PACS, RIS, image archive and sharing services

Core statement of requirements

PACS programme
18 November 2011
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glossary of terms</td>
<td>6</td>
</tr>
<tr>
<td>Terminology</td>
<td>8</td>
</tr>
<tr>
<td>Definitions</td>
<td>9</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>10</td>
</tr>
<tr>
<td>1.1 Background</td>
<td>10</td>
</tr>
<tr>
<td>1.2 Purpose</td>
<td>10</td>
</tr>
<tr>
<td>1.3 Commercial context</td>
<td>10</td>
</tr>
<tr>
<td>1.4 Requirement scope</td>
<td>11</td>
</tr>
<tr>
<td>2 Core principles</td>
<td>12</td>
</tr>
<tr>
<td>2.1 Background</td>
<td>12</td>
</tr>
<tr>
<td>2.2 Scope</td>
<td>12</td>
</tr>
<tr>
<td>2.3 Technology</td>
<td>12</td>
</tr>
<tr>
<td>2.4 Patient safety</td>
<td>13</td>
</tr>
<tr>
<td>2.5 Interoperability and connectivity</td>
<td>13</td>
</tr>
<tr>
<td>2.6 Assured products</td>
<td>13</td>
</tr>
<tr>
<td>2.7 Variation and Choice</td>
<td>14</td>
</tr>
<tr>
<td>2.8 Pricing</td>
<td>14</td>
</tr>
<tr>
<td>3 Functional requirements</td>
<td>15</td>
</tr>
<tr>
<td>3.1 General imaging requirements</td>
<td>15</td>
</tr>
<tr>
<td>3.2 Interoperability and interfacing</td>
<td>18</td>
</tr>
<tr>
<td>3.3 Storage requirements</td>
<td>21</td>
</tr>
<tr>
<td>3.4 Network requirements</td>
<td>23</td>
</tr>
<tr>
<td>3.5 Commercial off the shelf (COTS) products</td>
<td>24</td>
</tr>
<tr>
<td>3.6 Functional requirements - PACS</td>
<td>24</td>
</tr>
<tr>
<td>3.7 Functional requirements – RIS</td>
<td>30</td>
</tr>
<tr>
<td>Requesting</td>
<td>31</td>
</tr>
<tr>
<td>Worklists</td>
<td>32</td>
</tr>
<tr>
<td>Appointments</td>
<td>32</td>
</tr>
<tr>
<td>Booking</td>
<td>33</td>
</tr>
<tr>
<td>Examinations</td>
<td>34</td>
</tr>
<tr>
<td>Clinical reporting</td>
<td>36</td>
</tr>
</tbody>
</table>
PACS, RIS, image archive and sharing services. Core statement of requirements.

Data handling and security............................................................................................................. 37
Billing ........................................................................................................................................... 38
Messaging requirements .................................................................................................................. 38
Management statistics and administration .................................................................................... 38
Shared RIS instances ...................................................................................................................... 39
Standards.......................................................................................................................................... 40
3.8 Functional requirements - CR / DR .......................................................................................... 40
Digitiser/ CR Reader .......................................................................................................................... 42
CR Image capture plates .................................................................................................................. 42
3.9 Acquisition workstation ............................................................................................................. 43
3.10 Voice recognition (VR) ............................................................................................................ 44
Dictionary and spelling .................................................................................................................... 45
Reporting .......................................................................................................................................... 45
Training ............................................................................................................................................. 45
Editing .............................................................................................................................................. 45
Security ............................................................................................................................................ 45
3.11 Radiotherapy/ oncology.............................................................................................................. 45

4 Non Functional Requirements .................................................................................................... 46
4.1 Performance requirements .......................................................................................................... 46
4.2 Reliability/availability ................................................................................................................. 46
4.3 Scalability .................................................................................................................................... 46
4.4 Information Governance .............................................................................................................. 46
Authentication .................................................................................................................................... 46
RBAC .................................................................................................................................................. 47
Legitimate relationships, restricted access and consent ................................................................. 48
Network ............................................................................................................................................ 48
Session ............................................................................................................................................. 49
4.5 Audit and Audit Analysis ............................................................................................................ 49
Audit .................................................................................................................................................. 49
Audit analysis ..................................................................................................................................... 50
Functional requirements .................................................................................................................. 51

5 Service delivery ............................................................................................................................ 51
5.1 Joint management and collaboration .......................................................................................... 51
Implementation .................................................................................................................................. 52

Copyright © 2013, Health and Social Care Information Centre.
6 Service management

6.1 Availability management ................................................................. 57
6.2 Performance management ................................................................. 58
6.3 Hosted communications infrastructure .............................................. 59
6.4 Service provision and management requirements ................................ 60
6.5 Service levels .................................................................................... 61
6.6 System maintenance ........................................................................ 65
6.7 Response times .................................................................................. 66
6.8 Severity levels .................................................................................... 66
6.9 Fix times ............................................................................................. 67
6.10 Problem management ....................................................................... 67
6.11 Service desk ....................................................................................... 67
6.12 Service failure log ............................................................................ 70
6.13 Escalation .......................................................................................... 70
6.14 Resolving service failures ................................................................. 70
6.15 Performance reporting and performance review ............................... 70
6.16 Additional considerations ................................................................. 71
6.17 System configuration and monitoring ................................................. 71

7 Standards

7.1 Safety standards ................................................................................ 71
7.2 Imaging standards .............................................................................. 72
7.3 Integrated Healthcare Enterprise (IHE) ............................................... 72
7.4 Information Standards Board (ISB) Standards .................................. 73

8 Image archive requirements

8.1 Overview ............................................................................................ 74

9 Image archive services

9.1 Key general service requirements ....................................................... 76
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2 Functional requirements</td>
<td>76</td>
</tr>
<tr>
<td>9.3 Non Functional requirements – image archive services</td>
<td>84</td>
</tr>
<tr>
<td><strong>10 Sharing services</strong></td>
<td>85</td>
</tr>
<tr>
<td>10.1 Functional requirements</td>
<td>85</td>
</tr>
<tr>
<td>10.2 Non functional requirements</td>
<td>89</td>
</tr>
</tbody>
</table>
# Glossary of terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>ADT</td>
<td>Admit Discharge Transfer</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface</td>
</tr>
<tr>
<td>ATNA</td>
<td>Audit Trail and Node Authentication</td>
</tr>
<tr>
<td>AV</td>
<td>Antivirus</td>
</tr>
<tr>
<td>CAP</td>
<td>Common Assurance Process</td>
</tr>
<tr>
<td>CCN</td>
<td>Change Control Note</td>
</tr>
<tr>
<td>CE</td>
<td>Conformite Europeene</td>
</tr>
<tr>
<td>CHECK</td>
<td>The National Technical Authority for Information Assurance</td>
</tr>
<tr>
<td>CIS</td>
<td>Cardiology Information System</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information related Technology</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off The Shelf</td>
</tr>
<tr>
<td>CR</td>
<td>Computed Radiography</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma Separated Value</td>
</tr>
<tr>
<td>CREST</td>
<td>Council of Registered Ethical Security Testers</td>
</tr>
<tr>
<td>CT</td>
<td>Computerised Tomography</td>
</tr>
<tr>
<td>CTDI</td>
<td>Computed Tomography Dose index</td>
</tr>
<tr>
<td>DAP</td>
<td>Dose Area Product</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management System</td>
</tr>
<tr>
<td>DD</td>
<td>Digital Dictation</td>
</tr>
<tr>
<td>DICOM</td>
<td>Digital Imaging and Communications in Medicine</td>
</tr>
<tr>
<td>DLP</td>
<td>Dose Length Product</td>
</tr>
<tr>
<td>DMWL</td>
<td>DICOM Modality Worklist</td>
</tr>
<tr>
<td>DNA</td>
<td>Did Not Arrive / Attend</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Naming System</td>
</tr>
<tr>
<td>DR</td>
<td>Digital Radiography</td>
</tr>
<tr>
<td>DTI</td>
<td>Desk Top Integration</td>
</tr>
<tr>
<td>e-GIF</td>
<td>eGovernment Interoperability Framework</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Compatibility</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>GA</td>
<td>General Anaesthetic</td>
</tr>
<tr>
<td>GP</td>
<td>General Practitioner</td>
</tr>
<tr>
<td>HL7</td>
<td>Health Level 7</td>
</tr>
<tr>
<td>HRG4</td>
<td>Healthcare Resource Group</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IEE</td>
<td>Institute of Electrical Engineers</td>
</tr>
<tr>
<td>IGSoC</td>
<td>Information Governance Statement of Compliance</td>
</tr>
<tr>
<td>IHE</td>
<td>Integrating the Healthcare Enterprise</td>
</tr>
<tr>
<td>ISB</td>
<td>Information Standards Board</td>
</tr>
<tr>
<td>ISN</td>
<td>Information Standards Notification</td>
</tr>
<tr>
<td>LCD</td>
<td>Liquid Crystal Display</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MDD</td>
<td>Medical Devices Directive</td>
</tr>
<tr>
<td>MDGN</td>
<td>Medical and Dental Guidance Notes</td>
</tr>
<tr>
<td>MDR</td>
<td>Medical Devices Regulations</td>
</tr>
<tr>
<td>MDT</td>
<td>Multi Disciplinary Team</td>
</tr>
<tr>
<td>MHRA</td>
<td>Medicines and Healthcare Regulatory Agency – Competent Authority in the UK under the Medical Devices Directive</td>
</tr>
<tr>
<td>MIP</td>
<td>Maximum Intensity Projection</td>
</tr>
<tr>
<td>MOF</td>
<td>Meta Object Facility</td>
</tr>
<tr>
<td>MPPS</td>
<td>Modality Performed Procedure Step</td>
</tr>
<tr>
<td>MPR</td>
<td>Multi Planar Reconstruction</td>
</tr>
<tr>
<td>MR / MRI</td>
<td>Magnetic Resonance Imaging</td>
</tr>
<tr>
<td>NBSS</td>
<td>National Breast Screening Service</td>
</tr>
<tr>
<td>NICIP</td>
<td>National Interim Clinical Imaging Procedures</td>
</tr>
<tr>
<td>ODBC</td>
<td>Open Database Connectivity</td>
</tr>
<tr>
<td>OPG</td>
<td>Orthopantomograph</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PACS</td>
<td>Picture Archiving and Communications System</td>
</tr>
<tr>
<td>PAS</td>
<td>Patient Administration System</td>
</tr>
<tr>
<td>PBR</td>
<td>Payment By Results</td>
</tr>
<tr>
<td>PDS</td>
<td>Patient Demographics Service</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>PIR</td>
<td>Patient Information Reconciliation</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Change</td>
</tr>
<tr>
<td>RIS</td>
<td>Radiology Information System</td>
</tr>
<tr>
<td>RT</td>
<td>Radiotherapy</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SNOMED</td>
<td>Systematised Nomenclature of Medicine</td>
</tr>
<tr>
<td>SOP</td>
<td>Service Object Pair</td>
</tr>
<tr>
<td>TCE</td>
<td>Teaching File and Clinical Trial Export</td>
</tr>
<tr>
<td>TCI</td>
<td>To Come In</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptable Power Supply</td>
</tr>
<tr>
<td>US</td>
<td>Ultrasound</td>
</tr>
<tr>
<td>VDU</td>
<td>Visual Display Unit</td>
</tr>
<tr>
<td>VR</td>
<td>Voice Recognition</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WES</td>
<td>Warranted Environment Specification</td>
</tr>
<tr>
<td>XA</td>
<td>Modality code – X-Ray Angiography</td>
</tr>
<tr>
<td>XDS</td>
<td>Cross Enterprise Data Sharing</td>
</tr>
<tr>
<td>XDS-I</td>
<td>Cross Enterprise Document Sharing for Imaging</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>

**Terminology**

The following key words are to be interpreted as described in Internet Engineering Task Force RFC 2119.

- **MUST** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.
- **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behaviour described with this label.
Definitions

Services The Services SHALL include <to be defined by the trust>
1 Introduction

1.1 Background

This document collates a number of inputs including the Output Based Specification (OBS) used in the procurement of the Local Service Provider (LSP) contract. The update has included input from more recent procurements, from the Royal College of Radiologists and with the needs of the NHS today and lessons learned from the LSP contract experience.

The document is not meant to be “perfect” as trust engagement sessions that have taken place during its creation have clearly shown that one size does not fit all and that in some areas there is no consensus. It is therefore a set of core requirements which is intended to be used by NHS trusts to assist them in producing their own OBS for procuring PACS, RIS, CR/DR and integration services. The document can be used by trusts procuring individually or using a collaborative procurement approach, for example a consortium OJEU, or a centrally provided framework.

This set of core requirements is not guaranteed to be exhaustive. It is also recognised that many of the requirements may not be needed by all trusts or may benefit from tailoring locally.

The document, in places, refers to and includes “Standards”. Consideration should be given in a procurement process to the mandating of “Standards” where applicable. It is advised that all procurement activity be standards and requirements based and these are tailored to the needs of the local organisation or set of organisations.

1.2 Purpose

This document serves the following purpose:

To combine a set of requirements that is known to support the NHS today once, so that this exercise does not have to be repeated by every trust;

To drive a requirements and standards based re-procurement;

To gain broad NHS input and as a result develop a shared view of good practice.

1.3 Commercial context

PACS and RIS Services are presently provided to 75% (128) of NHS acute trusts by Local Service Providers under contract to the Department of Health. These contracts expire in June 2013 in all regions except London (21 trusts). A one year extension is available that could extend this date to June 2014. Additionally 2 years transition assistance is available that can be taken in parallel or sequence to the one year extension.

The situation in London is that contract Change Control Note (CCN2) in 2006 formally extended the contract so that it expires in June 2014 and agreed that 13 months of the transition assistance would run subsequent to this. The London contract currently has a defined end date of July 2015 with the option of an additional 11 months of transition assistance.

This document is one of the tools that will be provided by the national team to assist trusts to re-procure PACS and RIS Services in the available time window. However, it is also available to non LSP trusts who wish to use it.
1.4 Requirement scope

This document aims to cover the requirement areas highlighted within the diagram (Figure 1) below. The diagram also references other areas for integration where necessary.

Figure 1
2 Core principles

2.1 Background

All trusts in England have a functioning PACS and RIS system that is in most cases highly integrated, enterprise wide, and connected to external archives and data sharing tools.

These systems have been generally delivered to a high standard and run 24/7, 365 days a year with over 99% availability and limited Service issues. They also have a very good track record in the area of maintaining patient safety. This does not mean the present situation cannot be improved, and the re-procurement hopes to drive improvements, or that it is what an individual trust requires going forward. It is however, a high baseline and trusts need to take this into account when making their decisions Suppliers also need to understand this is the existing baseline and they are not dealing with a "greenfield" site.

As well as the detailed requirements this document also, includes some core principles based on NHS feedback and lessons learned. As with all the requirements these are included here but can be tailored by trusts in their own procurement exercises.

2.2 Scope

The supplier should be aware that the overall solution needs to support the following and they will need to demonstrate how this will be achieved with evidence of previous success:

The ability to support a 365 day per year 24/7 critical clinical Service in an organisation of the type of the English NHS;

To support users outside of radiology across the clinical enterprise including Primary Care;

To integrate non radiology images as well as radiology images and non radiology reporting;

To support the sharing of images, reports with those images and ideally worklists across a health care community (which will involve a number of legal entities and may include primary care and the independent sector) either on their own or by permitting and supporting integration to other third party systems;

To support cross organisational working, specifically multidisciplinary team (MDT) working, such as clinical networks for trauma, cancer or stroke. Shows a willingness to work with organisations as they look to improve and reconcile Services in the future;

To support integration and interoperability with legacy systems; PACS and RIS are core critical systems in an acute trust environment. The supplier MUST demonstrate how disaster recovery and business continuity will be supported; and

The Service MUST be upgradeable and expandable to continue to meet the future requirements and to make best use of technological improvements/refresh and cost reductions.

2.3 Technology

Experience to date demonstrates that the most effective product is a „Commercial off the Shelf“ (COTS) product with a clear development path. This particularly applies to PACS. Attempts to change the standard market available PACS products under the LSP contracts have proved difficult and costly and although there have been some notable successes a lesson to learn is that these products are often global standard products and local bespoke developments can be fraught with issues.
Trusts will have existing IT assets which is some cases will have a remaining life. A trust will need to decide if they wish to change or keep these assets and suppliers may need to take into account the trusts existing asset base.

Trusts will have a significant volume of existing clinical data that will need to be either decommissioned in line with the Data Protection Act 1998 or most likely transferred to the new arrangements. Trusts and suppliers will need to take this into account.

Suppliers will be required to meet the relevant principles of the NHS Information Strategy, NHS Technology Strategy and comply with NHS Information Standards as published by the ISB.

2.4 Patient safety

Suppliers MUST demonstrate that they are able to maintain patient data safely in accordance with ISB 0129 Patient Safety Risk Management System - Manufacture of Health Software.

The Services and procedures supporting the design, development and deployment of the Service provided MUST adhere to ISB0129 and the timescales associated with ISB0129.

Where the supplier hosts the Service, the Service MUST be compliant, with the standards and guidance for Clinical Safety as covered in the ISB0160.

Where elements of the Service are deployed into trust infrastructure, the supplier MUST assist the trust to carry out tests that provide the necessary assurance that the system is clinically safe to deploy in a live patient environment. Refer to ISB0129.

