 | The system shall provide drop down and list boxes for all key entry, and text entry will display existing values for selection (system based auto fill) but specifically disallow client browser based autofill. Include how the drop down list is populated and if it can be customized or searchable (ex: type first three letters and goes to that selection) |  |
| GT | 7.08 | Wherever applicable, the system shall accommodate point and click selection and check box entry for all relevant data entries. Once data field entered, the information is populated to same data field in other forms so the user does not have to enter textual data that may already be available to the system. |  |
| GT | 7.09 | The system shall provide field level on-screen edits with limited user override capabilities. Describe the functionality for the drop down list as supporting the organizational and reporting structure of the agency such as programs (location/cost center, unit/subunit), service code, payers/covered services/billing rules, etc. |  |
| GT | 7.10 | The system shall provide the ability to make fields visible/invisible depending on parameters, user rights, consent, and access controls. |  |
| GT | 7.11 | The system shall not show fields not accessible to a given user based on access rights, client consent, nor will the System show fields not in use. |  |
| GT | 7.12 | The system cursor shall ~~automatically~~ advance to the next logical input field when the user presses the “Tab” key. What does your system do when it reaches the maximum allowed number of characters is reached for a given field? |  |
| GT | **8** | ***Data and document management including storage and retention*** |  |
| GT | 8.01 | The Offeror shall ensure that incremental backups of the entire system's database(s) are completed at least daily, and full backups are completed at least weekly. |  |
| GT | 8.02 | The system shall be built on a relational database (SQL2012 or higher). |  |
| GT | 8.03 | The system shall have a data dictionary that shall be kept regularly up-to-date. All changes shall be updated in the dictionary within 30 days of modification or addition of fields in production (Update requirements may change based on SLAs). |  |
| GT | 8.04 | The system shall maintain the integrity of data element sources used by reporting functions (the data warehouse) and integrate necessary data elements. |  |
| GT | 8.05 | The information required for on line help functions shall be maintained in the data dictionary. |  |
| GT | 8.06 | The system shall include the ability to add new data sets and data sources as directed by Community Healthcore and per state and federal guidelines. |  |
| GT | 8.07 | The system shall retain reports for time frame specified by Community Healthcore. |  |
| GT | 8.08 | The system shall maintain a data dictionary and relationships of database fields/elements, defined so that they are understandable to end users |  |
| GT | 8.09 | The system shall include the ability to support the deletion of data when necessary. |  |
| GT | 8.10 | The system shall include the ability to append and update information into the solution database in accordance with Community Healthcore SLA time requirements. |  |
| GT | 8.11 | The system shall send out alerts when the reporting and business intelligence module/component load is complete. |  |
| GT | 8.12 | The system shall provide the ability to identify if an error occurred during a load process and automatically notify a list of contacts by email and direct contact (text, page, or phone), and produce an error report. The error report would specify the type of error (i.e. data error, processing error, system error, etc.). Community Healthcore specific error types or codes can be added to a specific implementation with additional cost. |  |
| GT | 8.13 | The system shall provide the ability to roll back the most recent data load. |  |
| GT | 8.14 | The system shall conform to HIPAA standards for data and document management. |  |
| GT | 8.15 | The system shall contain controls to maintain information integrity. These controls shall be in place at all appropriate points of processing. The controls shall be tested in periodic and spot audits following a methodology to be developed jointly by and mutually agreed upon by the Offeror and Community Healthcore. |  |
| GT | 8.16 | The Offeror shall house indexed images of documents used by Patients and Providers in the appropriate database(s) and document management systems so as to maintain the logical relationships between certain documents and certain data. |  |
| GT | 8.17 | The system shall enable Community Healthcore to modify the labels and arrangement of information in the data model documentation templates and can create custom data fields. |  |
|  | 8.18 | The system shall enable Community Healthcore to create custom data tables and fields. |  |
| GT | **9** | ***Audit support and compliance*** |  |
