|  |
| --- |
| **National Framework Agreement for Legacy Information Integration and Management**  **Project Reference: F/085/LIM/22/SM**  **SCHEDULE A**  **FRAMEWORK AGREEMENT SPECIFICATION** |

**SCHEDULE A. FRAMEWORK AGREEMENT SPECIFICATION**

1. **Legacy Information Integration and Management**

Legacy Information Integration and Management is defined as the system(s) and/or services required to host and integrate data from multiple archived systems into one live system, such as an Electronic Patient Records (EPR) system. This will result in quicker and easier access to archived data and allow contracts with archived systems to be ended.

The Supplier’s Solution must seamlessly interface with the Participating Authority’s Electronic Patient Records (EPR) system, or other system(s) as determined by the Participating Authority.

The Participating Authority will provide the Supplier with the following:

* Name(s) of the current system(s) where data is held
* Size of the database(s)
* Current hosting location(s) e.g. cloud-based or on-site
* Database type(s) e.g. SQL etc.)
* Number of patients in the system(s)
* Proposed timelines

The Supplier will work with the Participating Authority to develop a project plan from this information and agree timelines.

The Supplier should have experience with large, complex migrations and archiving of a range of systems including, but not limited to:

* Electronic Patient Records (EPR) systems
* Department-specific records systems e.g. Radiology Information Systems (RIS)
* Picture Archiving and Communication Systems (PACS)
* Financial systems

The Solution must be able to operate across multiple facilities, including but not limited to separate sites and/or hospitals in the same Trust, or multiple Trusts or organisations working together.

**General Requirements**

Systems must not compromise any Contracting Authority’s compliance with the NHS Data Security and Protection Toolkit (DSPT) Standard.

Systems must support role-based user access and be accessed through secure password or pass card.

Systems must provide that screens lock after a predefined period of inactivity if required and log a user out of the system on screen lock.

By default, systems must be in “private” mode or locked mode showing minimal patient information.

Users must log in to the system to access any functionality.

Systems must support the authentication of individual users and not just groups.

All user authorisation facilities must be maintained centrally and integrated across all system modules, such that user/group access profiles can be defined once and applied consistently through the system.

Systems must be capable of implementing and supporting role-based access and allow different user profiles to be linked to a user’s Active Directory profile.

Systems must contain controls that can ensure that individuals can be held accountable for their actions.

Solution components should be internally integrated so that users do not need to switch between modules to perform their roles.

Systems must be compatible with all commonly used server/client anti-virus software.

The transfer of data via wireless or fixed line communications must be protected from interception, where sensitive data is being transmitted over a public network, e.g., the internet.

Data transferred and/or stored must be encrypted, with an encryption key length of 128 bits as a minimum with wireless keys.

Backup processes must not involve system down time, interruption or degradation of service.

Systems, if web-enabled, must operate properly with standard configurations of all commonly available network browsers. Any restrictions on network browsers or on versions thereof supported must be notified to the Framework Manager and to Contracting Authorities.

Access to the archived data must be via Single Sign-On (SSO) from within the EPR.

The data should be accessible in a way that is user friendly and intuitive to use.

The Solution will be customisable to meet the requirements set out in this specification and the requirement of Contracting Authorities.

The Supplier must utilise highly secure data capture, transmission, storage and analysis processes.

Systems must offer/be compliant with Cloud Native hosting from UK location(s) only.

Suppliers must operate a defined quality management system for the design, development, manufacture, service, installation and distribution of their archive Solution to the standard of EN ISO 9001:2008 or operate a quality management system to an equivalent level. Details of this quality management system will be made available to Contracting Authorities on request.

Suppliers must operate a defined quality management system for their servicing and technical support services. Details of this quality management system will be made available to Contracting Authorities on request.

Suppliers must follow a defined and documented software quality accreditation process to a level at least equivalent to that of IS EN ISO 9001:2008 (or an equivalent recognised standard).

Suppliers must operate a defined and documented information system security management system to a level at least equivalent to that of IS EN ISO 27001:2013 (or an equivalent recognised standard). Details of this information system security management system will be made available to Contracting Authorities on request.

Suppliers must hold (or commit to obtain, prior to commencement of the Framework Agreement if awarded) Cyber Security Essentials Plus accreditation.

Suppliers must provide the results of a recent comprehensive remote security assessment and penetration test (Pen test), demonstrating their system resistance to attack.

Implementation processes must follow a defined and documented project methodology (for example PRINCE2).