2.5 Interoperability and connectivity

The Government’s direction of travel with regards to informatics is that healthcare IT systems should “connect all” as opposed to requiring an unnecessary “replace all” strategy. Suppliers will need to demonstrate the tools and behaviours that will allow trusts to connect up their PACS and RIS systems to other systems as required. If the supplier has restrictions upon this or there are consequences on Service levels or processes to follow in order to achieve connectivity and interoperability, these should be stated at the time of procurement.

Information Governance: Suppliers MUST be able to demonstrate that their systems will operate in a way that ensures the trust can meet the requirements of the Care Record Guarantee and the requirements of the NIGB Guidance for Patients, Healthcare Professionals, Access to Health Records by Diagnostic Staff and Information Governance Standards Baseline

The Care Record Guarantee can be found at http://www.nigb.nhs.uk/guarantee.

The NIGB Guidance can be found at http://www.nigb.nhs.uk/pubs/guidance/diagtestguidance

The Information Governance Standards Baseline can be found at: http://www.isb.nhs.uk/use/baselines/ig

2.6 Assured products

It is anticipated that within the time window of these new contracts, any system needing to use national infrastructure such as N3 will need to have demonstrated a level of capability and be an “assured” product. The National Integration Centre and Assurance (NICA) division of the CFH Technology Office currently expect that future assurance will concentrate on
protection of National Application Service Provider (NASP) Services such as Spine Security Broker, Personal Demographics Service, other NHS Spine Services and Choose and Book.

The assurance process has not yet been defined but is likely to be based on the Common Assurance Process (CAP) already in use for assuring non-LSP systems connecting to NASP Services and that it will be based on a risk management approach.

Trusts will also need to be provided with the ability to test and train on new systems, including testing of integration with other trust systems. The level of this requirement will differ between trusts and needs to be expanded at the point of procurement. Trusts MUST have access to a test environment which can be configured to behave as their live environment and can be integrated to other test environments as needed. This access will be needed throughout the life of the system.

The NICA and wider Technology Office team will retain considerable expertise in the area of standards for interoperability, integration and Clinical Safety, as well as in software testing and quality assurance. This is in addition to their knowledge of the PACS and RIS systems currently used in the LSP estate, and industry contacts built up over the last seven years.

If a suitable model can be agreed, this knowledge and expertise can be made available to NHS trusts.

Typical activities where the NICA and Technology office teams could contribute and add value:

Technical and design review of migration strategies, infrastructure design for new Services;
Arbitrating between suppliers who are in dispute over specific integration problems;
Suggest investigations and resolutions to overcome particular blockers in PACS/RIS implementations or migrations;
Assisting the trust to manage testing or helping to write structured regression and commissioning test plans, test scenarios and test scripts; and
Help escalate clinical safety concerns if trusts believe they are not getting appropriate response from manufacturers / vendors.

2.7 Variation and Choice

Trusts may wish to select different suppliers for different Services and for example, purchase peripheral items such as workstations off the open market and integrate with their PACS and RIS systems. The supplier will need to state their approach to this at the point of procurement and highlight any implications and consequences should a trust choose to take this approach.

Trusts using the core requirements within this document will need to define the scope of the services being procured. The term Services throughout this document can then be interpreted as defined:

**Services** - The Services SHALL include <to be defined by the trust>

2.8 Pricing

Trusts currently have largely revenue budgets for PACS and RIS and may find it difficult to raise significant capital in the change time window. Suppliers should consider pricing options, for example on a utility based model and be able to offer trusts flexibility in the payment model to fit in with the trust financial needs.
3 Functional requirements

This section sets out the functional requirements needed to perform the Service.

<If the trust requires an image archive service and/or an enterprise sharing service, the requirements in Sections 9.1, 9.2 and 10.1 MUST also be included>

Suppliers should describe how they will meet each of the requirements below:

3.1 General imaging requirements

3.1.1 Any demographics update or patient merges on the Patient Administration System (PAS) or the Master Patient Index (MPI) for the trust MUST update the Service in „real time“.

3.1.2 The Service MUST comply with ISB 1505, Common User Interface - Patient Banner.

3.1.3 As a minimum, the Service MUST be capable of storing the following patient information associated with each study/examination: NHS number (preferably verified), family name, first name, previous name(s) where applicable, hospital number(s), Date of Birth (DOB), Date of Death, address, accession number or specialty information solution (e.g. PACS/CIS) examination number, date and time of examination, modality, body part (laterality if applicable), referring clinician, reporting clinician, supervising specialist clinical user, patient status (e.g. GP, inpatient, outpatient) and patient alert information.

3.1.4 The verification status of the NHS number SHOULD be stored and displayed.

3.1.5 On-call radiologists MUST be able to report remotely. Suppliers MUST describe how they will meet the following requirements:

- Secure and appropriate remote access to any image / report from any legitimate location (including home) at diagnostic quality: access will be controlled by trust administration;
- A method of loading images which is effective even over slow network connections;
- Consistent high image quality; and
- Access to other information: request cards, scanned documents, clinic letters, electronic request information and reports.

3.1.6 Suppliers SHOULD demonstrate how a 3 click reporting workflow can be achieved for the following:

- Generating a RIS worklist for reporting;
- Launching a patient”s exam for reporting on RIS (e.g. automatic display of images on PACS with automatic display of relevant prior, dictate/VR report on RIS); and
- Click on the next exam on the RIS worklist which closes the previous PACS images & launches the next patient on RIS & PACS.

3.1.7 The Service MUST support paper-light / film-less operation. The supplier MUST describe how the Service supports the diagnostic process workflow from examination request through to image and report distribution without the use of paper documents. For example, the examination request, management of image acquisition workflow e.g. vetting,
capture of justification, queue management, historic exams, creation of the diagnostic report, and distribution of a report.

3.1.8 The Service MUST display the clinical indications / reason for request of an exam, both to support justification of requests and reporting of exams.

3.1.9 The Service SHOULD be configurable:

- Service configurations SHOULD be capable of being associated with a particular user or group of users;
- Configurations SHOULD be capable of being copied;
- Configurations SHOULD be held centrally and be capable of being “picked up” on any workstation (i.e. the Service SHOULD facilitate a “roaming profile”);
- The supplier SHOULD describe how the “roaming profile/configuration” is cached on a device for performance and resilience purposes. The supplier SHOULD describe how this information is secured;
- The supplier SHOULD describe how the Service limits the number of users;
- The Service SHOULD NOT allow concurrent logins for each profile; and
- The idle log-off time SHOULD be configurable by trust system administrator on a per workstation basis, for individual users or groups of users.

3.1.10 The supplier SHOULD describe their approach to enabling “session persistence” (i.e. allowing the user to move between workstations whilst keeping the users session intact between workstations or on the same workstation over time) within their Service and how this can be integrated within an access control framework.

3.1.11 The supplier MUST state how exam status is synchronised between Order Comms, RIS, PACS and Results Reporting Systems:

- Requested;
- Request justified;
- Request held/deferred with reason;
- Scheduled or appointment given;
- Cancelled with reason;
- Arrived/attended;
- Did not attend;
- Exam started;
- Exam completed;
- Exam not performed, with reason;
- Report dictated;
- Unauthorised report;
- Authorised/verified report;
- Amended report;
Report viewed;

Report acknowledged; Review requested; and

Waiting status.

3.1.12 If the supplier is providing workstations, servers and other hardware, they SHOULD describe any restrictions to or consequences of use of alternatives by the trust over the contract period. The supplier SHOULD consider not restricting hardware and instead SHOULD provide a minimum specification so that trusts have the option to purchase these items from other suppliers. Suppliers MUST state their position on this.

3.1.13 The supplier MUST be capable of supporting the National Interim Clinical Imaging Procedure Codes (NICIP) and show how they can be kept up to date in compliance with DSCN27/2009. The supplier SHOULD also provide a roadmap to support replacement of NICIP with SNOMED CT® (SNOMED CT) by 2015.

3.1.14 When displaying numerical values, the Service MUST present the unit of measure being used alongside.

3.1.15 The Service SHOULD be capable of being integrated with the trust directory service to provide single sign on functionality for users logged in individually to trust’s servers and workstations.

3.1.16 In response to the General Imaging Requirements the supplier MUST describe how the Service complies with the following standards:

- ISB 1503, Common User Interface – Date Display;
- ISB 1504, Common User Interface – NHS Number Input and Display;
- ISB 1505, Common User Interface – Patient Banner;
- ISB 1506, Patient Name Input and Display;
- ISB 1507, Sex and Current Gender Input and Display;
- ISB 1508, Telephone Number Input and Display;
- ISB 1501, Time Display; and
- ISB 0149-02, NHS Number for Secondary Care.

3.1.17 In response to the General Imaging Requirements the supplier MUST describe how the Service complies, or will achieve compliance over time, with the relevant elements of the following:

- IHE, Patient Information Reconciliation (PIR);
- IHE, Post-processing Workflow(PWF);
- IHE, Reporting Workflow (RWF);
- IHE, Scheduled Workflow - Modalities (as acquisition modality actor), RIS (as departmental system scheduler actor) and PACS (as Image Manager & Image display) MUST all support scheduled workflow (SWF);
- IHE, Radiation Exposure Monitoring (REM); and
3.2 Interoperability and interfacing

3.2.1 The supplier MUST confirm DICOM and HL7 interoperability between the connecting systems, and identify any issues preventing full integration. A reference to specific standards and details of any proprietary software SHOULD be provided. The supplier MUST ensure that all contracted imaging-related elements supplied are interoperable and integrated into the overall solution as part of the implementation process.

The interfaces to the trust’s RIS MUST allow passage of referral/request information from the RIS to the PACS such that authorised users have access to it via the PACS workstations and modality workstations. For each examination, users MUST be able to determine patient demographics, referring clinician, type of examination, reasons for the examination and date of request.

3.2.2 The DMWL SHOULD allow transfer of demographic information between RIS and modalities.

3.2.3 Subject to appropriate information governance controls, the Service MUST provide a shared workflow across all connected trust domains. This SHALL NOT be interpreted as requiring a specific architecture, rather it requires that the user be able to find and access any examination known to the Service without knowing details of the architecture. This requirement SHALL NOT be interpreted as precluding location-specific default views of the information.

3.2.4 The Service could be extended to all other non-radiological forms of imaging as required by the trust. The design of the Service MUST allow for such developments during the expected life of the Service, which MUST be stated by the supplier. The supplier MUST list which additional forms of imaging / file types are currently supported. The supplier MUST provide a framework for how requesters outside of Radiology will be accommodated. Suppliers are invited to give an indication of their experience to date in this area e.g. list of image types incorporated, devices interfaced to etc.

3.2.5 The supplier MUST state by architecture component (workstation, servers, etc.) what versions of third party software have already been ratified for use alongside the Service e.g. Microsoft Office, antivirus software, Java runtime components and versions. The supplier MUST support impact assessment and ratification of additional third party software as identified by the trust and provide a compatibility roadmap document, including forward and backward compatibility by software type, version and date of anticipated support deprecation. The list of third party software will be trust specific and SHOULD be stated wherever possible by the trust at the point of procurement.

3.2.6 Where the supplier does not wholly own or control its product, the supplier MUST identify any third party dependencies in hardware / software / licenses.

3.2.7 All functions permitted to the user of the Service MUST be available (including Voice Recognition (VR)) through a single workstation with desktop integration. The supplier MUST list VR products and versions compatible with the Service. Suppliers SHOULD describe their approach to VR and whether the workflow will be PACS or RIS driven.

3.2.8 The interfaces MUST be able to operate both in real time and batch mode. Interface requirements will be specific to trusts and SHOULD be listed at the time of procurement.

3.2.9 The supplier MUST provide for interfaces to all existing modalities at each site. The supplier will be provided with a locally generated list of modalities in use and MUST undertake a review of these modalities as part of its due diligence report. The supplier MUST
provide a table of all existing modalities and show how these can be connected to the Service and the related cost. In the absence of suitable DICOM operability within certain study acquisition equipment, Service providers MUST provide DICOM gateways or suitable methods of study transmission to the Service.

3.2.10 This document recognises the importance of automating as far as possible all communication between the Service, other computer systems and modalities. Therefore, in addition to DICOM functionality required to produce a solution which MUST function at a basic level (query retrieve, store, print etc), it is expected that the widest ranging and earliest implementation of features such as Modality Performed Procedure Step and Storage Commit functionality MUST be provided. Details MUST be supplied of precisely which DICOM features it is proposed to implement in the interface to each of the modalities and systems with which it SHALL communicate (it is recognised that in many cases the modality, rather than PACS SHALL determine this). For Modality Performed Procedure Step, suppliers SHOULD describe how information about the exam (for example, radiation dose, and number of images) can be automatically recorded in the Service.

3.2.11 The supplier MUST provide DICOM conformance statements covering all DICOM functions of the proposed Service. On request, the supplier MUST provide conformance testing results that validate DICOM conformance statements without charge.

3.2.12 The supplier MUST provide:

- a full data dictionary of all public and private DICOM attributes used or created by the Service, to include value representation and valid values; and
- a full description of DICOM SOP classes.

3.2.13 The supplier MUST state which versions of HL7 are supported for communicating with other clinical systems and provide their HL7 integration specification for their standard interfaces, such as Order Communications, results reporting, applicable to both PACS and RIS.

3.2.14 The supplier SHOULD support bidirectional integration between RIS, PACS and trust remote electronic ordering (Order Comms / Electronic Patient Record system) and results reporting to encompass status updates, reflex ordering, request rejection & cancellation.

3.2.15 DICOM Modality Worklist (DMWL) MUST be provided for all modalities. With existing non-DICOM equipment, the supplier MUST provide a solution. Suppliers MUST state their solution to the provision of DICOM worklist functionality for existing non-DICOM equipment.

3.2.16 The Service MUST allow processing/vetting of order requests including clinical indications for the requested examination, both electronically and by manual input from paper requests and display the details on acquisition worklists and specialist clinical user’s reporting worklists.

3.2.17 Where the trust provides breast screening services, the Service MUST meet the PACS requirements as specified by the NHS Breast Screening Programme (NHS BSP). The NHS BSP website can be found at http://www.cancerscreening.nhs.uk/breastscreen/

3.2.18 Where required, the supplier SHOULD support DMWL integration to the National Breast Screening System (NBSS) fixed and mobile screening units, including an electronic link to transfer studies acquired on the mobile unit back to the Service.
3.2.19 Suppliers SHOULD make available to the trust the necessary API elements of the Service required by the trust to facilitate launch and context control of the Service from within trust software. APIs/Interface specification SHOULD be open and published.

3.2.20 The Service MUST support desktop integration and context synchronisation between PACS and RIS. Suppliers SHOULD describe the options available for achieving this requirement.

3.2.21 The Service SHOULD support single sign-on. Additional user name and password submission SHOULD NOT be required when using RIS and PACS. When a user logs into the RIS for reporting the user credentials SHOULD be passed onto PACS with no need for additional user name and password input (and vice versa). Suppliers SHOULD describe the options available for achieving this requirement.

3.2.22 The Service MUST describe any APIs available for single sign-on/DTI.

3.2.23 Where trusts have or are implementing a single sign-on system, suppliers SHOULD provide integration where specified.

3.2.24 The supplier MUST describe how Desk Top Integration (DTI) can be achieved with other information systems.

3.2.25 The supplier MUST describe their approach to interfacing multiple sources of demographic information, such as multiple PASs and NBSS, within the Service; an explanation MUST also be provided as to how data quality is maintained with minimal user intervention when there are inconsistencies between these systems.

3.2.26 The supplier MUST describe the functionality of systems provided by third parties required for the correct functioning of the Service they provide (e.g. messaging).

3.2.27 The supplier MUST demonstrate connectivity or the potential to connect with the national and regional data sharing tools of choice, Accenture’s PACS Connect and the Image Exchange Portal. This MUST include detail of DICOM and HL7 integration and any available APIs/Interface specifications which enable remote access. APIs/Interface specifications SHOULD be open and published.

3.2.28 The supplier SHOULD demonstrate appropriate connectivity to other systems such as GP systems and portals to support patient access to their data.

3.2.29 The supplier MUST demonstrate its capability or roadmap towards an XDS-I compliant product and how it would provide interoperability by utilising this architecture. The supplier SHOULD describe the existing capability and any experience in this area, highlighting which part of a complete sharing system it can provide. It is acknowledged there are alternatives to XDS-I and suppliers must notify trusts if their Service provides any alternative.

3.2.30 The supplier SHOULD demonstrate its understanding of the interoperability challenge across an NHS healthcare community and demonstrate how it supports this. This SHOULD include as a minimum:

A description of how it would support multi-organisation, multidisciplinary team meetings;
Shared reporting via reporting centres; Shared workflow and a workforce shared across multiple organisations; and
Support of regional clinical networks, such as cancer and stroke networks.
3.2.31 In response to the Interoperability and Interfacing requirements the supplier MUST describe how the Service complies, or will achieve compliance over time, with the relevant elements of the following:

- IHE, Scheduled workflow (SWF);
- IHE, Patient information reconciliation (PIR);
- IHE, Post-processing workflow (PWF);
- IHE, Reporting workflow (RWF);
- IHE, Charge posting (CHG);
- IHE, Presentation of grouped procedures (PGP);
- IHE, Evidence documents (ED);
- IHE, Simple image and numeric reports (SNR);
- IHE, Portable data for imaging (PDI);
- IHE, Cross-enterprise Document sharing (XDS) and Cross-enterprise Document sharing for Image data (XDS-I);
- IHE, Access to radiology information (ARI); and
- ISB 0149-02, NHS Number for Secondary Care.