| GT | 9.01 | The Offeror shall provide secure, online access to select system functionality to at least five (5) Community Healthcore personnel to facilitate resolution of inquiries and to research issues as needed. |  |
| GT | 9.02 | Audit trails shall be incorporated into all systems to allow information on source data files and documents to be traced through the processing stages to the point where the information is finally recorded. The audit trails shall: a. Contain a unique log-on or terminal ID, the date, and time of any create/modify/delete action and, if applicable, the ID of the system job that effected the action; b. Have the date and identification “stamp” displayed on any on-line inquiry; c. Have the ability to trace data from the final place of recording back to its source data file and/or document shall also exist; d. Be supported by listings, transaction reports, update reports, transaction logs, or error logs; e. Facilitate auditing of individual claim records as well as batch audits; and f. Be maintained for ten (10) years in either live and/or archival systems. The duration of the retention period may be extended at the discretion of and as indicated to the Offeror by Community Healthcore as needed for ongoing audits or other purposes. |  |
| GT | 9.03 | The System shall support auditing at the object level (i.e. Table, Column) |  |
| GT | 9.04 | The System will allow an authorized administrator to set the inclusion or exclusion of auditable events based on organizational policy & operating requirements/limits. |  |
| GT | 9.05 | The System shall be able to perform time synchronization using Network Time Protocol (NTP)/Simple Network Time Protocol (SNTP) and use this synchronized time in all security records of time. |  |
| GT | 9.06 | The System shall prohibit all users read access to the audit records, except those users that have been granted explicit read access. |  |
| GT | 9.07 | The System shall protect the stored audit records from unauthorized deletion. The System will prevent modifications to the audit records. |  |
| GT | 9.08 | The System shall prevent modifications to the audit records. |  |
|  |  | **Conversion** |  |
| CON | 1 | The Offeror shall have a data conversion strategy and approach for supporting migration of data that emphasizes data integrity and no loss of referential integrity. |  |
| CON | 2 | The Offeror shall have a document conversion strategy and approach for supporting migration of documents that emphasizes no loss of referential integrity and ensures linkages across documents and between documents and applicable records are preserved. |  |
| CON | 3 | The Offeror shall have a record conversion strategy and approach that incorporates both data and document conversion and ensures no loss of referential integrity. |  |
| CON | 4 | The Offeror's approach to data, document and record conversion shall incorporate - at a minimum - a repeatable methodology that allows for backing out of conversions based on certain problems or issues being identified, thorough project planning, a proven project management methodology, specifics on how the relationship between source and target data structures will be defined and ensured, any changes in valid codes/values, and the use of automated tools. All of these will be detailed in a conversion plan which will be provided to Community Healthcore and approved by Community Healthcore before conversion activities are affected. |  |
| CON | 5 | The Offeror shall develop a Conversion Plan that will include a rollout schedule and the Offeror will perform (at a minimum) the following tasks: • Ensure a database backup is in place • Execute the data conversion packages • Validate the converted data to confirm success • Revert to backup if conversion failed • Provide Community Healthcore with of results of the conversion and any exceptions • Support Community Healthcore in the resolution nulls and non-converted data • Provide post conversion support through requested ad-hoc reporting and provision of access to the pre and post converted data for Community Healthcore confirmation analysis. |  |
| CON | 6 | The Offeror shall work with Community Healthcore to develop and implement a data conversion transition strategy consistent with any agreed-to phase-in of solution functionality (whether phase-in is based on programs or regions/geography) such that the solution and legacy systems are both properly populated, and the associated programs operating appropriately, during the implementation phase-in. This may involve a phase-in of the conversion of certain data. |  |
| CON | 7 | Describe your systems ability to import data multiple times during the implementation process before going live. Example: Staff initially uploaded at one point and then later import staffing to capture changes in personnel. |  |
|  |  | **Testing** |  |
