**Technical Standards  
Electronic Health Records**

03/03/2016

Vendor shall review the following technical standards and indicate deviations with explanation. A non-response indicates technical standard agreed compliance.

Download [MS Excel version](http://austinea.org/arch/hhs/ehr/technicalStandards/technicalStandardsEHR_update.xlsx)

**SaaS/PaaS** - Solutions using Software as a Service (SaaS).

Mandatory - Essential requirement  
Expected - Anticipated or presumed requirement

| **ID** | **Topic** | **Description** | **SaaS** |
| --- | --- | --- | --- |
| 1 | Application Architecture | The application provides Web-enabled components to meet the Rehabilitation Act of 1973 Section 503, W3C and industry standards for graphics and design; speed; reliability; and security for dynamic content and user interaction. | Mandatory |
| 2 | Application Architecture | No requirement to deploy additional application, code or 3rd party plug-in to client workstations (note: If Java Runtime Environment (JRE) is required, please list all supported versions). | Mandatory |
| 3 | Application Architecture | The application provides the ability to automate the deployment of software and updates to user workstations including, but not limited to Web-based deployment tools to push/pull software to the desktop (note: applicable only to run-time environment, like Java). Unless the contractor provides an alternative solution, users do not require administrative privileges. | Mandatory |
| 4 | Application Architecture | The application provides built-in application and system configuration tables accessible by all modules. | Mandatory |
| 5 | Application Architecture | The application provides forms-based data validation (field level validation) and displays error messages when validation fails (i.e., user enters text in a numeric field). | Mandatory |
| 6 | Application Architecture | The application provides copy, cut, paste, and undo functions from all data fields to/from other applications. | Mandatory |
| 7 | Application Architecture | The application provides ability to perform mass changes to a defined group of transactions with appropriate selection criteria. Sometimes item descriptions or nomenclature change, the application provides advanced users of the system the ability to globally replace textual items with identity grouping constraints using SQL (or similar technology) like replacements when necessary. | Mandatory |
| 8 | Application Architecture | The application provides ability to effective date transactions and table updates including, but not limited to future and retroactive changes, based on user-defined criteria. | Mandatory |
| 9 | Application Architecture | The application provides ability to drill down from a transaction view to the supporting source document or record, regardless of the module source. | Mandatory |
| 10 | Application Architecture | The application provides ability to apply upgrades and patches without impact to existing user interface customizations (e.g., user-defined forms/fields, Web interface, etc.). | Expected |
| 11 | Application Architecture | Solution provides a patch management program that includes testing patches prior to implementation. | Expected |
| 12 | Data Entry Support and On-Line Help | The system provides ability to restrict free form entry for structured data types (e.g., require use of drop-down calendar for date field). | Mandatory |
| 13 | Data Storage and Archiving | The solution provides a complete copy of hosted data using comma separated view (CSV) format or other agreed to and usable formats in the event of contract termination with 30 days of the request. | Mandatory |
| 14 | Data Storage and Archiving | The solution supports future releases of the application without rendering the archived data unusable or provides an upgrade script to convert archived data to supported format. | Mandatory |
| 15 | Data Storage and Archiving | The solution provides online access to the current year plus unlimited previous years of all types of data retained in the system, and provides archive capabilities thereafter for inactive historical records. The solution provides a method to retrieve archived records back into active state. | Expected |
| 16 | Database Architecture | The application provides standardized data extraction functions or Application Program Interface (API) to allow import and export of data to/from other systems. | Mandatory |
| 17 | Database Architecture | The application provides ability to encrypt sensitive data - federal or state compliance required (e.g., PII, PCI, HIPAA, etc.). | Mandatory |
| 18 | Database Architecture | The application provides ability to exchange database information using industry accepted standards and formats including JavaScript Object Notation (JSON). The solution uses the same data validation criteria for bulk data loads as it does for manual data entry. The application provides ability to exchange database information using industry accepted standards and formats including Extensible Markup Language (XML). | Mandatory |
| 19 | Database Architecture | The application provides ability to perform database maintenance including, but not limited to, backup and upgrades without requiring system downtime during core business hours. | Expected |
| 20 | Database Architecture | The solution includes a method of purging record data from the database(s) ensuring referential integrity with master/child records. | Expected |
| 21 | End-User Interface | The system meets Web Accessibility standards including, but not limited to, ability to support ADA and compliant with Section 508 of the Federal Rehabilitation Act (see http://www.access-board.gov/sec508/summary.htm). Web based applications must be ADA compliant following the specifications of 508c of the Americans With Disabilities Act. If compliance is not possible, reasonable alternatives may be considered. | Mandatory |
| 22 | Information Management | The system prevents the loss or unauthorized deletion of records before the expiration of their retention period as authorized by an approved records control schedule or with the written permission of the Texas State Library and Archives Commission. Texas Local Government Records Act §202.001(a). | Mandatory |
| 23 | Information Management | The system prevents the unauthorized alteration of records before the expiration of their retention period. The system provides logs or audit trails that document edits and views of records. This is a requirement for records governed by HIPAA; and, depending on the type of record, there may be additional integrity requirements governed by Texas House Bill 300. | Mandatory |