3.3 Storage requirements

3.3.1 The storage Service MUST provide short term and/or long term storage, where short term storage provides fast data retrieval <to be determined by trust> and long-term storage provides archiving and/or back-up of data.

3.3.2 The storage Service MUST support data sharing that may be delivered nationally, regionally and/or locally; whose content is federated, such that images and reports can be viewed and shared by any authorised person within the patient care pathway. Federated means that although content such as images and reports can be stored and managed in different systems those systems and their authorised users can both search and retrieve data across any system. The Supplier MUST describe how sharing will be achieved.

3.3.3 The short term storage Service MUST be “agnostic” of the storage hardware to allow trusts to change or add storage hardware as necessary.

3.3.4 The storage Service MUST deliver a cost effective Service utilising trust data retention policy to balance the appropriate Service levels against the total lifetime cost of storage of the data.

3.3.5 The storage Service MUST allow the trust to change local applications (e.g. PACS) with no loss of access to historic data and in a way that ensures trusts can limit parallel running and transition to no more than <4 weeks suggested but trusts to determine> . This MUST include the ability to migrate data to or from the storage Service to alternative data stores.

3.3.6 The design, architecture and implementation of the storage Service MUST be based on appropriate open standards, which are published and available both to the trust and trust approved third parties needing to interact with the storage Service. The Supplier MUST provide details of standards used.
3.3.7 DICOM data MUST be stored as received, as specified in part 10 of the DICOM standard.

3.3.8 DICOM standard transfer syntax MUST be used.

3.3.9 All database schemas and structures SHOULD be open, accessible and documented and made available to the trust when requested, for example to support data migration and system integration.

3.3.10 The storage Service SHOULD require minimum proprietary software or standards in order to operate and maintain the Services provided.

3.3.11 Suppliers SHOULD describe their approach to utilising a trust's existing Storage Area Networks or other enterprise storage. <trust SHOULD specify enterprise storage (make, model and interfaces) with which the Service would be required to integrate >

3.3.12 The storage Service MUST allow data to be stored in a way that supports the Greening Government ICT Strategy, ensuring that the data can be kept long-term in a sustainable and efficient way. The Strategy can be found at http://www.cabinetoffice.gov.uk/sites/default/files/resources/greening-government.pdf

3.3.13 The Service MUST be able to store studies other than radiological images e.g. DICOM structured reports, PDFs, photographs, scanned images and video images.

3.3.14 The supplier MUST provide details of the method for calculations undertaken in sizing the archive. The supplier MUST describe their approach to provisions for archive growth and scalability. Trusts SHALL provide historical usage data in order to enable suppliers to meet this requirement (for example, KH12 or usage reports from existing PACS).

3.3.15 The supplier MUST provide a list of third party archives which they have previously, successfully integrated with, including the interfaces provided with and required by the Service to facilitate successful integration.

3.3.16 Where trusts have stated they require an interoperable image sharing solution with other trusts, storage MUST be configured such that access to images created and viewed in trust 1 are available within <trust configurable time> and archived images from trust 2 can be retrieved to trust 1 in a <trust configurable time> time without manual intervention. Suppliers MUST describe how they will measure and report on the impact of the image sharing solution on the network.

3.3.17 Retrieval is required for all images to predetermined locations and workstations at specified times i.e. images MUST be available when and where required. Precise timescale definitions MUST be mutually agreed between the trust and the supplier.

3.3.18 The supplier MUST ensure no loss or corruption of images and guarantee that there SHALL be no distortion or degradation of the data as a result of the storage, retrieval and transmission process, unless specifically intended by administrators, specifying lossy compression for that exam or group to which that exam belongs.

3.3.19 The Service MUST allow studies to be stored using various levels of compression, both lossless, and lossy. The choice of whether to use lossy compression and what degree of compression MUST be under the control of authorised users and SHALL be configurable by type of examination (modality and body part) and date that the study was acquired and last accessed. These rules SHOULD be configurable based on the contents of any DICOM tag. Details of the compression algorithms and validation of claims for lossless compression MUST be provided. Suppliers MUST describe how users are alerted to the fact that lossy...
compression has been used, and whether or not they support the use of the lossy compression DICOM tag (0028,2110) in images transferred onto other DICOM destinations.

3.3.20 The Service MUST have the facility to Query Retrieve and store any studies stored in modality or other legacy databases. The supplier MUST state how it will make available for viewing and subsequent archiving images stored in legacy databases, including the management of private tags and proprietary metadata. Suppliers MUST provide details of the method and examples. The supplier SHOULD state which tools are available for lifecycle management of archived data and the level of user configurability.

3.3.21 The supplier MUST demonstrate how the storage Service can comply with the Records Management NHS Code of Practice Part 2 (2nd Edition, January 2009) and the RCR Retention and Storage of Images and Radiological Patient Data, BFCR(06) 4. The supplier MUST demonstrate how they can provide hierarchical data management and deletion according to trust policies as required.

3.3.22 The Service MUST be capable of receiving demographic feeds from PAS or RIS to keep the demographics relating to all the data stored up to date. Suppliers MUST describe how patient merges and image rejections/deletions on the main PACS will be synchronised to the long term storage. Suppliers must describe the mechanisms available for merging and unmerging of records on RIS & PACS.

3.4 Network requirements

3.4.1 Where the N3 or networks are used, the supplier MUST describe via their technical design documentation how:

- They will comply with any registration requirements;
- The various traffic classes can be identified whilst in transit over N3 or other networks, so that they can be marked for QoS purposes to minimise network contention;
- They will report on traffic broken down by type to allow validation of the correct marking of the traffic (e.g. reported on by source and destination IP address); and
- They will not preclude the possibility that groups of trusts sharing the Service may want to utilise private WAN and/or VPNs Internet as the network Service.

3.4.2 The supplier MUST ensure that it delivers the performance requirements stipulated. Network usage MUST be capable of being constrained such that it can meet service levels whilst remaining within WES requirements.

3.4.3 The supplier MUST state preferred and minimum/maximum network requirements for acceptable performance. Requirements MUST include bandwidth, latency, packet loss and jitter.

3.4.4 The supplier MUST provide a networking specification within their Warranted Environment Specification (WES) and agree with trusts the impact of changes on the WES.

3.4.5 Where the current network is not capable of delivering the performance and availability standards required (as documented in the WES), the supplier MUST propose necessary upgrades and evidence of why upgrades are deemed necessary, to the trust.

3.4.6 The supplier MUST check that the trust networks and connections are satisfactory to deliver optimum performance. The supplier MUST state (via a WES audit, compliance check or similar) if any changes are needed to trust networks.
3.4.7 The supplier MUST identify the network Services which the Service requires and check that those network Services are provided (e.g. time Services, DNS, AD, LDAP, intrusion detection, AV and monitoring).

3.5 Commercial off the shelf (COTS) products

3.5.1 Products offered SHOULD be based on Open Source solutions where applicable, in line with the Government ICT Strategy (ref: http://www.cabinetoffice.gov.uk/resource-library/uk-government-ict-strategy-resources).

3.5.2 Where applicable and where future functionality is proposed to meet these requirements it SHOULD be clear that the product is in a future plan and a product roadmap SHOULD be made available to the trust.

3.5.3 Where a future development is necessary to support these requirements, delivery of that development path SHOULD be clearly defined in the contractual agreement.

3.5.4 For all COTS operating systems and proprietary or tailored software (e.g. modified Open Source) used in providing the Service, the supplier MUST maintain in a timely manner <to be agreed with trust> the application of software patches, bug fixes and new Service pack updates, which MUST be included an agreed maintenance schedule.

3.5.5 The supplier is responsible for the licensing of all COTS products used in providing the Service, unless otherwise agreed with the trust. The supplier MUST specify where a trust is responsible for any license procurement.

3.6 Functional requirements - PACS

3.6.1 The Service MUST support the use of common search criteria for a single or group of patients using one or any combination of the following:

- Name;
- Date of Birth (including date ranges);
- Date of Death;
- Sex;
- NHS Number (preferably verified);
- PAS or Hospital Number;
- Current Responsible Consultant;
- Requesting Responsible Consultant;
- Current Patient Location;
- Exam Status of study;
- Modality;
- Exam Description;
- Exam Room;
- Date Range (for exams);
- A sounds like / Soundex function for patient name searching; and
- Urgency flag.
3.6.2 The Service MUST support information that needs to be stored for the clinical user/radiologist viewing the PACS image (also identified as metadata fields or tags):

- Patient demographics;
- Name;
- Date of Birth;
- Date of Death;
- Sex;
- PAS / Hospital Number;
- NHS Number (preferably verified);
- Current patient location;
- Current responsible consultant;
- Requester (synchronized with RIS);
- Name of requester;
- Requesting responsible consultant/GP (team and also recipient);
- Requesting specialty/department/GP surgery;
- Requesting institution;
- Date & time of request made;
- Date & time request received in radiology system/department;
- Image document (synchronized with RIS and modalities);
- Modality;
- Exam description (national exam codes and descriptions);
- Exam status;
- Date and time image acquired on modality;
- Date and time of image sent from modality;
- Date and time received on PACS;
- Exam room (where the exam has been performed);
- Operator/image creator (synchronized with RIS and modality);
- Name of operator;
- Performing responsible consultant;
- Performing department/specialty (e.g. radiology);
- Performing institution/NHS trust;
- Reporter (synchronized with RIS);
- Name of reporter;
3.6.3 The Service SHOULD support integration with multiple specialty information solutions (e.g. RIS, CIS, NBSS) or the equivalent, held within a typical trust. Suppliers SHOULD detail how the Service behaviour with respect to managing multiple demographic and order feeds, notably the issues of multiple exam numbers, location codes, referral codes and patient IDs.

3.6.4 Suppliers MUST describe how they may integrate and support third party PACS plug-in products (e.g. Orthopaedic templating, 3D volume rendering) chosen by the trust and detail the level of integration achievable between these third party plug-ins and the Service in terms of (but not limited to) functionality, performance and scalability. The supplier SHOULD declare how they intend to support the DICOM Application Hosting API, or supplement 118. Any APIs/interfaces SHOULD be open and published.

3.6.5 Suppliers MUST describe the advanced visualisation and analysis tools available, such as: 3D volume rendering, dataset registration and fusion, automated image segmentation (e.g. bone removal), virtual colonoscopy, vessel tracking, cardiac analysis packages, CAD packages.

3.6.6 User roles MUST be configurable locally within PACS by trust staff with the appropriate administration privileges.

3.6.7 The „enterprise client / web browser“ Service MUST provide an intuitive user interface and functionality sufficient to review and or annotate images and reports (and the ability to add notes) for the purpose of clinical decision-making by requesting clinicians, the Service MUST enable:

- Display of grayscale and colour images from any modality;
- Visual navigation of the available series of images through the use of thumbnails;
- Side-by-side comparison of at least two sets of images (with synchronized scroll, pan and zoom for cross-sectional modalities);
- Annotation of laterality, orientation, and spatial localization;
- Annotation of demographics, management and basic technique information;
- Simple measurements of linear distance and angle;
- Ciné capability for images that involve motion (e.g. cardiac US, XA, CT or MR);
- View report only;
- Hide/turn off annotations; and
- Diagnostic web-compression, which MUST be configurable by the user, (subject to relevant permissions).

3.6.8 The „enterprise client / web browser“ Service SHOULD be capable of providing diagnostic quality imaging suitable for reporting from non dedicated PACS hardware.

3.6.9 Suppliers MUST describe how they would achieve an “enterprise client / web browser” deployment of the Service outside of the trust, with particular regard to:

- Deployment to primary care;
- Deployment to external healthcare facilities and outreach clinics with limited network bandwidth;
- Deployment to mobile workers in the community (e.g. community midwives, on call physicians); and
- Support for thin client / virtual desktops.

3.6.10 Regarding PACS cross sectional imaging display requirements:

- PACS MUST create and display on demand MPR/MIP image data from thin cross sectional MUST allow for synchronised scrolling in three planes;
- MUST automatically display of relevant prior exams, in accordance with system admin or user definable hanging protocols;
- MUST be able to synchronise scrolling with prior scan;
- MUST have the ability to create surface and volume rendered 3D images;
- MUST have the ability to define Regions of Interest (ROI). ROI information SHOULD be exportable and suppliers MUST explain how their product enables ROI information to be conveyed to other PACS instances, via DICOM or other means;
- During MPR/MIP/3D viewing, users MUST have the ability to save key images (a coronal / sagittal / axial image that shows the key lesion) as a separate series for reference to the report. Key images SHOULD be exportable and suppliers MUST explain how their product enables key image information to be conveyed to other PACS instances, via DICOM or other means;
- Users MUST have the ability to define slice thickness and create images of different thickness in real-time;
- MUST have the ability to measure distance, circumference, angle, and volume of lesions;
- MUST have the ability to measure pixel values (including Hounsfield Units) for example the mean, median and maximum and standard deviation of a lung nodule; and
- Ciné display MUST be present.

3.6.11 Authorised users MUST be able to create teaching folders with shared permissions via diagnostic workstations and web / enterprise clients. The Service MUST force users where relevant to remove all PID demographic headers and all annotation for the purposes of teaching, research and publishing. The Service MUST support the creation of multiple folders to support trust activity including (but not limited to):
PACS, RIS, image archive and sharing services. Core statement of requirements.

- MDT meetings;
- Audit;
- Research;
- Teaching;
- Quality Assurance;
- Conferencing; and
- Personal folders.

3.6.12 The Service MUST have the ability to DICOM push to other hospitals even when working remotely (for example, neurosurgical and cancer centres and other off site Multidisciplinary Teams).

3.6.13 The supplier MUST describe the Service”s capability to create DICOM PS3.10 compliant exchange media (CD, DVD, USB) including:

- Creation from standard workstation; Options to create on a robotic media creation system; and
- Ability to encrypt the data inline with current cryptographic standards.

3.6.14 The Service MUST allow for the exporting of suitably de-identified images as DICOM as well as a variety of other formats such as JPEG and AVI. Where images are exported as DICOM, viewing software should be included. The Service SHOULD allow for the images to be de-identified with specific new identity information to support export for trials. The Service MUST allow removal of private tags at the discretion of the user, and MUST warn of images that may still contain PID.

3.6.15 The Service MUST accommodate Multidisciplinary Team (MDT) meetings where high quality image viewing facilities are required along with the facility to project images on to a screen. The imaging studies used at these meetings may be sourced from a number of organisational entities with different PACS systems. The MDTs themselves may also involve a number of organisational entities. The supplier MUST demonstrate how they will deal with a complex MDT environment involving multiple organisations, multiple clinical specialties and information sourced from multiple PACS and information systems.

3.6.16 The Service MUST support interface of PACS to teleconferencing and videoconferencing systems to support “real time” synchronised review of imaging across multiple organisations, including support for Multidisciplinary Team Meetings.

3.6.17 The Service MUST provide the facility to schedule study images and reports for review at Multidisciplinary Team Meetings. The Service MUST provide each meeting with a worklist to enable prior review of imaging studies and reports at all participant organisations, and to serve as a permanent record of the studies reviewed at each meeting.

3.6.18 It MUST be possible to connect the workstations to data projectors providing functions such as dual projector and split screen projection. The minimum standard resolution is 1024 x 768 pixels. PACS workstations SHOULD be capable of using either analogue (VGA based) or digital (DVI based) connections to projectors.

3.6.19 The Service SHOULD support the viewing of several examinations which may be from more than one modality or be separated by time into one study and report.
3.6.20 The Service MUST alert the referring clinician to updates in the status of examinations they have previously requested, including the availability of reports. This alert MUST be configurable with the ability to turn off if required.

3.6.21 The Service SHOULD obtain Date of Death information from the PAS. The Service SHOULD be configurable so that all images related to the patient can be automatically deleted or archived from the repository at a point after death determined by the trust.

3.6.22 The Service SHOULD allow customisation such that it will be possible to create a “foreign film repository” i.e. the Service SHOULD accept “foreign films” / “study transfers” from third party image routing / data sharing solutions / point to point DICOM connections into this repository. This repository will facilitate enterprise wide distribution and be configured such that studies within the repository are physically or logically demarcated as “foreign”. The repository MUST be capable of being locally configurable with regard to image storage / lifecycle management.

3.6.23 The Service SHOULD allow imported images to be flagged as copy images, to avoid duplication of archiving.

3.6.24 The Service SHOULD be capable of auto-routing DICOM objects to locations and systems specified by the trust.

3.6.25 The PACS MUST be capable of functioning independently of the trusts RIS in case the RIS is unavailable. The PACS MUST be capable, with minimum operator intervention, of re-aligning/reconciling its Services with the RIS after such a period of independent operation.

3.6.26 The supplier SHOULD provide details of how the PACS handles incoming DICOM exams which do not have an exam record created by HL7 and the algorithms typically used to perform matching.

3.6.27 In response to the PACS requirements the supplier MUST describe how the Service complies, or will achieve compliance over time, with the following:

- ISB 1503, Common User Interface – Date Display;
- ISB 1504, Common User Interface – NHS Number Input and Display;
- ISB 1505, Common User Interface – Patient Banner;
- ISB 1506, Patient Name Input and Display;
- ISB 1507, Sex and Current Gender Input and Display;
- ISB 1508, Telephone Number Input and Display;
- ISB 1501, Time Display;
- ISB 0149-02, NHS Number for Secondary Care;
- IHE, Patient Information Reconciliation (PIR);
- IHE, Post-processing Workflow (PWF);
- IHE, Import Reconciliation Workflow (IRWF);
- IHE, Portable Data for Imaging (PDI);
- IHE, Nuclear Medicine Image (NM);
- IHE, Mammography Image (MAMMO);
IHE, Evidence Documents (ED);
IHE, Simple Image and Numeric Report (SINR);
IHE, Key Image Note (KIN);
IHE, Consistent Presentation of Images (CPI);
IHE, Presentation of Grouped Procedures (PGP);
IHE, Image Fusion (FUS);
IHE, Cross-enterprise Document Sharing for Imaging (XDS-I);
IHE, Cross-enterprise Scanned Document Sharing (XDS-SD);
IHE, Teaching File and Clinical Trial Export (TCE);
IHE, Radiation Exposure Monitoring (REM);
IHE, Access to Radiology Information (ARI); and
IHE, Audit Trail and Node Authentication (ATNA) – Radiology Option.