| TEST | 1 | The Offeror will shall develop and submit a Test Plan. The Test Plan will include the procedures for documenting the completion of each test phase, test scripts, test conditions, test cases, and test reports. Detailed test plans will be created for the following testing areas: • Solution Component Unit Testing • Integration Testing • Security Testing • Availability and Performance Testing • User Acceptance Testing • Operational Readiness Testing  The Offeror shall be responsible for building test plans, executing test plans, and creating the requisite reports. Community Healthcore will evaluate the Offeror test plans and test results, and may validate the testing done by augmenting it with Community Healthcore testing. |  |
|  | 2 | The Testing Plan will also cover critical state/federal requirements of the EHR system including but not limited:   * Billing * Encounter Reporting * Care Batching * Texas Forms * Staffing and Credentialing * CCBHC Measures * FQHC measures |  |
| TEST | 3 | The Offeror shall organize and facilitate user acceptance testing (UAT) - testing conducted by system users to determine if specific system requirements and/or specifications have been met; UAT acts as a final verification of required system functionality and proper functioning of the system, emulating real-world usage conditions and employing test cases or scenarios. |  |
| TEST | 4 | The Offeror shall repeat any test cycle when a failure occurs at any stage of said cycle (e.g., a failure in User Acceptance Testing that necessitates a code change will require the component to go back through Unit Testing, Integration Testing, and so forth). |  |
| TEST | 5 | The Offeror shall provide Community Healthcore with the results of all testing activities defined in the Test Plan. |  |
| TEST | 6 | The Offeror shall update and maintain the test documents, procedures, and scripts throughout development and through full system acceptance to reflect the as-built design and current requirements. |  |
| TEST | 7 | The Offeror shall produce a User Acceptance Test (UAT) results report. The Offeror will support Community Healthcore User Acceptance Testing (UAT) activities, including: • Script development and requirements traceability • System support for the UAT environment • Document UAT Results for Community Healthcore management approval |  |
| TEST | 8 | The Offeror shall correct any functionality that does not pass UAT within a timeframe agreed to by Community Healthcore and perform system Regression Testing. |  |
|  |  | **Knowledge Management, Transfer, and Training** |  |
| KMT | 1 | The Offeror shall produce documentation for the entire system. |  |
| KMT | 2 | The Offeror shall produce user manuals including desk level procedures, for the system in the format and electronic version approved by Community Healthcore. |  |
| KMT | 3 | The Offeror shall store system documentation and user manuals electronically in a central location accessible by Community Healthcore staff. |  |
| KMT | 4 | The Offeror shall update all training documentation prior to the implementation of any new system changes while under contract with Community Healthcore. |  |
| KMT | 5 | The Offeror shall write system and component narratives so that they are understandable by non-technical persons. |  |
| KMT | 6 | The Offeror shall prepare system documentation that contains a general system narrative, system flow, a description of the operating environment and hierarchical, multi-level diagrams that depict the online and offline processes. Each component must be referenced, and documentation must be consistent across all components. |  |
| KMT | 7 | The Offeror shall organize user documentation in a procedural, step-by-step format. |  |
| KMT | 8 | The Offeror shall include a table of contents and index in all documentation. |  |
| KMT | 9 | The Offeror shall identify error messages including descriptions, for all fields incurring edits and provide the necessary steps to resolve. This list must be a composite of system level and component level errors. |  |
| KMT | 10 | The Offeror shall ensure that the use of acronyms and codes are consistent with windows, screens, reports and databases or data dictionary. |  |
| KMT | 11 | The Offeror shall: • Use abbreviations consistently throughout the documentation • Use field names consistently for the same fields throughout the documentation  • Include in the user manual tables of valid values for all data fields including codes • Include in the user manual illustrations of windows, frames, screens used, by component, with all data elements |  |
| KMT | 12 | The Offeror shall provide version control for all documentation to maintain historical document archives. |  |
| KMT | 13 | The Offeror shall provide the ability to print select pages, sections, and entire manuals. |  |
| KMT | 14 | The Offeror shall develop end user classroom training materials, including end of training assessment or comprehension tools. |  |
| KMT | 15 | The Offeror shall deliver centralized or regional train the trainer (T3) training to designated Community Healthcore resources no less than 30 days prior to each go live phase or pilot and implementation. |  |