Contract Implementation Plans are required for each Contract under this Framework (preferably in Gantt chart format); this must reflect the planned procedure of data migration and integration, setting out expected timetables for the completion of activities.

The Implementation Plan provided by the Supplier is subject to alteration and agreement with the Participating Authority(s).

The Supplier may provide data validation services if requested by the Participating Authority.

Suppliers must be committed to continuous product improvement with a clear development roadmap for their product/applications proposed. Suppliers must commit to provide details on expected enhancements with scheduled dates for same to Contracting Authorities.

Suppliers must be registered with the Information Commissioners Office as a Data Processer throughout the life of the Framework Agreement and the period of all Contracts called off from the Framework Agreement.

Suppliers must take full responsibility for implementing and supporting their archive system regardless of whether those goods or services are delivered by the Supplier or a third party(s).

Suppliers must hold, and commit to hold throughout the period of the Framework Agreement and any Contracts called off from the Framework Agreement, all necessary OEM accreditations and licences and rights to exploit any intellectual property for each element of software modules that are considered to form part of the product/application proposed.

On written request from a Contracting Authority, Suppliers must provide relevant sections of any third-party contracts on which they rely to deliver their proposed system and/or services. Such contracts, where they exist, must be of sufficient nature so as to support the requirements of the Contracting Authority.

The system should permit for searches using multiple different terms including but not limited to patient name, date of birth and NHS number. NHS number must be the core data record utilised for archived data.

The data centre/server facility where the archived data will be held must be located in the UK.

The Supplier will provide the quantity of licenses agreed with the Participating Authority. There must be a mechanism for requesting additional licenses as and when required.

The Solution should not store protected health information in the cache.

The Supplier must comply with the following:

* Data Protection Act 2018
* Caldicott Guidelines 1997
* The relevant requirements of the Access to Health Records Act 1990
* Access to Medical Reports Act 1988
* Confidentiality Code of Practice 1998
* Any other relevant statutory requirements
* Any amendments to the above

**Service and Support**

Suppliers will provide support for both functional and non-functional components of their system. Support will be available for the following areas at a minimum:

* Support at Go-Live
* Post Go-Live support (including out of hours support)
* Call logging procedures and response times
* Escalation procedures
* Business Continuity and Recovery
* New Functionality / Requirements Requests

The Solution should have online help functionality for all system functions.

Suppliers will provide maintenance, inspections and software update services to ensure optimal equipment performance and minimise system downtime. Software updates will be included at no additional cost in all levels of maintenance plan.

Suppliers will offer a range of service and maintenance plans to fit the requirements of Participating Authorities.

Suppliers will provide a detailed maintenance schedule at the commencement of each Contract.

The Supplier must have detailed and robust backup and disaster recovery processes in place in case of server(s) going down, to minimise the impact to Participating Authorities and prevent the loss of data.

Backup processes must not involve system down time, interruption or degradation of service.

Systems must be available to staff 24 hours per day, 7 days per week and 365 days per year (366 days in a leap year). Any system must provide for a complete disaster recovery (DR), which will require the same level of support as the normal live system.

Customer support should be available 24 hours per day, 7 days per week and 365 days per year (366 days in a leap year). Expected response times to queries will be agreed with Participating Authorities at Call Off Contract stage.

**Training**

Suppliers will provide comprehensive training, both on-site and on-line, to support the successful implementation of their Solution.

Training for key staff will be available during implementation, at go live and in the post go live period.

Training will be tailored to the needs of potential users across the hospital and or healthcare system.

Suppliers will provide Contracting Authorities with online documentation to assist the Contracting Authority in its use of the Solution.

The Supplier must provide training to cover support of the Solution, including backup, access and troubleshooting. This may be provided at the Participating Authority’s site(s) and/or virtually. Ideally both options will be available.

Soft copy manuals and/or user guides must be made available to the Participating Authority.

When a new version is released, the Supplier must provide soft copy release notes as a minimum in advance of the new version being released. If significant changes have been made, it is expected that additional training should be offered by the Supplier to the Participating Authority staff.

**Reporting Analysis and Audit**

The Solution will have the ability to output to printers, screens, multi-function devices and files.

Solutions must have a detailed audit trail capability.

The Solution must have the capability to run reports for data, audit logs and analytics. Ideally, trained users will be able to create their own reporting templates to be run on an ad-hoc basis and/or auto-run at intervals to be set by the user.