3.7 Functional requirements – RIS

3.7.1 The Service MUST afford users with convenient access facilitated by log on functions, integrated at desktop level with PACS and ensuring that users are uniquely identified for audit purposes at all times. RIS MUST be capable of functioning independently of a trust PAS/EPR in the case it is unavailable; this MUST include the acceptance and viewing of patient demographic data and examination details including those not already known to the RIS. The RIS MUST be capable, with minimum operator intervention, of re-aligning/reconciling its Services with PAS/EPR and PACS after such a period of independent operation.

3.7.2 The Service SHOULD be capable of being integrated with the trust directory service to provide single sign on functionality for users logged in individually to trust’s servers and workstations.

3.7.3 The service MUST be capable of providing status update messages automatically in response to status changes within RIS. Although a default configuration should be offered, these should be locally configurable by an appropriately trained Trust employee.

3.7.4 The supplier SHOULD describe how the system will support pooled radiographer worklists in a paper-lite/paper-less environment.

3.7.5 The service MUST support the following data items:

- Forename;
- Surname;
- Date of Birth;
- Date of Death;
- Gender;
- Ethnicity;
- Identification number (radiology number, hospital number and unique examination identifier in radiology);
• Trust site code;
• Commissioner code;
• Referring clinician;
• Radiologist;
• Ward/ clinic;
• Speciality;
• Examination;
• Examination Report;
• Order filler Number:
• Status (i.e. Private, NHS etc);
• NHS Number (preferably verified);
• GP name, address, telephone number and practice code;
• Patient telephone number and mobile number;
• Patient e-mail address; and
• Patient type, e.g. outpatient.

**Requesting**

3.7.6 The Service MUST provide the capability to receive requests, vet them, capture justification and process both paper-based and electronic requests for examination.

3.7.7 The Service SHOULD have the ability to receive scheduled requests from the PAS / Order Comms and multiple other external sources and the ability to receive electronic requests with digital signature from future PAS or other sources and present for completion if incomplete.

3.7.8 The Service MUST clearly and safely display clinical and supporting information received from PAS / Order Comms or any other external sources.

3.7.9 The Service MUST have the ability to receive and display the requestor’s preferred appointment time and date slots.

3.7.10 The Service MUST have the ability to calculate the diagnostic wait time for the patients.

3.7.11 The Service MUST have the ability to capture from the PAS, the patient pathway identifier.

3.7.12 The Service MUST have the ability to scan documents into the Service, read any barcodes and insert that information into the request record and ensure this is visible throughout the system.

3.7.13 The Service MUST have the ability to capture and alert the user of patients alerts both electronically and input manually from paper records.

3.7.14 The Service MUST have the ability to track the progress of the order and its current location within the department ensuring that updated status information is fed back to relevant systems via standard messaging.
3.7.15 The Service MUST be able to obtain Date of Death information from the PAS. The Service SHOULD be configurable so that all images related to the patient can be automatically deleted or archived from the repository at a point after death determined by the trust.

**Worklists**

3.7.16 The Service MUST have the ability to automatically and manually create scheduled worklists, e.g. electronic order lists, vetting lists, request lists, waiting lists.

3.7.17 The Service MUST have the ability to print and/or export request summary to mobile device.

3.7.18 The Service MUST have the ability for the individual users within a trust to configure/produce filtered worklists. This SHOULD also be available at trust and group levels.

3.7.19 The Service MUST automatically generate a refusal/change advice, specifying the reason and suggest action and message to the requestor and requesting system.

3.7.20 The Service MUST have the ability to mark a requested imaging procedure as “pending” and provide a notification that the appointment is due < at a user configurable time period>, prior to the appointment being booked.

**Appointments**

3.7.21 The Service MUST have the capability to automatically and manually create appointments from manual and electronic requests.

3.7.22 The Service MUST have the ability to receive appointments from external systems and incorporate them into the RIS with the request information.

3.7.23 The Service SHOULD have the ability to automatically appoint accepted requests according to configurable protocols and to automatically create appointment advice and notify the requestor.

3.7.24 The Service SHOULD have the ability to categorise patients according to their anaesthesia requirements, and/or other requirements specified by the trust.

3.7.25 The Service SHOULD be able to display a breach date (or similar) for appointments configurable by the trust.

3.7.26 The Service MUST create an appointment/instruction letter with barcode and pass to print queue or export.

3.7.27 The Service MUST support trust configurable management of content and structure of appointment letters.

3.7.28 The Service SHOULD be capable of printing address labels/envelopes simultaneously with any letter.

3.7.29 The service MUST support configurable batch printing of reports, with the ability to exclude reports that have been sent electronically and reports that do not require printing.

3.7.30 The Service MUST support review of multiple room and resource bookings filtered as required (e.g. by consultant, room, exam group for either days, weeks or months) and manually allocate slots without navigating through multiple screens (it SHOULD be noted that a single room may be utilised for multiple purposes during one session and that a single
consultant may undertake several different activities in different places during a single session.

3.7.31 The Service MUST be capable of automatically producing appointment reminders in advance of the appointment according to set criteria and SHOULD be capable of generating letters, email or text to patients.

3.7.32 The Service MUST be capable of showing alerts at the booking stage and highlight alerts on the „front page“.

3.7.33 The Service MUST alert users of related appointments/examinations for the same patient.

3.7.34 The Service SHOULD create a scheduled demand for the associated resources and consumables; view it in advance and log the use of consumable and prepare summaries of usage and cost.

3.7.35 The Service MUST be capable of supporting NCIP codes (DSCN 27/2009) including spare fields to facilitate HRG4 / PBR / SNOMED reporting.

3.7.36 The supplier MUST be capable of supporting updates to Commissioner, GP Practice, Referring Clinician and Clinical Coding tables and SHOULD support updates to other tables as required. These activities SHOULD, wherever possible be managed by the supplier. The supplier MUST notify the trust of those activities the trust are responsible for managing.

3.7.37 The Service MUST search for and schedule appointments against a set of rules per consultant, modality and specialty, taking into account annual leave. The Service MUST allow the user to override the rules with a full audit trail and reason for the „force booking“ of the patient.

3.7.38 The Service SHOULD be capable of automatically producing a To Come In (TCI) card from the system when a bed is required for a General Anaesthetic (GA).

3.7.39 The Service MUST be capable of cancelling an appointment, capturing the reasons why the appointment was cancelled and by whom; a cancellation notification MUST also be provided:

The cancellation notification MUST be communicated back to the requestor/requesting system; and

Where a cancellation has been made, the Service SHOULD be capable of sending a new appointment linked to the original electronic appointment request.

3.7.40 The Service MUST be able to distinguish between a cancelled appointment and a rejected request. This distinction MUST be reflected in the messaging.

3.7.41 The Service MUST be capable of reserving slots for particular types of procedure, such as “sedation“ and GA.

3.7.42 The Service SHOULD be capable of marking an appointment as pending when a confirmation of a bed is required.

Booking

3.7.43 The Service MUST be capable of supporting the booking process, including the ability to:

- Support the patient arrival, identification, booking in and generation of all subsequent documents and messages;
• Receive a request from external systems, acknowledge receipt, send a booking confirmation to external systems, and receive allergy and other critical information from external systems;

• Recognise a patient appointed for that day by bar code or any other given information fields and book in that patient changing the examination status and reviewing allergy or other alert information i.e. from the bar code the patient is pulled up onto the screen;

• Provide a DICOM worklist to the appropriate modality;

• Re-direct DICOM worklists to an alternative modality following equipment failure or room closure;

• Locally and remotely review booked-in patient/s arrival times, appointment times, waiting times, current status and audit the results;

• Manually or automatically record patients who Did Not Attend (DNA) and notify requestor;

• Create a worklist to transfer patients;

• Book in an unappointed patient even if the PAS link is down, with the ability to reconcile demographic data when the PAS link is restored;

• Book in an unknown patient without any delay and create a data quality report to prompt for information later;

• Be able to enter a retrospective appointment date and time for importing previous images and support reconciliation after a Service outage;

• Book multiple appointments as a schedule of events, for example split acquisition in Nuclear medicine;

• If the patient is categorised as requiring a GA, the system MUST produce a prompt to book a bed and link to scheduling module within PAS;

• Produce labels which are configurable by the trust and contain bar codes to navigate around the system;

• Have a free text field to add comments when booking a patient; and

• Notify the department of deceased patients with outstanding appointments.

3.7.44 Regarding imported studies, the Service MUST have the ability to:

• Back date an exam to “true date of examination”, whilst also retaining the date of exam import;

• Identify as either “copy or imported images” on RIS for each exam / modality;

• Import report (PDF / Word document) to report field on RIS identifying it as referring hospital report; and

• SHOULD have the ability to import reports from HL7 feeds and DICOM Structured Reports.

Examinations

3.7.45 The Service MUST clearly display all alert information including allergies and infection control information.
3.7.46 The Service MUST allow the receipt of dose information from the modality, including all other examination information and the examiners comments including, but not limited to:

- Dose units, which need to be configurable per modality/room, (for example it needs to cater for one DR room where the DAP is in cGy.cm\(^2\) and another where it is in dGy.m\(^2\)). It also needs to cater for CT, with DLP per series and Total DLP for a study;
- For radiography, Exposure Factors and dose details (KV, mAs, and DAP)
- For CT, exposure dose details (CTDIdvol and DLP);
- Fluoroscopy screening time and DAP;
- Doses in configurable SI units; Maximum activity in MBq; and
- Stock number dose in MBq and time;

3.7.47 The Service MUST allow the receipt of information from the modality, including all other examination information and the examiners comments including, but not limited to:

- Justifier (and if unjustified, the reason for this). The service MUST be capable of providing this information to the requesting system via messaging;
- Log of carer and log of chaperon;
- Drugs administered including volume, expiry date, lot number and person injecting with output of cost; it SHOULD also provide the capability to record this information via barcode from the injection vial or drug packaging;
- Radiopharmaceutical prescription, including person preparing nuclide and compound definitions;
- Recount and net details;
- Admission time;
- Patient charges, noting exam description and code;
- A field for units;
- The attending radiologist;
- The charge; and
- A space for operator’s comments.

3.7.48 The Service SHOULD be capable of recording cancelled, not performed, rejected and incomplete examinations and log the reason, notifying the requestor.

3.7.49 The Service SHOULD be capable of maintaining controls and record usage of all consumable and pharmacy items, including radionuclide materials.

3.7.50 The Service SHOULD be capable of scanning and retaining any paper traces or records generated during the examination.

3.7.51 The Service MUST be capable of facilitating maintenance and availability of normal value tables, graphs and protocols.

3.7.52 The Service SHOULD be capable of holding templates for reports and support reporting during the examination.
3.7.53 The Service SHOULD be capable of supporting the addition or amendment of exams during attendance.

3.7.54 The Service MUST be capable of undertaking multiple examinations from one form.

3.7.55 The Service SHOULD support the addition of an examination not present in the current catalogue.

Clinical reporting

3.7.56 The Service SHOULD support "one step" or "multi step" reporting.

3.7.57 The Service SHOULD enable prompt reporting by configurable worklist.

3.7.58 Suppliers MUST describe how the Service prevents two people from reporting the same exam (i.e. lock the study).

3.7.59 Suppliers MUST describe how the Service locks an event while reporting is being undertaken, including reporting by Voice Recognition (VR).

3.7.60 Suppliers MUST describe how the Service refreshes worklists with current exam (reporting) status, and remove reported exams from worklist.

3.7.61 Suppliers MUST describe how the Service supports reporting using VR with keyboard and voice generated macros and enable addenda to be created.

3.7.62 Suppliers MUST describe how the Service supports multiple authors per exam.

3.7.63 Suppliers MUST describe how the Service supports reporting by radiographers, registrars, etc with authorisation requirements set by configurable rules.

3.7.64 Suppliers MUST describe how the Service supports un-authorisation of a report with the relevant security access.

3.7.65 Suppliers MUST describe how the Service supports blind and non blind double reporting via the worklist identified by both automatic criterion and manual selection with support for highlighting exceptions and discrepancies.

3.7.66 The supplier SHOULD demonstrate how workflow can be shared easily across organisation boundaries.

3.7.67 The Service SHOULD:

- Enable access to clinical information, including previous reports whilst undertaking a report, without having to break off;
- Support reporting templates according to exam type;
- Support full bi-directional desk top integration with the PACS solution;
- Pass reports to any number of systems including the PACS, other trust information management solutions and to external destinations, as required (including configurable by specified parameters, requestor, location, physician, modality);
- Auto send notification of report status messages to referrers by email, SMS, etc. with any necessary security to ensure confidentiality;
- Search and select reports by single or multiple words in the report;
• Support remote reporting. This SHOULD include the ability to use resources across organisational boundaries and to move to shared reporting centres, where required;
• Link external letters relating to the exam within the report, if required;
• Use spell check and user customisation and correction of the dictionary to accommodate complex medical terminology;
• Identify reports that have not been authorised for any given time period; and
• Change the colour of the exam within the worklist according to its status within the system.

Data handling and security

3.7.68 The Service MUST support wide ranging capabilities to import and export data and maintain data integrity, including the ability to:

• Export data to external systems in standard formats;
• Conduct flexible searches by any field or part field; Update PACS with exam status;
• Support data entry from hand held devices via industry standard wireless connectivity. The supplier MUST state the wireless connectivity standards which will be supported; Facilitate synchronisation of system clock with trust IT systems or other external time sources to ensure correct validations, where dependent on time stamp; and
• Facilitate manageable audit trails showing the activity of all system users which can be exported in standard formats, (for example, CSV, XML).
• For each of the above, the supplier should indicate the mechanism and whether this is a Trust responsibility or will need supplier intervention.

3.7.69 The Service MUST:

• Identify possible duplicate records and easily merge them;
• Produce an output of possible merges so that the merge can be undertaken on both PAS and RIS; and
• Automatically flag similar records when a record is accessed, so possible duplicates are clearly identified.

3.7.70 The Service MUST support the Import and export of data tables (e.g. consultants, GP, rooms) to and from other systems and enable full mapping with national exam codes (and any other coding cross references).

3.7.71 The Service MUST support the ability to manually create and amend records in data tables and pass these changes to PACS, where appropriate.

3.7.72 The Service MUST handle restricted address for patients with „special status” e.g. child protection patients.

3.7.73 The Service MUST be capable of driving MDT workflow, assigning tasks to members of the MDT group and recording decisions.
3.7.74 The Service MUST be capable of driving MDT workflow and provide the facility to schedule study images and reports for review at Multidisciplinary Team Meetings.

3.7.75 The Service MUST provide each MDT meeting with a worklist to enable prior review of imaging studies and reports at all participant organisations, and to serve as a permanent record of the studies reviewed at each meeting.

3.7.76 Radiologists MUST be able to create temporary worklists on RIS, which enables them to document enhanced opinions or simply document "reviewed at MDTM".

Billing

3.7.77 The Service MUST support the production of management reports and separate tariffs in relation to a single radiology procedure (e.g. completion of acquisition, completion of reporting and any additional procedure steps). In a shared domain this functionality must be held in trust specific tables.

3.7.78 The Service MUST support costing the planned and actual activities at departmental level <and more detailed level if required> with given cost rates and overheads and identify costs attributable to specific patients.

Messaging requirements

3.7.79 The Service MUST be capable of (dependent on whether reporting is/can be undertaken on PACS) receiving reports from PACS with suitable review of status and time raised (PACS/RIS/PAS/Order Comms integration).

3.7.80 The Service MUST support transparent and manageable interfaces with errors evident through flagging (not hidden in logs).

Management statistics and administration

3.7.81 The Service MUST support the management of a department and its resources, including the ability to:

- Set performance targets with the ability to generate graphs of the results;
- Log, control and re-order consumable items and generate order forms/ screens with stock and account codes;
- Monitor the flow of patients through the department and;
- Review security audit trails.

3.7.82 The Service MUST enable full support for film packet and film library control as part of the department business continuity plans for when PACS not available.

3.7.83 The Service MUST provide user friendly, comprehensive and user customisable business reporting, enabling both custom queries of the database and a range of pre-defined management reports including (but not limited to):

- Statutory radiology returns;
- Workload activity, based on numbers of attendances and examinations performed by operator, procedure and worklist (including modality worklist and MDT meetings);
- Waiting time returns for patients from the time of referral and turnaround times between changes in status in procedure workflow (requested, booked, performed, reported, verified, issued, etc);
- Capacity and demand reports based on modality work area availability and scheduling usage;
- Reporting activity by reporting clinician and modality; and
- Staff training logbooks detailing the number of examinations observed, reported, and supervised by procedure and modality.

3.7.84 Suppliers MUST define what reports are supplied as standard and supported export file formats:

- Produce a report for all unreported and unauthorised exams;
- Support group referrers (e.g. GP practices, different specialities) for statistical analysis;
- Regarding exported studies, the ability to record how files were transmitted (e.g. electronic, film, CD), when transmitted; what studies were transmitted and by whom (e.g. date, time and user);
- Export a report with images (DICOMDIR CD / DVD) on removable media (electronically on patients file); and
- Produce a dose audit report by examination, by room etc.