| KMT | 16 | The system shall include online training that includes a self-guided introduction to the solution and a comprehensive training environment for programs and procedures based on user roles and program rules. |  |
| KMT | 17 | The system shall provide a training environment that replicates, **to the extent possible**, the functionality and operations of the production solution. This includes but is not limited to copies of software, tools, databases, and files loaded with copies of production cases. |  |
| KMT | 18 | The training environment shall have the functionality to add and change data based on user roles and business needs. |  |
| KMT | 19 | The training environment must provide an automated process to populate and refresh with production data customized according to business needs. |  |
| KMT | 20 | The training environment shall produce all outputs of the production environment. |  |
| KMT | 21 | The training environment shall have a process that ensures changes to the production solution are migrated to the end user training environment. |  |
| KMT | 22 | The Offeror shall provide knowledge transfer services at the end of the contract period as part of a transition or turnover plan to ensure Community Healthcore has knowledgeable system administrators and other technical support staff to maintain and operate the system independently. |  |
|  |  | **Hosting** |  |
| HOST | 1 | The Offeror shall host, maintain, and operate the solution within the United States of America. Please describe your hosting options. All systems and data must reside in the United States – Private data center preferred. Please describe you standard hosting options. |  |
| HOST | 2 | The solution shall be hosted in a Tier III or IV data center. |  |
| HOST | 3 | The Offeror will have a minimum of two locations with full hosting capacity. Locations must be separate in different Electricity Grid regions according to the USEPA and NERC of the continental US. Please list your sites. |  |
| HOST | 4 | The Offeror shall propose, specify, implement and support as many environments or instances within each environment type as necessary to fully support the design, construction, delivery, operation and ongoing maintenance of the solution as required by Community Healthcore |  |
| HOST | 5 | Do you support or provide any type of VPN/secure access to your hosted solution other than HTTPS? If so, what? |  |
| HOST | 6 | Discuss data archiving and restoring from archive within all applications of the software. What are the capabilities in restoring from archive? What tools/media are used for archiving data? |  |
|  |  | **Availability including Business Continuity and Disaster Recovery (BC-DR)** |  |
| BC-DR | 1 | The system shall be architected such that changes to operating environment or component applications/modules can be affected without availability being compromised. |  |
| BC-DR | 2 | The system shall be available for user access, including ad hoc reporting, during standard Community Healthcore business hours. |  |
| BC-DR | 3 | The system shall process data off hours as needed. |  |
| BC-DR | 4 | The BC-DR plan shall include initial development, continuous updates, ad-hoc updates as warranted by certain events/developments. |  |
| BC-DR | 5 | The Offeror shall ensure that the system is available to users twenty-four (24) hours a day, seven (7) Calendar Days a Week, except during periods of scheduled System Maintenance agreed upon by Community Healthcore and the Offeror. Unavailability caused by events outside of a Offeror’s span of control is outside of the scope of this requirement. |  |
| BC-DR | 6 | Upon discovery of any problem within its span of control that may jeopardize system availability and performance as defined in the contract, the Offeror shall notify the applicable Community Healthcore staff by electronic mail. The Offeror shall deliver notification as soon as possible but no later than 7:00 pm (Central Time) if the problem occurs during the Business Day and no later than 9:00 am (Central Time) the following Business Day if the problem occurs after 7:00 pm (Central Time). |  |
| BC-DR | 7 | Where the operational problem results in delays in report generation or problems in on-line access during the business day, the Offeror shall notify the applicable Community Healthcore staff within the first hour of discovery of the problem, in order for the applicable work activities to be rescheduled or be handled based on System Unavailability protocols. |  |
| BC-DR | 8 | Unscheduled system unavailability of system functions as deemed "critical" by Community Healthcore, caused by the failure of systems and telecommunications technologies within the Offeror’s span of control shall be resolved, and the restoration of services implemented, within thirty (30) minutes of the official declaration of System Unavailability. |  |