| 24 | Information Management | The system provides systematic deletion of records upon expiration of their retention period as authorized by an approved records control schedule or with the written permission of the Texas State Library and Archives Commission. Texas Local Government Records Act §202.001(a) and §201.003(16), Austin City Code §2-11-11. Sufficient metadata must be present to identify records eligible for disposition based on defined triggering events and dates. | Mandatory |
| 25 | Information Management | Upon expiration of the retention period, the system ensures destruction of all duplicate records to include convenience copies. Texas Rules of Evidence, Rule 1003. The system's back-up strategy ensures retention of backup records doesn't excessively exceed destruction of originals. System procedures must ensure retention rules apply to copies of production data used to develop, test, or train. | Mandatory |
| 26 | Information Management | The system ensures records are retrievable and available until the expiration of their approved retention period. Texas Local Government Records Act §205.008(b). Records stored on contractor, outsourced, cloud, or hosted platforms remain the property and responsibility of the City. When contacted by an authorized City employee or when the contract ends or is terminated, contractors must deliver records, in all requested formats and media, along with all finding aids and metadata, to the City at no cost. Austin City Code §2-11-15. | Mandatory |
| 27 | Information Management | Until expiration of retention period, hardware and software must be available to access records and sufficient metadata must be present to facilitate timely retrieval of records. Contracts with hosted solution providers must specify the contractor’s duties with respect to management of records as required by Austin City Code §2-11-15. The system ensures retention of specific records – even if their retention period has expired – if they are the subject of known or reasonably anticipated litigation, public information request, audit or other legal action. Texas Local Government Records Act §202.002, Austin City Code § 2-11-11. The system maintains a log of litigation and other holds allowing release of holds after resolution of litigation, audit, or public information requests. | Mandatory |
| 28 | Information Management | The system creates records/logs of destruction activity. Texas Local Government Records Act §203.046, Austin City Code §2-11-11. Destruction logs must (a) show a minimal set of metadata sufficient to uniquely identify the records purged; (b) show who approved and who executed the destruction, and the dates on which these events took place; (c) reflect compliance with an approved, written standard operating procedure; and (d) be retained permanently. | Mandatory |
| 29 | Information Management | Solution provides a data recovery plan and tested procedures within the last 6 (six) months. | Mandatory |
| 30 | Integration Architecture | If application requires integration with other City data, the application must integrate using industry standards useful to a service-oriented architecture (SOA) and an enterprise service bus (ESB). | Expected |
| 31 | Security and Authentication | The system uses Microsoft Active Directory Federated Services (ADFS) [current version minus 1] for federated identity management. The City is migrating to Microsoft Office 365 (O365) and ultimately migrating to a Microsoft managed Active Directory service. Therefore, the system uses single sign on for application access. | Expected |
| 32 | Security and Authentication | The system allows user registration and de-registration, at a minimum, communicates relevant policies to users and requires signed acknowledgement, checks authorization and minimum level of access necessary prior to granting access, ensures access is appropriate to the business need (consistent with sensitivity/risk and does not violate segregation of duties requirements), addresses termination and transfer, ensures default accounts are removed and/or renamed, removes or blocks critical access rights of users who have changed roles or jobs, and automatically removes or disables inactive accounts. | Mandatory |
| 33 | Security and Authentication | Conduct an annual security assessment of all tiers of hosting facility, including application servers and network devices. Provide annual summary copies of the security audit reports to the City of Austin. We prefer an annual 3rd party security assessment, which we may require depending on the hosted data. | Mandatory |
| 34 | Security and Authentication | The system provides ability to restrict remote access to the application by client IP address or network address range. | Expected |
| 35 | Security and Authentication | Vendor provides a Health Insurance Portability and Accountability Act (HIPAA) Report on Compliance (HROC) or SSAE 16 SOC 2 Type II validating they are compliant against the Office for Civil Rights (OCR) HIPAA Audit Protocol covering HIPAA Privacy Rule, Security Rule and Breach Notification Rule. | Mandatory |
| 36 | Security and Authentication | Solution provides a process for secure disposal of data when requested by COA. | Mandatory |
| 37 | Security and Authentication | Solution/Application provides SSAE 16 or SAS70 audit covering application controls. | Expected |
| 38 | Security and Authentication | Solution provides regularly engagements with 3rd parties to perform system evaluation. | Expected |
| 39 | Security and Authentication | Solution provides journals and/or procedures to determine compromised assets. Solution provides system vulnerability scans on a regular basis, notifies user staff, and publishes potential issues and risks. | Mandatory |
| 40 | Security and Authentication | Solution utilizes methods to detect and block application level software attacks. | Mandatory |
| 41 | Security and Authentication | The solution performs SAS70, SSAE16, or SOC1 data center audit and a current report is available for review. | Expected |
| 42 | Security and Authentication | Application audit logs record and are regularly reviewed to examine user IDs, dates, and times of log on and log off, log in failures, changes to security parameters, and other security actions. | Mandatory |
| 43 | Security and Authentication | All data encrypted (even at rest) using 256 bit AES encryption or better/similar technology. | Mandatory |
| 44 | Security and Authentication | Solution securely transmits data over public networks. | Mandatory |
| 45 | Security and Authentication | Solution provides emergency access (only) for authorized personnel while maintaining appropriate security controls. | Mandatory |
| 46 | System Flexibility | The system provides the ability to define business rules based on user-defined criteria (e.g., organizational level, account code, bargaining unit, location, program, grant, etc.). | Expected |
| 47 | System Flexibility | The application provides integration with patient survey system. | Expected |