3.7.85 The Service SHOULD support the ability to automatically, securely distribute scheduled reports locally over the trust network and more widely via e-mail.

3.7.86 The Service MUST support the ability to monitor when reports have been read and by whom.

3.7.87 It MUST be possible to display user-defined database query results and reports within the GUI and to export these results in standard formats and spreadsheet / statistical analysis software (e.g. CSV, Excel). The Service SHOULD support saving of locally defined queries for modification and repetition.

3.7.88 The Service MUST support the constraining of reporting to allow the impact on the Service to be minimised. The Service SHOULD support the scheduling of reports to run at a predetermined time and on a periodic basis.

3.7.89 The Service database SHOULD be ODBC compliant via third party reporting systems.

3.7.90 The Service MUST support coding to facilitate the recording, sharing, exchange and comparison of data and information. Coding MUST comply with NHS data standards, guidance and rules as defined in the NHS Data Dictionary and the ISB.

3.7.91 The NHS Data Dictionary and ISB are regularly updated (e.g. via ISNs). The coding used by the Service MUST be updated by the supplier to reflect these updates within a reasonable timeframe. This timeframe will be agreed between the supplier and the trust.

Shared RIS instances

3.7.92 The option to share a hosted RIS across a number of trusts within a healthcare community SHOULD be made available by the supplier, if required. Trusts who share a RIS MUST be able to appropriately configure the system at a local trust level.

3.7.93 Suppliers SHOULD describe how unique numbering will be maintained in the context of shared RIS instances and when migrating historical data.
3.7.94 The supplier MUST demonstrate how their RIS solution will allow the sharing of information, so that over time, organisations can share workload and set up shared reporting centres if required. Suppliers are invited to list which configuration items must be shared i.e., those that are not configurable at trust level.

3.7.95 The Service MUST support the import of reports from external systems and pass reports to PACS.

3.7.96 The Service MUST support export of optionally encrypted patient records to an external organisation (the Service MUST allow for the copying of patient data onto encrypted media and MUST also allow for the data to be shared electronically).

3.7.97 The Service MUST support the exchange of reports (and other data) to other systems and to external referrers within and outside of the trust. The supplier MUST explain how this will be achieved.

Standards

3.7.98 In response to the above RIS requirements, the supplier MUST describe how the Service complies with the following standards:

- ISB 0103, Diagnostics Waiting Times and Activity Data Collection;
- ISB 0070, Healthcare Resource Groups;
- ISB 0148, Interim Clinical Imaging Procedure Codes;
- ISB 0084, OPCS Classification of Interventions and Procedures;
- ISB 1552, READ Clinical Terms v3;
- ISB 1553, READ v2;
- ISB 0095, Referral to Treatment Waiting Times;
- ISB 1577, Diagnostic Imaging Dataset (to be issued April 2012);
- IHE, Patient Information Reconciliation (PIR);
- IHE, Post-processing Workflow (PWF);
- IHE, Reporting Workflow (RF);
- IHE, Evidence Documents (ED);
- IHE, Simple Image and Numeric Report (SINR);
- IHE, Cross-enterprise Document Sharing for Imaging (XDS-I);
- IHE, Access to Radiology Information (ARI);
- IHE, Audit Trail and Node Authentication (ATNA) – Radiology Option;
- IHE, Radiation Exposure Monitoring (REM); and
- IHE, Charge Posting (CHG).

3.8 Functional requirements - CR / DR

This section has been included within the core requirements as CR is currently provided through the LSP model and trusts will need to ensure continuity of this service. It is acknowledged that trusts may choose to procure DR as opposed to CR.
3.8.1 The supplier MUST state which CR/DR options it can supply but allow the trust to purchase from alternative suppliers if they choose. In this case, the supplier MUST state their integration requirements and provide connection support.

3.8.2 The supplier MUST demonstrate how their CR/DR complies with the relevant guidelines, industry best practice and regulations relating to doses, such as IR(ME)R.

3.8.3 The Service MUST be capable of digitally capturing all plain film images/ examinations, including intra-oral dental plates, OPG / Cepholostat and mobile radiography on cassettes and produce laser hard copies to a networked DICOM imager, as required.

3.8.4 The supplier MUST state what contingencies are in place, so that in the event of a PACS failure, the department can continue to use the CR/DR.

3.8.5 The supplier MUST state what contingencies are in place, so that in the event of a power failure, the department can continue to use the CR/DR.

3.8.6 The supplier MUST state what contingencies are in place, so that in the event of a PACS failure, the department can continue to use the CR/DR and safely retain the acquired examinations for automatic export to PACS, as soon as the PACS is available.

3.8.7 The Service MUST be fully integrated with the RIS, such that patient demographics can be automatically added to the imaging worklist and film marking system. The supplier MUST state how this will be achieved.

3.8.8 All DICOM requirements MUST be supplied to enable the system to integrate fully and any optional DICOM Services MUST be clearly stated. The supplier is responsible for ensuring successful integration with RIS, PACS, and x-ray equipment.

3.8.9 Suppliers MUST state whether the unit supports DICOM Modality Performed Procedure Step (MPPS).

3.8.10 Suppliers MUST work with third parties to achieve integration, e.g. for orders and results. Suppliers are invited to explain how this will be achieved, if it is chargeable, the responsibilities of each party and their approach to issue resolution.

3.8.11 Software upgrades MUST be supported free of charge during the life of the contract. The supplier MUST state how these will be implemented so that the trust’s user configurations, export settings and interfacing will be maintained.

3.8.12 The supplier MUST provide details of the image processing algorithms used to produce a diagnostic image from the raw data. The supplier MUST state whether the algorithms can be changed should an incorrect one be applied, and the time/processing limit to when this is achievable.

3.8.13 The supplier SHOULD state whether dedicated „specialist” (e.g. paediatric) software is available.

3.8.14 The supplier MUST describe the solution for prioritising urgent images. Some examinations will need to be processed more urgently than others; the supplier MUST describe how prioritisation of urgent images will be achieved within the CR/Digital system.

3.8.15 The supplier MUST describe the user interface device and how users can select or enter patient/exam details. The supplier MUST define how many user interfaces will be supplied with each type of digitiser/reader.
Digitiser/ CR Reader

3.8.16 The supplier MUST state the dimensions and weight of each unit type on offer including footprint, and identify any additional space that MUST be left to the front, rear and each side.

3.8.17 The supplier MUST state the power requirements and other environmental requirements and whether the digitiser/CR reader can operate from a standard UK 240V,50Hz 13 amp socket. This SHOULD include any requirement for air quality or temperature. The supplier MUST state if the CR reader/digitiser performs any self-calibration to reduce non-uniformity, and if so, describe how this will be achieved.

3.8.18 The supplier MUST state if the CR reader includes a cassette buffer and if included, state how many cassettes can be loaded within the input buffer at any one time and how many can be stored within the output buffer at one time.

3.8.19 The supplier MUST state the throughput (images per hour) for each cassette size, available for both a multi-loader and single processing unit.

3.8.20 The Service SHOULD state the expected life span of cassettes or plate readers both in terms of exposures or physical longevity if the maximum number of exposures is not achieved. Any relationship between the validity of the warranty or charges for replacement / repair must be clearly stated.

3.8.21 The supplier MUST define the plate processing time, and also the throughput time for a typical adult (35cmx43cm) plain film chest examination, stating all assumptions and defining each step of the workflow. Please indicate time to view preview and final image separately.

3.8.22 The supplier MUST state the range of effective speeds of the system and how these have been measured. The supplier SHOULD state the speed at which their system can operate and provide clinically acceptable images. Suggested minimum acceptable speed should be 400 (or 2.5uGy) and 300 for chests (3.33uGy).

3.8.23 The supplier MUST give details of the method by which a cassette jam is dealt with and whether this can be manually rectified by a trust user.

3.8.24 The supplier MUST detail how images that fail to transmit from the CR reader/digitiser can be resent remotely and the timeframe involved. This SHOULD include the support time this Service will be available to the trust.

3.8.25 The supplier MUST provide details of the method by which the cassette is identified with the patient’s examination details and if a separate piece of equipment is required. Demonstrate that it is not possible for a cassette, once identified with a patient, to be associated with another patient in error, stating the means by which cassette identification is achieved. The supplier MUST state whether the patient’s details can be changed if they are incorrect.

CR Image capture plates

3.8.26 The supplier MUST:

- Give details of the type and range of cassette sizes that can be used. The supplier MUST for each size, state the image size (cm), cassette size (cm), and sampling rate (pixels per mm).
• The supplier MUST state if high resolution plates will be supplied. If so, state whether they are combined with the proposed digitiser/reader as standard and whether they are suitable for „specialist use“ (e.g. paediatrics);

• State the number and range of cassette sizes that are included as standard with each type of digitiser/reader;

• State the expected or guaranteed lifetime of the image plates (number of cycles), and how the number of cycles a plate has undergone is identified;

• State the dynamic range;

• State if the cassettes include a scatter plate and what this is constructed from;

• State if the image plates are hard backed or flexible; and

• Provide a graph of the latent image decay as a function of time.

3.9 Acquisition workstation

3.9.1 The supplier MUST:

• State the type of acquisition workstations to be supplied as part of the solution;

• State the time between image plate entering digitiser/reader to be read and the time for the image to be ready for manipulation;

• Suppliers MUST state whether it is possible for the operator to change the reconstruction algorithm SHOULD an incorrect one be chosen initially and whether this change could take place at a later date;

• Suppliers MUST state what post processing functions are available on the workstation (e.g. annotation) and whether these are supplied as standard features;

• State which of the patient and examination details are attached to the image as standard and if this can be configured to display further details e.g. anatomical markets, free text notes; and

• State at what stage a patient”s demographics, image annotation, and other post processing operations „fixed“ (i.e. no longer able to be changed by the operator).

3.9.2 Regarding the monitor, the supplier MUST state the following:

• Brightness (in foot lamberts or candela/sqm);

• Refresh rate in Hertz;

• Spot size at the centre and within 12mm of the periphery;

• Expected lifetime of the monitor, before maximum brightness falls below the specified value;

• The quality assurance programme for monitors – i.e. what needs to be done and by whom and when to achieve a stated result;

• Monitors MUST be of the flat panel;

• Monitors MUST be designed to meet statutory requirements for the operation of VDUs and the recommended lighting conditions for each type of workstation MUST be stated;
• State if an automatic brightness adjustment control is included. Confirm that the workstation is suitable to support a radiographer in undertaking preliminary diagnostic work; The supplier MUST give details of any dose monitoring package/s and whether these are provided as standard or as an option;

• State if it possible to configure the workstation to suit the user’s requirements, e.g. to add or remove tools and options which are or are not routinely used.

3.9.3 The supplier MUST describe whether the workstation can be used to burn CDs of patient examinations which can be for subsequent viewing on any standard PC without the need for a separate DICOM viewer.

3.9.4 The supplier MUST describe whether it is possible to view previous images on the workstation.

3.9.5 The supplier MUST state how many images can be stored on the hard disk drive, and at what image resolution.

3.9.6 Suppliers SHOULD state whether images stored on the hard drive are automatically deleted or, have to be manually deleted by an operator.

3.9.7 The Service MUST provide image reject analysis and have the facility to retain and display rejected images as part of a quality assurance programme. The trust MUST be able to configure who has access to these images.

3.9.8 The Supplier MUST state details of Quality Assurance package(s) available and state whether QA packages are included as standard or supplied as extra cost options.

3.9.9 The Supplier MUST state the recommended quality control procedure.

3.9.10 The Supplier MUST state:
  • details of Dose Analysis package(s) available;
  • state whether this is part of the QA package or separate; and
  • state whether Dose Analysis is included as standard or supplied as extra cost options.

3.10 Voice recognition (VR)

3.10.1 The VR Service SHOULD be fully integrated into the trust <PACS and/or RIS Service> to support the radiology workflow and enable “hands-free” worklist reporting (e.g. download patient, upload of completed reports; synchronisation of images to reports, support “talk and image manipulation” simultaneously).

3.10.2 The Service:
  • MUST support a “UK English” language setting;
  • MUST reliably support roaming profiles;
  • MUST enable “accession numbers” to be linked (e.g. associate one report to two or more separate accession numbers);
  • SHOULD enable authorised users to view the history of prior reports;
  • SHOULD support the addition and storage of customised data fields (e.g. additional reference numbers, multiple clinicians names); and
  • SHOULD have the ability to enable the control of the reporting environment by voice.
Dictionary and spelling
3.10.3 The Service MUST provide an appropriate “spell-check” and a “drop-down” selection of alternative spellings.
3.10.4 Voice commands MUST be supported for formatting of reports (e.g. bold, underline, capital letters).
3.10.5 The Service MUST provide a radiology specific dictionary. Specialist dictionaries SHOULD also be available to the trust, if required.
3.10.6 The Service SHOULD support automatic correction of reports (e.g. automatic capitalisation).
3.10.7 The Service MUST support “learning” of new voice/accents.
3.10.8 The Service MUST allow the dictionary to be updated by authorised users to include new words (e.g. addition of new drugs).

Reporting
3.10.9 The Service MUST support navigation within a report using voice commands.
3.10.10 The Service SHOULD enable report templates to be added and deleted by authorised Service users.
3.10.11 There MUST be the ability to add addenda items to VR reports.
3.10.12 The Service SHOULD support the use of short-cuts.

Training
3.10.13 Service users MUST be fully trained at the outset in the use of the VR Service. Suppliers are also invited to what additional training options exist post go live.

Editing
3.10.14 The Service MUST enable reports to be edited by authorised Service users.
3.10.15 The Service MUST support the editing of changes by voice and/or keyboard command. An “undo” function SHOULD also be provided (e.g. in case a report has been approved/deleted in error). This type of change MUST be messaged to the order comms system.

Security
3.10.16 The Service MUST use appropriate user authentication.

3.11 Radiotherapy/ oncology
3.11.1 The Service MUST support the storage of RT image, RT plan, RT dose, RT structure set and RT treatment record.
3.11.2 The Service SHOULD support the display of RT image, RT plan, RT dose, RT structure set and RT treatment record.
3.11.3 The Service SHOULD be capable of autorouting DICOM RT objects between RT software systems, <criteria to be specified by trust>.
3.11.4 The supplier SHOULD be compliant with the IHE (IMAGE) fusion profile including: Support of the DICOM Blending Presentation State; and
4 Non Functional Requirements

This section sets out the Non-Functional requirements needed to perform the Service.

<If the trust requires an image archive service and/or enterprise sharing services, the non functional requirements in Sections 9.3 and 10.2 MUST also be included>

Suppliers MUST describe how they will meet each of the requirements.

4.1 Performance requirements

Performance is the speed (response time) or effectiveness (throughput) of a computer, network, software programme or device.

4.1.1 Trusts will need to define local performance requirements.

4.2 Reliability/availability

Reliability is the ability of a system or component to perform according to its specifications for a designated period of time.

Availability is the ratio of time a system or component is functional to the total time it is required or expected function.

4.2.1 Trusts will need to define local requirements.

4.3 Scalability

Scalability is the ability of a system to continue to function well when it is changed in size or volume in order to meet a user need.

4.3.1 Trusts will need to define local requirements.

4.4 Information Governance

4.4.1 The supplier MUST be able to demonstrate that their product can be implemented in a way that allows the trust to meet the Care Record Guarantee.

Authentication

4.4.2 User access to the Service SHOULD be authenticated by an e-GIF level 3 compliant two-factor authentication mechanism, such as that provided by the Spine Security Services. The supplier SHOULD describe how it intends to meet this requirement.

4.4.3 Where e-GIF level 3 compliant two-factor authentication mechanisms cannot be achieved; authentication SHOULD be based on alternative strong (2-factor) authentication systems.

- Where strong 2-factor authentication cannot be achieved, single factor authentication solutions MUST be implemented.
- The supplier MUST describe how it intends to achieve authentication by an e-GIF level 3 compliant two-factor authentication mechanism in their future product roadmap.

4.4.4 Passwords MUST be managed following the recommendations in the Good Practice Guide - Password Policy for Non-Spine Connected Applications which is available for those with N3 connectivity on the following link:
The supplier MUST describe how it intends to achieve authentication by an e-GIF level 3 compliant two-factor authentication mechanism in their future product roadmap.

4.4.5 The Service MUST be capable of authenticating users, and providing an active user session (in which the application can be navigated and used) in less than five seconds from the point at which authentication is achieved, such as following Smartcard Passcode entry.

4.4.6 The Service SHOULD support federated security and appropriate NHS Information Governance controls.

4.4.7 The Service SHOULD support the use of NHS Spine as an Identity Provider (IdP).

4.4.8 The Service SHOULD support use of future Spine authentication methods. i.e. The Service SHOULD support Authentication of x509 certificate-based credentials.

4.4.9 The system SHOULD support consumption of SAML 2.0.

4.4.10 The Service SHOULD support federated identity, where an end user or end system indicates a trusted IdP against which they can be authenticated.

4.4.11 If the system is unable to take advantage of Federated Identity (such as that provided by Spine) the Service MUST provide its own Identity Provider (IdP). This MUST provide end user and end system security credentials. It MUST also provide the ability to define user groups. User accounts can be:

- Added;
- Updated;
- Deleted;
- Locked; and
- Unlocked.

User groups can be:

- Created;
- Add accounts;
- Remove accounts; and
- Deleted.