| BC-DR | 9 | Unscheduled system unavailability of all other Offeror system functions caused by systems and telecommunications technologies within the Offeror’s Span of Control shall be resolved, and the restoration of services implemented, • within four (4) hours of the official declaration of Unscheduled System Unavailability, when unavailability occurs during business hours, and • within two (2) hours of the start of the next Business Day, when unavailability occurs during non-business hours. |  |
| BC-DR | 10 | Cumulative system unavailability caused by systems and telecommunications technologies within the Offeror’s span of control shall not exceed two (2) hours during any continuous five (5) Calendar Day period for functions that affect client and enrollee services. For functions that do not affect clients and enrollees, cumulative System Unavailability caused by systems and telecommunications technologies within the Offeror’s span of control shall not exceed four (4) hours during any continuous five (5) Business Day periods. |  |
| BC-DR | 11 | For any system outage that is not corrected within the required time limits, the Offeror shall provide full written documentation that includes a Corrective Action Plan, describing how the problem will be prevented from occurring again, within five (5) Business Days of the problem’s occurrence. |  |
| BC-DR | 12 | Regardless of the architecture of its systems, the Offeror shall develop and be continually ready to invoke a **Business Continuity and Disaster Recovery (“BC-DR”) plan** that at a minimum addresses the following scenarios: (i) the central computer installation and resident software are destroyed or damaged, (ii) System interruption or failure resulting from network, operating hardware, software, or operational errors that compromises the integrity of transactions that are active in a live system at the time of the outage, (iii) System interruption or failure resulting from network, operating hardware, software or operational errors that compromises the integrity of data maintained in a live or archival system, (iv) System interruption or failure resulting from network, operating hardware, software or operational errors that does not compromise the integrity of transactions or data maintained in a live or archival system but does prevent access to the system, i.e. causes unscheduled system unavailability. The BC-DR plan shall account for and be in effect during the entire period beginning with project kickoff and continue throughout the contract period. Offeror will update the plan as needed. This BC-DR plan and any updates must be prior approved by Community Healthcore. |  |
| BC-DR | 13 | The Offeror shall test its BC-DR plan through simulated disasters and lower level failures in order to demonstrate to Community Healthcore that it can restore System functions per the standards outlined elsewhere in this Section. The results of these tests shall be reported to Community Healthcore within thirty (30) Calendar Days of completion of said tests. The frequency of these tests will be agreed upon between Community Healthcore and the Offeror but shall be annual at a minimum. |  |
| BC-DR | 14 | In the event that the Offeror fails to demonstrate in the tests of its BC-DR plan that it can restore system functions per the standards outlined in this Contract, the Offeror shall be required to submit to Community Healthcore a Corrective Action Plan that describes how the failure will be resolved. The Corrective Action Plan will be delivered within five (5) Business Days of the conclusion of the test. |  |
| BC-DR | 15 | The Offeror shall submit a monthly Systems Availability and Performance Report to Community Healthcore in accordance with the specs in defined in the SLAs. |  |
| BC-DR | 16 | The system will have the ability to support session replication and transparent failover using high-availability architectural options. |  |
| BC-DR | 17 | The system's Recovery Point Objective (RPO) will be no more than 1 hour of data loss. In case of a disaster that effects operations, 1 hour of data inputs to the system (but no more) may be lost and need to be re-entered. |  |
|  |  | **Maintenance and Operations** |  |
| MO | 1 | Upon completion and acceptance of each solution implementation phase, the Offeror shall provide a one hundred and eighty (180) calendar day warranty period for the respective phase in which the Offeror will support the system at no additional cost to Community Healthcore and provide all necessary technical support, updates and fixes necessary to operate the solution in the manner prescribed. |  |
| MO | 2 | Upon expiration of the warranty, the Offeror shall provide a fee-based annual maintenance and operations program to include all technical support, updates and fixes necessary to operate the solution in the manner prescribed. |  |