The Solution must be able to report on the following areas as a minimum:

* Real-time storage capacity
* Growth of the database size
* Upcoming data purge details
* Data age, archive type and purge date

The Solution must allow the export of reports into a range of formats, including Excel.

The Solution must provide data and access auditing, including the retention of activity logs.

**Interfacing**

Systems will interface bi-directionally with Participating Authority systems via HL7 (examples of systems include but are not limited to; Patient Administration Systems, Electronic Patient Records Systems, Radiology Information Systems and Picture Archiving and Communications Systems).

Systems will accept and display orders and results from other third-party systems.

Systems will accept scanned documentation via an Electronic Document Management System or via direct scanning.

The Supplier must maintain expertise in, and compatibility with, the Electronic Patient Records system used by a Participating Authority throughout the term of the Framework Agreement, and any subsequent Call Off Contracts.

# Data Formats

The Solution must support a variety of data formats to cover the full range of data to be migrated. Required data types may include but not be limited to:

* DICOM images and associated reports
* Waveform data such as haemodynamic, foetal etc
* Visible light images and video such as endoscopic, surgical or digital photos
* Open data formats such as XML, CSV, PDF and others
* Other such data formats as are required by the Participating Authority

# Data Migration

Data migration processes should restore the original access time to files on the source when reading and copying them to the destination.

The Supplier must have robust processes in place to ensure there is no duplication or skipped data in the event of a failure requiring the re-starting of the migration operation.

As part of the migration process, the migration utility should run a checksum, and then compare that with the checksum of the file that’s been written to the destination to identify errors.

Any permanent failures during data migration must be identified and reported to the Participating Authority.

The Solution should ideally be optimised to rapidly scan for files that have changed to allow for quick migrations of changed data.

The Solution must provide the ability for staff to specify archive and purging rules according to data retention policies. This should ideally be an automated process, once specified. Where data must be exceptionally kept outside of the data retention policies, it must be possible to override the planned destruction of specific or groups of documents until such time as they are no longer required.

The Solution must archive all data; including data used in the production system, audit data, inbound and outbound correspondence, attachments, notes, reports, and log files; in compliance with applicable data retention policies.

System data integrity must be maintained during the archive process.

Archived records must be identified as such by systems.

The Solution must prevent audit trails from being deleted, except in compliance with defined record retention, purge and archival criteria.

The Solution must perform routine reviews of archived data to verify no loss of archived files and verify the ability to retrieve archived files.

The Solution should support complex searches of content within documents.

Searches extracting records from the archive should not noticeably impact system response times.

After the initial data migration, Participating Authorities may require future archiving of systems, such as when existing contracts expire. The Supplier should work with Participating Authorities to plan future migrations. This plan may be subject to change by the Participating Authority.

Some classes of data must be retained for long periods of time. The Solution must support the long term storage of such data.

# 

# Technical Requirements

The Solution must at a minimum be able to utilise standard desktop PCs and laptop computers as workstations. Other workstation options such as tablets may be required and will be detailed by the Participating Authority at Call Off Contract stage.

It should be possible to run the Solution in a Citrix environment if required.

Remote access to the Solution may be required, and this must be supported.

The Solution should have a test environment available to designated users.

The Supplier must work with the Participating Authority to ensure the Solution can support the Authority’s security patching methodology.

The Supplier must be able to offer customer support to the Participating Authority’s IT team, where the IT team are offering first line support to users.

The Participating Authority may also require customer support routes for users. Where this is required, it will be agreed at Call Off Contract stage.

The Solution’s architecture should permit VPN/external tunnels for remote support, application access and data transfers to allow the Participating Authority’s IT team to offer user support.

The Solution must utilise secure cryptographic protocols for data transfer within networks, such as the current version of TLS or other such protocols as are requested by the Participating Authority.

The Solution should support multi-factor authentication.

It must be possible to limit access to data in the archive based on role.

Where the database is cloud-based, backups of archived data must be completed at intervals agreed with the Participating Authority. These must be retained for a period of one year.

Where the database is held on-site, the Participating Authority will be responsible for backing up the archived data.

The Solution should operate on standard desktop and laptop computers. Where any additional hardware, equipment or technology such as the installation of specific software is required to view or administrate the Solution this must be made clear to Participating Authorities at Call Off Contract stage.

The Solution must have open APIs.

The Solution must utilise a web-based user interface.

The Solution must be compliant with the following standards:

* Fast Healthcare Interoperability Resources (FHIR) Standard.
* DCB0129 (Clinical Risk Management Standard)
* SNOMED CT and/or ICD10