4.4.12 All authentication activity MUST be fully audited.

RBAC

4.4.13 A default set of roles MUST be defined within the Service if role based access control is used. Additional roles can be created or deleted by the trust administrator. The Service MUST enable permissions to be added or removed from roles by the trust administrator.

4.4.14 The Service SHOULD support use of Spine RBAC for authorisation information.

4.4.15 All access control activity MUST be fully audited as defined in PACS RIS Core Statement of requirements section 4.5.

4.4.16 The Service MUST support the use of Role Based Access Controls to provide access levels and privileges (including view only, edit, etc.) by certain criteria, e.g. individual, group,
template. Suppliers SHOULD briefly describe the implementation of their role-based access control.

4.4.17 The system SHOULD implement local role-based access controls which support the allocation of access rights in line with the nationally-defined Job Roles/Areas of Work and Activities. The national set of RBAC roles and activities are published in the national RBAC Database (NRD), available by email request to esp.ig@nhs.net. Those local RBAC mechanisms SHOULD:

- Restrict users” use of the system to specific functions, assigned by the system manager(s) and only by the system manager(s); and
- Not allow any user access to their allocated functions until they have successfully authenticated.

4.4.18 Access controls MUST include the ability to segregate access to the following functions:

- Viewing the audit trail;
- Accessing inactive staff details; and
- Accessing the records of patients that are not normally accessible to system users.

4.4.19 The Service MUST ensure that, when stored locally, user profile information which supports RBAC mechanisms is protected from unauthorised access (including view, modify, or delete).

4.4.20 The national set of RBAC roles and activities are published in the national RBAC Database (NRD), and contain activities that are valid for access to audit trails. The NRD is available by email request to esp.ig@nhs.net. The Service SHOULD ensure that systems are configured to support the most current release of these. If suppliers have not implemented the national RBAC model then the local access controls SHOULD demonstrate that only appropriate roles can access the audit trail.

Legitimate relationships, restricted access and consent

4.4.21 The supplier MUST describe how the Service limits access to patient related information, by reference to certain criteria, including (but not limited to): authenticated identity, patient class e.g. medicine, patient location, legitimate relationship, application/menu/function, data element, time, and workstation location.

4.4.22 The supplier MUST demonstrate how their system will be implemented so that patient consent preferences to the sharing of their data can be ensured.

4.4.23 The supplier MUST demonstrate how their system will be implemented to enable legitimate relationships between patients and system users to be enforced.

4.4.24 The supplier MUST demonstrate how their system will be implemented so that the NHS Information Governance control Sealing – keeping certain patient information confidential – can be ensured.

Network

4.4.25 The Service MUST prevent any unauthorised connections.

4.4.26 All Patient Identifiable Data (PID) MUST be secured in transit. Across the trust network, where cryptographic methods / techniques are utilized the preferred method is TLS protocol; where TLS cannot be utilized the next preferred method is SSL protocol; where
neither TLS nor SSL are viable options the alternative SHALL be IPSec protocol. The provider MUST describe how this will be achieved.

Session

4.4.27 The Service MUST be able to automatically timeout a user session, after an interval of inactivity or if the maximum session timeout has been exceeded, and MUST be capable of being adjusted according to global/local computer requirements.

4.4.28 The Service SHOULD support the option of persisting the session. This SHOULD allow the user to reconnect and resume their work without re-navigating to the screen/study/image they were viewing when the session was terminated.

4.4.29 In the absence of session persistence the Service session MUST be able to close down tidily without any corruption to data files, e.g. close down server sessions, and remove any patient identifiable information from the desktop or local hard drive (cache and/or display and image caches).

4.4.30 Procedures to ensure data integrity and security, including backup and software patches, updates, operating system / DBMS updates and upgrades, SHOULD be able to be carried out with no impact on the normal operation of the Service.

4.4.31 The Service SHOULD provide session persistence capabilities that allow user sessions to be suspended (e.g. on Smartcard removal) and resumed (e.g. when the same Smartcard is re-presented). When a session is resumed the user context from the previous session SHOULD be restored within a configurable time period. Sessions should not be arbitrarily „killed“ when a user temporarily leaves a session or removes a Smartcard; rather the session should be terminated only when user explicitly log out, or after a configurable period of inactivity.

4.4.32 It SHOULD be possible to regain access to a suspended session in less than 5 seconds of re-presentation of the correct Smartcard.

4.5 Audit and Audit Analysis

Audit

4.5.1 To ensure accurate time stamping of audit events and support for the Consistent Time IHE profile, the Service MUST be synchronised with a reliable external time source that implements the Network Time Protocol (NTP).

4.5.2 Audit records MUST be kept indefinitely and on termination of service usage by a trust, must be transferred to the trust in an agreed format.

4.5.3 The supplier MUST describe how the Service audits activities undertaken by the trust, such that relevant data can be retrieved and provided to the requestor.

4.5.4 The collection of personal identifiable data, such as the creation of, or entry of data into a healthcare record, MUST generate an audit record.

4.5.5 Transmission of personal data outside of the Service / trust / data controlling organisation MUST be recorded along with details of the sender (user/system, organisation), receiving entity (user/workgroup/system), organisation, and at what time.

4.5.6 Audit data MUST be available to a trust without the need to contact the supplier. Audit data SHOULD be available in a useable way to a specified key user at the trust.

4.5.7 The Service MUST facilitate audit and analysis of all processing activities undertaken on personal data.
4.5.8 The Service MUST audit the access to personal data along with by whom, where and when the access occurred.

4.5.9 The Service MUST audit the storage of studies, images and reports along with an identifier of what is stored (meta-data).

4.5.10 The Service MUST audit the deletion of studies, images and reports along with an identifier of what was deleted (meta-data).

4.5.11 The Service MUST provide audit trail functionality to record, retain and report on system use that covers all Service events including (but not limited to) Create, Read, View, Print, Update and Delete functionality.

4.5.12 The Service MUST ensure that Audit Data Entities are kept by the Service to identify the following:

- User or system activity;
- Unique user identification;
- Unique user role profile;
- Unique device identification;
- Unique organizational identification; and
- Unique patient identification.

What:
- Identification of Service events;
- Changes to application data including type of change and where to go to find the change;
- Changes to system configurations;
- Message interactions between systems;
- Printer output; and
- Alerts generated.

Where:
- Unique identification of network access point IP addresses; and
- Identification of audit source.

When:
- Time and date user logs onto the Service;
- Time and date users log off the Service; and
- Time and date application data accessed by users.

Audit analysis

4.5.13 The audit analysis Service MUST never modify the source audit trail data.
4.5.14 The audit analysis Service MUST provide facilities for only approved users to retrieve audit data and produce reports that identify system use.

4.5.15 Access to audit trail data or its interrogation by any means MUST be restricted and controlled using Role Based Access Control.

4.5.16 The audit analysis Service MUST be able to retrieve audit trail data from multiple sources, including databases, applications, network devices and operating systems. A range of adaptors MUST be provided as standard to interface to the most common types of source system.

4.5.17 Audit trail retrieval may be from networked devices, or data imported from physical media onto the device hosting the tool. The audit analysis Service MUST be able to accept either mechanism.

4.5.18 Audit trails may be in multiple formats including flat text files (CSV, XML, or database extracts). As a minimum the audit analysis Service MUST be able to import these file types.

Functional requirements

4.5.19 The audit analysis Service MUST determine recurrences of the same event and aggregate and present this information in a meaningful manner.

4.5.20 The audit analysis Service MUST present reports either on-line (web interface), via email, or to a printer.

4.5.21 Reports MUST be in a form that enables the matching of the audit trail data so that those originating from different sources can be correlated.

4.5.22 The audit analysis Service MUST allow an authorised user at the trust to search audit trail data and produce ad hoc reports based on configurable time periods for configurable event categories.

4.5.23 The audit analysis Service MUST provide the capability for authorised users at a trust to review trend/variance status of events categories.

4.5.24 In response to the audit requirements the supplier MUST consider how the Service complies with the following standards:

- ISB 1512, Information Governance Standards Framework;
- ISB 0086, Information Governance Toolkit;
- IHE, Access to Radiology Information (ARI);
- IHE, Audit Trail and Node Authentication (ATNA); and
- IHE, Basic Patient Privacy Consents (BPPC).

5 Service delivery

This section sets out the Service Delivery requirements needed to perform the Service. Suppliers SHOULD describe how they will meet each of the requirements below.

5.1 Joint management and collaboration

5.1.1 The supplier will be required to operate in a complex and changing environment. Working with multiple stakeholders including NHS trust departments and potentially other third party suppliers will be required. The supplier MUST demonstrate skills and experience of working across multiple stakeholders.
5.1.2 The supplier will need to demonstrate that during the contract lifetime:

- They will provide a mechanism to ensure the Service users have input into future system design/ functionality updates;
- Ideally this SHOULD include a user group including an electronic forum (with both clinical users and system administrators involved) allowing users visibility of and feedback into the product roadmap;
- Ideally a product developer will be present at the user group meetings and involved in the electronic discussions to have an honest dialogue between users and supplier about what enhancement suggestions are viable for the supplier; and
- There will be a rolling agenda for product enhancement during the contract. The supplier MUST provide clarity on how subsequent versions of the product will be rolled out including any reasonable assumptions of financial or resource implications for the trust.

5.1.3 The supplier MUST confirm their willingness to enter into a source code escrow agreement with the trust as part of the support contract.

Implementation

5.1.4 The supplier MUST demonstrate the capability to implement their system to the timescale dictated by the trust.

5.1.5 The supplier SHOULD demonstrate how they might best use the existing trust PACS and RIS assets, if required.

5.1.6 The supplier SHOULD demonstrate that they are able to effectively integrate with the systems as defined by the trust.

5.1.7 The supplier MUST demonstrate that they will effectively migrate any existing imaging data safely using a mechanism approved by the trust Caldicott Guardian.

5.1.8 The supplier MUST integrate the PACS system to the trusts chosen off line archive ensuring data integrity is maintained.

Delivery and installation

5.1.9 The supplier MUST deliver the following implementation Services:

- Integration of all new hardware and software with existing, retained, hardware and software;
- Integration of imaging equipment;
- Setup of code tables to national and trust standards as appropriate; and
- Setup of interface software to map Service code tables to code tables of external systems.
- The supplier MUST state for each Service how these shall be provided.

5.1.10 The supplier MUST provide a Warranted Environment Specification (WES) detailing the minimum and recommended specification requirements of trust computers and workstations.

5.1.11 The supplier MUST give full details of the physical Warranted Environment Specification (WES) requirements for server room hosted components, including space,
minimum access clearances during installation (i.e. minimum door frame sizes, etc.), load bearing capacity, electrical supply, water, drainage and cooling, humidity, and UPS requirements for each item of equipment proposed, to be installed.

5.1.12 The supplier MUST state what environmental monitoring and reporting is provided and required and what options exist to alert and take automated action in the event of a WES breach (e.g. initiate a tidy closedown if it is detected that the Service is running on UPS).

5.1.13 The supplier MUST act as prime contractor for the supply, installation, upgrades and maintenance of all interfaces relating to this Service. The supplier SHOULD provide a project management resources in this respect to work with the Trust to agree and document a project plan including cutover arrangements and detailing Trust responsibilities e.g. modality supplier management.

5.1.14 In response to the Service requirements the supplier MUST consider how the Service complies with the following standards:

- ISB 0160, Patient Safety Risk Management System – Deployment and Use of Health Software; and
- ISB 0129, Patient Safety Risk Management System – Manufacture of Health Software.

User training

5.1.15 The supplier MUST propose an approach to training that includes the following:

- All relevant trust staff groups MUST be appropriately trained at the outset and the training MUST be reviewed after <six months> by the trust, supplier and trust/supplier jointly; and
- All relevant trust staff groups MUST be appropriately trained with regard to each new version and / or significant change in functionality of the Service and the training MUST be reviewed after <six months> by the trust, supplier and trust/supplier jointly.

5.1.16 The supplier MUST supply experienced trainers to train trust staff.

5.1.17 The supplier MUST provide a training schedule. Training MUST be both structured and timely. It MUST produce a workforce that is competent in all required aspects of the operation of the Service.

5.1.18 Training MUST highlight the need for local contingency plans for use when functions of the Service do not work.

5.1.19 All documentation MUST be provided both on-line (and/or electronically) and in hard copy form. The supplier MUST confirm that printing on-line documentation and duplicating hard copy documentation for use within the trust will not breach their copyright.

5.1.20 The supplier SHOULD supply details of their approach to computer-based training packages and on-line training support.

5.1.21 The supplier MUST supply details of training support provided post-implementation, including the training approach for new staff.

5.1.22 The supplier MUST state any prior training or qualifications required before any member of trust staff is considered suitable to participate in the suppliers training programme.
5.1.23 Training methods MUST be clearly stated.

5.1.24 The supplier MUST describe and SHOULD also supply examples of the following: trainer documentation, trainee documentation, lesson plans, structured course programme, evaluation forms that form part of the training programme. This MUST also include training packages for new radiology and clinical staff external to radiology.

5.1.25 There SHOULD be a test and training system which is separate from the live environment. This SHOULD act as a test-bed for integration with other clinical systems and 3rd party plug-ins and testing new builds and versions prior to roll out into live environment.

5.1.26 The supplier MUST provide training (to a schedule agreed with the Trust) for a minimum of <two system administrators>.

5.1.27 The supplier SHOULD describe what options exist for further staff training post go live e.g., for new system administrators.

5.2 Benefits and outcomes

5.2.1 The supplier SHOULD be committed to supporting the benefits as described in the <trust”’s Benefits and Statement of Needs documents>.

5.3 Trust’s responsibilities

5.3.1 The supplier MUST detail all responsibilities required to be performed by the trust. These responsibilities MUST be agreed between the two parties.

5.4 Clear leadership

5.4.1 An explanation of the supplier”’s governance and product development arrangements MUST be provided, particularly detailing where UK market development requirements compete against requirements from other territories. The supplier SHOULD state the name, role and briefly outline the qualifications and experience of their key clinical leaders.

Suppliers SHOULD also outline the extent of clinical leadership within their UK organisations.

5.4.2 The supplier SHOULD briefly describe their framework for ensuring Clinical Safety of their product(s) and name the role and postholder with overall responsibility for Clinical Safety:

- In their worldwide organisation; and
- In the UK organisation.

5.4.3 The supplier MUST describe the types of code releases they issue (including major releases, minor releases, Service updates / packs, safety releases / patches, Field Safety Corrective Actions) and the quality assurance relating to each release.

5.4.4 The suppliers MUST use the following template in responding and SHALL complete a new table for each discrete product provided as part of the Service:
Where a supplier’s release introduces new or significantly changed functionality, the supplier SHALL support the trust in testing the new release on their test environments and provide training at no additional cost.

5.4.5 The supplier SHALL describe their overall governance and post-market vigilance framework. For PACS, CR / DR and other products classed as Medical Devices, this MUST refer to:

- How users can report safety incidents;
- The mechanism of notification of Field Safety Correction Actions, as defined in MHRA Directive Bulletin 3;
- How corrective actions are implemented and how the trust are expected to accommodate the supplier in making the necessary changes; and
- Any tasks / responsibilities the trust are expected to carry out under the suppliers’ framework.

5.4.6 For RIS and other aspects of the Service not currently classed as medical devices, the supplier MUST outline their quality assurance procedures for safety incident notification, incident management, safety notifications and responsibilities of trust and supplier in implementing safety-related changes.

5.5 Adequate qualifications

5.5.1 The supplier MUST provide details of the names and qualifications of the team members who will participate either wholly or partly in delivering and developing the Service. This information MUST be updated on a regular (at least annual) basis.

5.6 Organisational Capacity

5.6.1 The supplier MUST demonstrate they have the capacity to support all of the business they have across NHS England, and that they have a scheduling process that ensures trusts are not in competition for scarce resources as a result of the supplier over committing or
failing to plan effectively. Suppliers SHOULD also document whether they would need to undertake additional recruitment in order to adequately provide the Service.

5.6.2 Given the volume of re-procurement that will take place between 2013 and 2016 the supplier MUST demonstrate that they not only have the capacity to take on the individual trust based on their existing workload, but also on any future planned workload.

5.7 Detailed data migration and implementation plan

5.7.1 The supplier is responsible for the migration of the current trust data from the existing PACS and RIS into the new Service.

5.7.2 As part of the Service, the supplier MUST:

Submit a detailed project plan to demonstrate the proposed activities and tasks to be undertaken (and their associated resource allocations) to meet proposed delivery timescales;

- Detail support the supplier will require from the trust;
- Detail support the supplier will require from the existing supplier;
- Detail the impact on existing trust infrastructure;
- Provide timescales for the migration;
- Describe how legacy data stored in private DICOM attributes can be mapped into an appropriate public attribute during migration (where a public tag exists that should have been used in the first place);
- Describe how legacy data not stored in the DICOM (for example, annotations and measurements) can be migrated;
- Provide method and examples;
- NOT require a protracted break in Service during transition. The timescale will be agreed with the trust, but is likely to be less than 8 hours; and
- Provide a cost breakdown for the migration.

5.7.3 The supplier MUST support the migration of data from their Service to a replacement Service if required at the end of the contract.