| MO | 3 | The Offeror shall develop a comprehensive system **maintenance and operations (M&O) plan**. The M&O plan shall be submitted to the Center for review and approval and must, at a minimum: • Ensure the Offeror's system continually meets Community Healthcore requirements;  • Ensure that system maintenance windows do not interfere with Community Healthcore business or occur during business hours; • Accommodate new legislation and evolving regulations, standards, and Community Healthcore organizational processes; and • Provide regular and periodic maintenance to the system on a semi-annual basis or on a schedule agreed upon by the Offeror and Community Healthcore. |  |
|  |  | **Issue and Problem Management** |  |
| ISS | 1 | The Offeror shall use a single-Issue Tracking System, agreed to by Community Healthcore, that the Offeror and Community Healthcore will use collaboratively for the tracking of system defects, security issues, data quality anomalies, enhancements, and other system issues or change management items. |  |
| ISS | 2 | The Issue Tracking System shall, at a minimum, include: • All defects in the solution identified during any testing phase must be recorded, prioritized, tracked, and resolved in a timely manner. Each must be assigned a “Defect Level” based a mutually agreed upon standard (e.g., Critical, Serious, High, Moderate, Low, etc.) • The Offeror will allow Community Healthcore full access to the Issue Tracking System. • The Offeror will address defects as such: Critical and serious defects may require remediation and retesting before the solution enters production. All defects will be fixed and tested to Community Healthcore's satisfaction prior to system acceptance during the implementation phase. |  |
| ISS | 3 | The Offeror will use a release management approach to correct defects and installing any other changes and will only implement the release once Community Healthcore has signed off on all changes and has agreed that all defects are fixed or do not impact customers or staff. |  |
|  |  | **Solution Administrator Support** |  |
| SAS | 1 | The Offeror shall provide a Help Desk which will serve as the single point of contact for the reporting of solution issues. The Help Desk, to be staffed during business hours (to be determined by Community Healthcore), will provide support for issues related to the systems business and technical functionality which need to be escalated for investigation and resolution. The Help Desk and associated staff must be physically located in the continental United States. |  |
|  |  | **Staffing** |  |
| STAF | 1 | The Offeror shall provide and retain qualified staffing at levels necessary to ensure successful implementation of the system, as well as support for the system through the life of the contract as bid. |  |
| STAF | 2 | Community Healthcore shall have the right to request Offeror staff be replaced in the event of incompatibility and the Offeror will propose replacement staff within 1 week of notification by Community Healthcore. |  |
| STAF | 3 | The Offeror shall adhere to the following general requirements for all staff: • The Offeror must comply with all federal and Texas state requirements concerning fair employment, employment of the disabled, and the treatment of all employees without regard to race, color, religion, national origin, or physical disability • The Offeror must follow all federal and Texas state laws regarding Social Security registration and legal work status of all staff employed or contracted by the Offeror or subcontractor |  |
| STAF | 4 | The Offeror shall provide the following information regarding subcontractors.  • Subcontractors name and address • Subcontractors qualifications • Tasks the subcontractor will perform • The estimated percentage of total contract dollars for each subcontract. • Plan for managing subcontractors Subcontractors are those that are employed and managed by the Offeror, who have responsibilities of the project. Community Healthcore reserves the right to prior accept all subcontractor(s) and their work locations. |  |
|  |  | **Assurances** |  |
| ASU | 1 | No offshoring of any business function or information technology service shall be allowed **either pre or** post-implementation of the solution. Offshoring is hereby defined as the relocation, by a company, of (1) a business process from one country to another—typically an operational process, such as manufacturing, or supporting processes, such as accounting or (2) the outsourcing of technical and administrative services from outside the home country ("offshore outsourcing"), by means of internal (captive) or external (outsourcing) delivery models. |  |
| ASU | 2 | The Offeror shall commit to stay continuously informed of all in-scope health care program changes including but not limited to : information management and reporting regulations and sub regulatory guidance including but not limited to HHS, CMS, TDCJ, TDPF, SAMHSA and the State of Texas might devise and promulgate with regards to in-scope programs, communicate these to Community Healthcore and proactively propose optimal approaches for addressing said changes. This assurance is aimed at achieving continual compliance with all applicable federal and state requirements. |  |