5.7.4 As part of migration into the replacement Service at the end of the contract, the supplier MUST:

- Submit a detailed project plan to demonstrate the proposed activities and tasks to be undertaken (and their associated resource allocations) to meet proposed delivery timescales;
- Detail support the supplier will require from the trust;
- Detail support the supplier will require from the replacement service supplier;
- Detail the impact on trust infrastructure;
- Provide timescales for the migration;
- Describe how private DICOM tags will be dealt with including the management of private tags and any other proprietary metadata. Suppliers are required to provide details of the method and examples;
- NOT require a protracted break in Service during transition. The timescale will be agreed with the trust, but is likely to be less than 8 hours; and
- Provide a cost breakdown for the migration.

6 Service management

This section sets out the Service Management requirements needed to perform the Service. Suppliers SHOULD describe how they will meet each of the requirements.

6.1 Availability management

6.1.1 The supplier MUST measure the availability of the Service; it will be measured against a target to be defined by the trust and agreed between the trust and the supplier. The supplier MUST be able to demonstrate the capability to manage a Service to the standard of availability experienced by the NHS today.

Good practice example 1:
The present LSP products perform to a minimum of 99.87% availability, defined as when End Users are able to access and utilise the functions of that Component System.

In March 2011 the Service achieved between 99.22% and 99.98% availability.

6.1.2 The supplier MUST monitor the availability of the system and SHALL provide the results of such monitoring to the trust via a mutually agreed time and format.

Good practice example 2:
Provision of unplanned downtime date in minutes on a weekly basis. From this weekly % availability can be calculated.

The supplier will measure the availability of the Service provided and will ensure a minimum availability of the target agreed with the trust measured across all sites over all business days in any calendar month. Any period of downtime previously agreed with the supplier by the trust will not count towards the calculation of this Service level with the exception of emergencies.
6.1.3 The supplier MUST describe how system availability is determined, specifically where no live transactions are being processed.

Availability SHOULD be measured in accordance with the following formula:

Where:

\[
\text{Service availability} \% = \frac{(MP - SD) \times 100}{MP}
\]

Where:

| MP | Total number of minutes, excluding planned maintenance up to a maximum of *trust to complete* |
| SD | Total number of minutes of Service downtime, excluding planned maintenance. |

6.1.4 The supplier MUST detail their approach to resilience in the case of failure of system components, storage and/or database systems.

6.1.5 The Service MUST tolerate hardware failure with zero data loss and remain operational with minimal interruption in alignment with agreed SLA availability targets.

### 6.2 Performance management

In response to the following requirements, the supplier MUST state any assumptions, particularly those concerning minimum infrastructure requirements especially local, remote and wide-area connectivity.

6.2.1 The supplier MUST ensure that the Service proposed is scalable to meet increases in numbers of users, and volumes whilst maintaining SLA’s. It MUST also be capable of dealing with the following occurrences:

- The handling of peak workloads of twice the average daily throughput in one day and key peaks of activity throughout the working day; and
- To repeat any scheduled or unscheduled backups during the day without interruption to the normal operation of the Service.

6.2.2 The supplier MUST describe how it will monitor and measure its SLAs.

6.2.3 The supplier MUST state their definition of a full load and provide details of how this will be calculated, including any assumptions on the following:

- Number of concurrent users;
- Concurrent user activities;
- Network traffic;
- Available network bandwidth;
- Service resilience;
- Study sizes;
- Concurrent applications open on the workstation / “enterprise class” trust PC;
- Concurrent applications executing on the workstation “enterprise class” trust PC;
- Workstation / “enterprise class” trust PC specification; and
- Workstation / “enterprise class” trust PC location.

6.2.4 The supplier MUST outline arrangements for the trust to be able to reduce or increase its assets and retire or add to equipment SHOULD the trusts situation change.

6.3 Hosted communications infrastructure

The following requirements are effective where all or part of the Service is hosted at an offsite data centre:

6.3.1 The supplier MUST provide details of the location/s of the data centre/s to the trust.

6.3.2 All hardware associated with elements of the Service that are hosted MUST reside in a secure data centre/s.

6.3.3 Patient identifiable data MUST not leave the secure data centre/s other than by the Service.

6.3.4 The Service MUST withstand penetration testing carried out by an independent agency that is a member of CREST and CHECK.

6.3.5 The hosting provider SHOULD be compliant with ISO27001 security management standards for this Service and provide the trust with <regular> reports. Reporting periods to be agreed with the trust. Compliance should be externally certified.

6.3.6 The hosting provider MUST complete the IG Statement of Compliance (IGSoC) before Service commencement.

6.3.7 The supplier MUST ensure that data is not altered during transmission.

6.3.8 The bandwidth of the connection to the data centre MUST be sufficient to accommodate workload estimates (bandwidth, latency, packet loss and jitter). The supplier MUST demonstrate the calculation used to assess workload and study estimated size, and ensure no significant delay in the transmission of data.

6.3.9 The supplier MUST explain how the Service will operate in the event of a communications/network failure/WAN congestion and endpoint failure. This SHOULD include:

- Communication integrity – transport failure during the receiving and sending of data; and
- Communications processes for repeating the send and receive function following communications failure.

6.3.10 The supplier MUST describe their approach to enabling end-to-end security for all patient identifiable data when in transit.

6.3.11 The supplier MUST describe how they intend to integrate their Disaster Recovery plan with the trusts Business Continuity plan in the event of a disaster at the trust which affects the Service.
6.3.12 In response to the Hosted Infrastructure requirements the supplier MUST consider how the Service complies with the following standards:

- ISB 0160, Patient Safety Risk Management System – Deployment and Use of Health Software;
- ISB 1512, Information Governance Standards Framework; and
- ISB 0086, Information Governance Toolkit.

6.4 Service provision and management requirements

6.4.1 The supplier SHOULD adhere to the trust’s Service management processes.

6.4.2 The supplier MUST align its processes in relation to this Service to ISO20000 Service management standards and provide access to the trust for audit purposes.

6.4.3 The supplier MUST monitor and measure its Service and provide detailed evidence that the supplier is monitoring the Service against agreed SLAs.

6.4.4 The supplier MUST proactively monitor the systems, Services, performance and capacity provided and will ensure that the trust is alerted to any issues or failure according to agreed SLAs.

6.4.5 The supplier MUST implement any changes to the Service required by relevant legislation and / or Information Standards Notes (ISNs – formerly DSCNs) by the date specified within the ISN or legislation, This MUST be at no additional cost to the trust either in terms of increased charges, development, additional licence fees, implementation, support or any other basis what so ever.

6.4.6 The supplier MUST provide Service critical upgrades as part of the maintenance and support agreements. The supplier MUST ensure all software is at least current version \(<\text{minus 1}>\) i.e. not later than the last supported version from the software vendors.

6.4.7 The supplier MUST upgrade the system (including but not limited to hardware) in the event that a software upgrade has the potential to or adversely affects the Service response or availability. The supplier MUST declare their policy with respect to the cost to the trust of meeting the Service levels.

6.4.8 The supplier MUST indicate the expected life span of the Service, its components and indicate technical refresh milestones.

6.4.9 The supplier MUST provide comprehensive audit reports that include (but are not limited to) the following items: user ID, date and time, workstation and transaction (including Accession Number / exam identifiers and patient identifiers where patient data has been changed). Person/Patient Identifiable Data MUST only leave, (i.e. be copied or exported) the Service through an auditable Service.

6.4.10 The supplier is required to detail their approach to Disaster Recovery in case of the loss of the Service a) at the trust or where all or part of the Service is hosted at a datacentre, b) at the data centre. The supplier SHOULD state the lead time; dependencies and cost of restoring services.

6.4.11 The Service MUST provide restricted access to the audit trails generated by the Service. These SHOULD be easily readable and be capable of being downloaded in standard formats, accessible by the trust.
6.4.12 The Service MUST be self monitoring and raise alerts of errors detected, and issue them through standard communication channels. The supplier SHOULD describe how these alerts are passed to external (e.g Trust owned) systems management tools.

6.4.13 The supplier MUST monitor Service and resource usage and provide real-time display of usage patterns and statistics to the trust. This data is to be available to approved users only. The Service MUST also provide flexible reporting to enable reports to evolve over time with no requirements for code modification.

6.4.14 The supplier MUST produce an annual:

- Capacity Plan;
- Business Continuity and Disaster Recovery Plan;
- Availability Plan;
- Updated Release Policy; and
- Updated Change Policy.

6.4.15 The supplier MUST produce a quarterly Release Plan.

6.4.16 The supplier MUST produce a monthly:

- Service Level Report; and
- Forward Schedule of Change.

6.4.17 In response to the Service Management Requirements, the supplier MUST describe how the Service complies with the following standards:

- ISO20000;
- Current ITIL Guidance;
- MOF; and
- COBIT.

6.4.18 The supplier SHOULD describe their support arrangements, including levels of support, key personnel, typical qualifications and experience of staff at each of those levels and whether each support level is UK-based or offshore.

6.4.19 The supplier SHOULD also detail:

- Security clearance status of staff accessing patient-identifiable information;
- Whether or not offshore staff will have remote access to UK-held patient-identifiable data; and
- Arrangements for checking previous convictions / security clearance of staff based in offshore jurisdictions, where they differ materially from practice in the UK.

6.5 Service levels

6.5.1 The Service is required to be supported 24 hours a day, 7 days a week including all Public Holidays.

6.5.2 The supplier MUST provide a maintenance schedule to the trust and MUST have an agreed set of Service Level Agreements (SLAs).
6.5.3 The supplier and trust MUST agree performance bands for the Service, and the associated definitions.

**Good practice example 3:**

The table below provides an example of the Service levels for fix times, agreed under the present LSP contract:

<table>
<thead>
<tr>
<th>Details of Service Level: Fix Times for Severity 1 Service Failures.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>OSL</td>
</tr>
<tr>
<td>FL1</td>
</tr>
<tr>
<td>FL2 (Critical Service Level)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Details of Service Level: Fix Times for Severity 2 Service Failures.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>OSL</td>
</tr>
<tr>
<td>FL1</td>
</tr>
</tbody>
</table>
6.5.4 The definitions of the Severity Levels taken from the present LSP contract are below:

| Severity 1 Service Failure | A Service Failure which, in the reasonable opinion of the allocating party (whether the Contractor, the Authority or an Authority Service Recipient) has the potential to:
have a significant adverse impact on the provision of the Service to a large number of End Users; or
have a significant adverse impact on the delivery of patient care to a large number of patients; or
cause significant financial loss and/or disruption to the Authority, an Authority Service Recipient or an Authority Party; or
result in any material loss or corruption of Authority Data, or in the provision of incorrect Authority Data to an End User. Non-exhaustive examples: |

| FL2 (Critical Service Level) | > 18 hours | 130 apportioned in accordance with the formula as outlined in Appendix 7 paragraph 7.2 |

| OSL | < 7 days | 0 |
| FL1 | 7 days – 10.5 days | Sliding Scale pro rata from 0 to FL2 level |
| FL2 | > 10.5 days | 60 apportioned in accordance with the formula as outlined in Appendix 7 paragraph 7.2 |

| OSL | next available scheduled maintenance release | 0 |
| FL1 | < OSL | 20 apportioned in accordance with the formula as outlined in Appendix 7 paragraph 7.2 |
| Loss of power to data centre causing failure of Services;  
Clinical data for a patient being displayed with demographics for another.  
Total loss of Service or an unusable core PACS or RIS function at the Entity level (Core PACS functions are: acquisition, exam and report display and report closure) |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity 2 Service Failure</strong></td>
</tr>
</tbody>
</table>
| A Service Failure which, in the reasonable opinion of the allocating party (whether the Contractor, the Authority or an Authority Service Recipient) has the potential to:  
have a significant adverse impact on the provision of the Service to a small (i.e. one or more) or moderate number of End Users; or  
have a moderate adverse impact on the delivery of patient care to a significant number of End Users; or  
have a significant adverse impact on the delivery of patient care to a small (i.e. one or more) or moderate number of patients; or  
have a moderate adverse impact on the delivery of patient care to a high number of patients; or  
cause a financial loss and/or disruption to the Authority, an Authority Service Recipient or an Authority Party which is more than trivial but less severe than the significant financial loss described in the definition of a Severity 1 Service Failure.  
Non-exhaustive examples:  
Corruption of any standing data tables e.g. prescription code list.  
One physical location of the NHS staff who are authorised End User’s are unable to access the Service  
Total loss of Service or an unusable core PACS or RIS function at the level of department within an Entity (Core PACS functions are: acquisition, exam and report display and report closure) |
| **Severity 3 Service Failure** |
| A Service Failure which, in the reasonable opinion of the allocating party (whether the Contractor, the Authority or an Authority Service Recipient) has the potential to:  
have a moderate adverse impact on the provision of the Service to a small (i.e. one or more) or a moderate number of End Users; or  
have a minor adverse impact on the provision of the Service to a large number of End Users; or  
have a moderate adverse impact on the delivery of patient care to a small (i.e. one or more) or moderate number of patients; or  
have a minor adverse impact on the delivery of patient care to a large number of patients.  
Non-exhaustive examples: |
As an example, the number of LSP responsible High Severity Service Incidents (HSSI) Levels 1 and 2 raised against PACS Services, during the week ending 22nd May 2011 was 6.

In the preceding 28 day period, the total number of LSP responsible HSSI’s logged were 37.

6.6 System maintenance

6.6.1 The supplier MUST submit all requests for change, to the trust in writing for approval and in alignment to an agreed Change Policy between both parties. All such communication is to be made within the agreed change management notice period.

6.6.2 The supplier MUST maintain a rolling maintenance schedule with mutually agreed impact on Service performance/delivery and mutually agreed scheduled downtime.

6.6.3 The supplier MUST carry out both routine maintenance and planned maintenance to the Service throughout the term of the contract in accordance with the maintenance schedule and in alignment with the agreed SLAs and Change Policy.
6.6.4 Where the supplier needs to carry out any planned maintenance to the Service, which will impact the availability of the Service, the supplier MUST ensure they notify the trust within agreed timescales and in alignment to the agreed Change Policy.

6.6.5 The supplier MUST carry out any emergency maintenance required. This might be either at the trust’s written request or on its own volition if the supplier is aware of a need.

6.6.6 The supplier MUST give as much notice as is reasonably practicable to the trust’s nominated Service owner prior to carrying out any emergency maintenance and in alignment to the agreed Change Policy.

6.6.7 Where the supplier undertakes either planned or emergency system changes a clear regression path must be available and documented and MUST be in alignment with the agreed Change Policy.

6.6.8 The supplier MUST indicate via their technical design/technical roadmap documentation the expected life span of the Service and its components.

6.6.9 The supplier MUST outline how they manage and record configuration status, including status of security patches / Service Packs for operating system and / DBMS components.

6.7 Response times

6.7.1 The supplier MUST define the Service response times for Service performance and agree these with the trust.

**Good practice example 4:**

**Transaction Type A:** A PACS Workstation displaying the first 20 search results out of a predefined query resulting in a maximum of 300 matches from the local PAS database. Display time SHALL be measured from the time the End User completes the selection of the query (e.g. worklist selection) until the 20th result is visible on the display device.

Target: 90% within 2 seconds and 99.9% within 10 seconds.

**Transaction Type B:** the display of the first image from a study where the study is stored on local storage.

Target: 95% within 3 seconds and 99.9% within 10 seconds.

6.7.2 The Service MUST support the access to and the processing/manipulation and display of imaging data, including 3 Dimensional rendering techniques, at the clinical user’s interface within:

< trust to define target times, for example [x%] within [x] seconds and [y%] within [y] seconds >.

6.7.3 The supplier MUST monitor response times aligned to and including SLA targets and SHALL provide the results of such monitoring to the trust via real time dashboards and daily / weekly / monthly reports.

6.7.4 Where a portion of the response time is outside the supplier’s direct control (e.g. while transiting N3) the supplier MUST describe how this portion of the response time is determined and accounted for.

6.8 Severity levels

6.8.1 The supplier MUST allocate a severity level to a reported Service failure. The supplier MUST provide details of their severity levels and the associated definitions. This SHOULD include examples of the severity level attached to common problems such as:
- Loss of DICOM Modality Worklist to all modalities;
- Loss of DICOM Modality Worklist to percentage of modalities;
- Modalities being unable to store images to PACS;
- Loss of web-viewing capability / enterprise image viewing outside of radiology;
- Loss of web-viewing capability / enterprise image viewing capability for recently acquired exams;
- Loss of Service:
- Loss of messaging; and
- Unable to authenticate new users.

6.8.2 The supplier will commit to fixing faults and issues within the agreed SLAs for each severity level.

6.8.3 The supplier MUST be clear in their proposal which areas of the system/solution they are responsible for and which they are not, also how they will deal with issues that occur at the “boundaries” of systems and as a result of interface failures.

**6.9 Fix times**

6.9.1 The supplier MUST provide proposed fix times for each of the proposed severity levels.

6.9.2 The fix time for each Service failure MUST be measured from the time the Service failure report is received by the suppliers service desk until the time the Service failure is resolved. The fix time will be confirmed with discussion and agreement from the trust.

**6.10 Problem management**

6.10.1 The supplier MUST provide the proposed fix times for any identified problems including RFC dates agreed with the trust.

**6.11 Service desk**

6.11.1 Suppliers SHOULD describe their approach and mechanisms to fault reporting and management - email, phone, minimum dataset needed, only accepting calls from particular individuals e.g. system admin/helpdesk.

6.11.2 The supplier MUST provide a Service Desk to support the Services and will be required to rectify faults reported.

6.11.3 A Service Level Agreement (SLA) MUST be entered into between the trust and the supplier in order that standards can be set for enquiry resolution and hand-off of calls.

Standards SHALL be as follows:

- Calls receiving an automated response or placed into a queuing system SHALL be deemed not to have been answered; and
- Call answer times: the following measurements SHALL be made each day, from the time the phone commences ringing to the time an advisor answers it, including any interactive voice response time:
- The measurement below is applied to the LSP solution but will be tailored by the trusts:
Call answer time > 90% of calls to be answered within < 20 seconds and >98% to be answered within <60 seconds.

- Trusts are to insert/agree local values as required:
  - <trust to insert value>, at least <trust to insert value>; and
  - <trust to insert value>, at least <trust to insert value>.

Call fix times: calls MUST be prioritised according to agreed criteria. Calls SHALL be graded from <trust to insert value>. The issues raised MUST be resolved within the times agreed with the trust:

- Severity 1: maximum of <trust to insert value>
- Severity 2: maximum of <trust to insert value>
- Severity 3: maximum of <trust to insert value>
- Severity 4: maximum of <trust to insert value>
- Severity 5: maximum of <trust to insert value>

Suppliers are invited to provide their own targets for trust review.

6.11.4 The Service Desk MUST provide advisors with the means to securely and accurately:

- Provide technical support;
- Catalogue the enquiry;
- Record caller contact details;
- Schedule and manage call back;
- Initiate management information;
- Validate caller identity; and
- Set / clear / monitor outstanding work.

6.11.5 The supplier MUST provide the trust with a documented Service support model, identifying the main procedures, including the procedures for passing calls on to other relevant parties.

6.11.6 Supplier MUST confirm that all 'back-to 'back' support arrangements are sufficient to ensure that the supplier can still meet their SLAs should they pass responsibility for the (partial) resolution of a service incident (e.g. service desk hours and fix times).

6.11.7 The supplier MUST provide the means to register, track and manage calls from initiation to resolution. Call histories MUST be retained for the contracted length of the Service. Access SHOULD be provided to allow users to track their call”s progress online.

6.11.8 The Service Desk MUST provide the means to handle and escalate complaints.

6.11.9 The Service Desk MUST provide the means for advisors to receive up to date information on known faults with any aspect of the Service to enable information to be quickly passed on to callers.

6.11.10 Advisors MUST record and update appropriate level of details for resolution and transfer of calls within their own Service Desk systems, for example:

- Name;
- Address;
- Daytime contact: telephone and / or pager;
- E-mail address;
- Enquiry type (option to categorize e.g., technical subsets or free text);
- Action taken;
- Preferred reply medium;
- Date expected to be resolved;
- Free text facility; and
- Advisors may not view any patient information on the Service.

6.11.11 Faults reported by Service users or detected by the supplier MUST be logged on a single system and given a unique reference number.

6.11.12 An electronic interface SHOULD be provided to allow incidents to be logged online.

6.11.13 The capture, retention and management of PID MUST comply with trust and national standards on the protection of patient information and the Data Protection Act and other relevant regulations and legislation. This includes processing of third party data.

6.11.14 The service desk MUST permit outbound voice calls to landline numbers and mobiles.

6.11.15 The Service MUST allow email correspondence in relation to faults and their resolution.

6.11.16 The system used in the Service Desk MUST automatically capture, record and report upon Service operation with appropriate management information, including the number and percentage (if appropriate) of:

- Actual and mean call duration;
- Actual and mean time to answer a call;
- Actual and mean time taken to resolve a call;
- Advisor occupancy;
- Call volumes by call type;
- Calls abandoned;
- Calls abandoned after x seconds (where x may be varied by the trust);
- Calls answered;
- Calls answered within n seconds (banded);
- Calls not in the language of preference;
- Calls offered (e.g. all calls made whether answered or not forecast and actual);
- Calls queued for advisors in real time; and
- Calls resolved at first point of contact.
6.11.17 The Service Desk MUST provide a single contact point for all enquiries by telephone and email. An automatic acknowledgement MUST be issued within a reasonable time of receipt as agreed with trusts, and a unique reference enquiry number MUST be issued, to be used if the Service user requires follow up of the enquiry.

The target response time presently experienced by trusts is > 90% within < 3 minutes and > 95% within > 3 minutes but less than 5 minutes.

6.11.18 The Service Desk call number MUST NOT be chargeable at more than local rates.

6.11.19 The Service Desk SHALL only be required to receive calls in English.

6.11.20 The Service Desk MUST comply with the requirements of the Disability Discrimination Act.

6.11.21 The Service Desk MUST provide access for the hard of hearing, using telephone-based communication systems.

6.11.22 The Service Desk SHOULD provide the capability for users to log non-priority calls on-line with the ability to attach images and documents in support of both new calls and existing cases. Service users SHOULD be able to view the progress of logged calls and to provide additional information to the supplier.

6.12 Service failure log

6.12.1 The supplier MUST ensure that all Service failures are logged on the Service Failure Log and SHALL ensure that the trust has verification rights in relation to the Service Failure Log.

6.12.2 Where the Service Desk receives more than one report of a Service failure then all such reports MUST be logged on the Service Failure Log (but for the avoidance of doubt, the first report SHALL be deemed to be the Service Failure Report).

6.12.3 The supplier MUST describe the details which will be recorded in the Service Failure Log in respect of each Service failure.

6.13 Escalation

6.13.1 The supplier MUST describe the escalation process in respect of any ongoing failure level.

6.14 Resolving service failures

6.14.1 The supplier MUST be responsible for resolving Service failures in alignment with agreed SLAs.

6.15 Performance reporting and performance review

6.15.1 The supplier MUST commit to measuring and monitoring the operation of the Service. It MUST collect data that will enable the Service to be accurately, efficiently and effectively monitored.

6.15.2 The supplier MUST provide Service level reports at the end of each reporting period for the purposes of review, agreement and sign off between both parties. This will be agreed with the trust, but is normally monthly.

6.15.3 The supplier MUST maintain a Continual Service Improvement Plan (CSIP) which forms part of a monthly Service Review.
6.16 Additional considerations

6.16.1 Service deployment over third party thin client SHOULD be supported.

6.16.2 The supplier SHOULD be open to receipt of both Requests for Change (RFC) and Change Control Notifications (CCN) from the trust regarding the Service and be SHOULD willing to impact assess these against the Service.

6.17 System configuration and monitoring

6.17.1 During the lifetime of a system, system administrators may seek information regarding the intended behaviour or advice about a recommended pattern of use/configuration to support change of usage. Suppliers are invited to suggest a mechanism by which this can be addressed.

6.17.2 The supplier SHOULD provide access to/ or copy of the Service asset and configuration management database for periodic audits <to be agreed by both parties>.

6.17.3 The supplier MUST provide a Service Request model to facilitate non functional changes to the Services, such as adding a new user.

7 Standards

In response to the requirements, the supplier MUST demonstrate how the Service complies with the following standards, by providing an electronic copy of the Declaration of Conformity for the product(s) the supplier intends to supply, along with electronic copies of their ISO 9001 or other certifications referred to onto that Declaration.

7.1 Safety standards

The supplier will state how the Services will comply with the following safety standards:

7.1.1 Products MUST bear the CE mark in accordance with the Medical Devices Directorate (93/42EED). The CE mark SHOULD include four-digit number of the Notified Body who accredits the Quality Management System and comply with all relevant European and/or British safety standards.

7.1.2 The supplier SHOULD provide electronic versions of the Declaration of Conformity applicable to the products they intend to supply and any other certificates (ISO 9001) to which the Declaration of Conformity refers.

7.1.3 All items MUST comply with the relevant UK standards including current health and safety legislations, details of which SHOULD be listed. These MUST include:

- NHS ME Guidelines HSG (91)11 – Patient Dose Reduction – Purchasing Radiology Equipment;
- Ionising Radiation Regulations 1999 & MDGN (2000) and amendment SI 2006/2523;
- IRMER - Ionising Radiation (Medical Exposure) Regulations 2000;
- Department of Health Document TRS89 “Technical requirements for the Supply and Installation of equipment for diagnostic imaging and radiotherapy (1989)”;
- The particular requirements for safety set out in BS 5724; Specification for the Safety of Medical Electrical Equipment 1979;
- Current Health and Safety Legislation;
- Current IEE Regulations; and
Current EMC Regulations for Medical equipment.

7.1.4 Confirmation MUST be given that equipment offered is CE marked and conforms to MDD and MDR.

7.1.5 All equipment MUST be user friendly with clear identification of all controls which are to be marked with standard IEC symbols.

7.1.6 Service providers SHOULD be aware of Health and Safety legislation (Health and Safety at Work Act 1974) with regard to manual handling and their responsibility to provide equipment that minimises the risk of injury to staff.

7.1.7 Additional regulations that SHOULD be considered are:

- The Manual Handling Operation Regulations 1992;
- The Management of Health and Safety at Work Regulations 1999;
- The Health and Safety (Display Screen Equipment) Regulations 1992; and

7.2 Imaging standards

7.2.1 The Service MUST adhere to DICOM 3.x, HL7 2.x, HL7 3.x IHE and their successors, to enable interoperability of multiple vendors’ equipment in a network environment.

7.3 Integrated Healthcare Enterprise (IHE)

7.3.1 The supplier MUST provide as part of the response to this document IHE Integration Statements for all of its products and, in particular, their compliance with the IHE Standard Radiology Profiles and the date that these were tested and proven.

7.3.2 The Service SHOULD support the appropriate elements of the following IHE Radiology Profiles <trust to amend as required>

- Workflow:
  - PIR, Patient Information Reconciliation;
  - PWF, Post-processing Workflow;
  - RWF, Reporting Workflow;
  - IRWF, Import Reconciliation Workflow;
  - PDI, Portable Data for Imaging; and
  - SWF, Scheduled Workflow - Modalities (as acquisition modality actor), RIS (as departmental system scheduler actor) and PACS (as Image Manager & Image display) MUST all support the Scheduled Workflow Profile of IHE.

- Content:
  - NM, Nuclear Medicine Image;
  - MAMMO, Mammography Image;
  - ED, Evidence Documents; and

- Presentation:
PACS, RIS, image archive and sharing services. Core statement of requirements.

- KIN, Key Image Note;
- CPI, Consistent Presentation of Images;
- PGP, Presentation of Grouped Procedures; and
- FUS, Image Fusion.
- Infrastructure:
  - XDS-I, Cross-enterprise Document Sharing for Imaging;
  - TCE, Teaching File and Clinical Trial Export;
  - ARI, Access to Radiology Information;
  - ATNA, Audit Trail and Node Authentication (ATNA) – Radiology Option; and
  - CHG, Charge Posting.
- The Service SHOULD additionally support the following profiles:
  <trust to add as required>

7.4 Information Standards Board (ISB) Standards

7.4.1 The supplier MUST provide as part of the response to this document a conformance table for all of its products and, in particular, their compliance with the below Information Standards Board (ISB) standards and the date that these were tested and proven.

<table>
<thead>
<tr>
<th>Standard number</th>
<th>Standard title</th>
<th>Current release</th>
<th>Link to documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISB 1500</td>
<td>Common User Interface - Address Input and Display</td>
<td>DSCN 01/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1502</td>
<td>Common User Interface - Date and Time Input</td>
<td>DSCN 02/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1503</td>
<td>Common User Interface - Date Display</td>
<td>DSCN 07/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1504</td>
<td>Common User Interface - NHS Number Input and Display</td>
<td>DSCN 03/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1505</td>
<td>Common User Interface - Patient Banner</td>
<td>DSCN 09/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1506</td>
<td>Common User Interface - Patient Name Input and Display</td>
<td>DSCN 04/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1507</td>
<td>Common User Interface - Sex and Current Gender Input and Display</td>
<td>DSCN 05/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1508</td>
<td>Common User Interface - Telephone Number Input and Display</td>
<td>DSCN 06/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1501</td>
<td>Common User Interface - Time Display</td>
<td>DSCN 08/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 0103</td>
<td>Diagnostics Waiting Times and Activity Data Collection</td>
<td>DSCN 09/2009</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 1556</td>
<td>Digital Imaging and Communications in Medicine (DICOM)</td>
<td>Amd 153/2010</td>
<td>Documentation</td>
</tr>
<tr>
<td>ISB 0070</td>
<td>Healthcare Resource Groups (HRG)</td>
<td>DSCN 17/2008</td>
<td>Documentation</td>
</tr>
</tbody>
</table>
8 Image archive requirements

This section of the Core Requirements has been added at a later date, subsequent to the issue of Version 1 (5th August 2011). The Image Archive and Enterprise Sharing requirements MUST therefore be applied with the General Imaging Requirements (sections 3.1 – 3.55) and the Non Functional Requirements, as appropriate (sections 4.1 – 7.4).

8.1 Overview

The Image Archive is primarily focused on providing organisations with a cost effective alternative to the continued storage, locally, of studies where there is limited clinical value of having fast access for ongoing care management. While the age and criteria for moving studies off local storage will be a local decision there is significant evidence that less than 5% of studies older than 13 months are ever viewed again (Laurence Sutton, The Image Data Sharing and Storage Steering Group Chair); and that for those studies that are reviewed, this forms part of a managed care provision where reviews are planned and pre-fetch or web viewing is a viable method to ensure images are available at the required time.

It is assumed that images stored within the Image Archive will be available to share with other health organisations; however, the Image Archive will NOT provide an immediate sharing method.

- The Image Archive will therefore provide:
- Connectivity via the N3 network;
- A DICOM interface to allow trusts to store and retrieve imaging data;
- A HL7 interface to allow trusts to provide demographic updates for their stored imaging data;
- A web portal that allows trusts to view audit reports, configure their service polices and provide Web Access to DICOM Persistent Objects (WADO) access;
- Comprehensive security management that provides authentication, authorisation and audit of all access to the Service by end users and end systems;
- Comprehensive enterprise management that monitors all aspects of service operation;
- Information lifecycle management that allows trust level policies for data retention and compression to be locally defined;
- Provision of long-term, reliable, secure and cost-effective storage for image data by the use of storage tiering and storage virtualisation; and
- Non-sharing access to data, but can be integrated with Sharing Services.

**Figure 1: Image archive functionality**

Distinct from the Image Archive requirements are a set of Sharing Service requirements that define Image Sharing Services that which health organisations may choose to use in conjunction with an Image Archive OR independent of an Image Archive. The intention is that Image Archives and Sharing Services should be interoperable so that a health organisation could use an Image Archive from one supplier and Sharing Services from a different supplier.

The Sharing Services will therefore provide:
● Connectivity via the N3 network;

● A XDS/XDS-I registry and repository. The repository can be used to store imaging data independently of an Image Archive if required. The registry can be used to index imaging data within the service repository and any other external repositories and stores, including other Image Archives;

● A Master Patient Index (MPI) using NHS PDS;

● A web based DICOM viewer to view imaging data indexed by the registry;

● A DICOM transform function to “tag morph” imaging data indexed by the registry before ingestion by external systems;

● Comprehensive security management that provides authentication, authorisation and audit of all access to the Service by end users and end systems, as for Image Archive, but with the addition of XDS federation and control of data sharing through NHS IG controls; and

● Comprehensive enterprise management, which monitors all aspects of service operation, as for Image Archive.

9 Image archive services

9.1 Key general service requirements

9.1.1 The Image Archive MUST provide long term data storage.

9.1.2 The Image Archive MUST be usable by more than one trust concurrently, with each trust’s data logically separated.

9.1.3 The Image Archive MUST provide a set of Services which provide a “minimum necessary service” for image archiving, such as the storage of data, making data available to a registry, providing audit and management functions.

9.1.4 The Service costing model MUST be based on a “utility pricing” model.

9.1.5 The Service MUST allow trusts to change their local PACS solution with no impact on the availability or accuracy of data held in the Image Archive.

9.1.6 The Image Archive SHOULD provide a set of Sharing Services, above those supplied as the „minimum necessary services”, which allows a trust to „add” functionality where they have appropriate business requirements. These additional sharing Services SHOULD be independent of the Image Archive so that a trust could can decide to use just the Additional Sharing Services and not the Image Archive.

9.1.7 The Image Archive SHOULD provide merging and reconciliation of stored data if two or more Trusts who use an Image Archive merge as health organisations.

9.1.8 The supplier MUST define whether or not their Service or elements of the Service are considered to be a medical devise.

9.2 Functional requirements

Storage service

9.2.1 The Service MUST provide a managed storage infrastructure on which the imaging data and other service operation information, such as audit and management data, are placed.
9.2.2 The storage subsystems used MUST be reliable and resilient to hardware and software failures. <The exact reliability requirements for the Image Archive will be for trusts to determine>.

9.2.3 The Service MUST be flexible enough so that as technologies progress and change over time, it can cope with those changes without any impact on service levels.

9.2.4 The Service MUST provide scalable storage of medical data for the life of the Service without loss. <The exact volume requirements for the Image Archive will be for the trusts to determine>.

9.2.5 The Service MUST be backed up; backup in this case means a separate copy of any online or offline storage contents, to include image data, metadata and audit data in a separate, geographically dispersed location.

9.2.6 The Service SHOULD support the use of different types of tiered physical storage to optimise storage costs against the required performance.

9.2.7 Physical storage MUST comply with open standards for connectivity.

9.2.8 Stored patient identifiable data MUST be encrypted to the NHS Cryptographic standards.

9.2.9 The Service SHOULD provide suitable tiered storage management software that provides the mechanism to move data between storage tiers.

9.2.10 Tiered storage management SHOULD run automatically at regular intervals, defined by the supplier, without human intervention.

9.2.11 Hashes SHOULD be used to ensure integrity of files stored within the storage tiers.

9.2.12 It SHOULD be possible for supplier administrators to temporarily override the automatic tiered storage management for operational purposes.

9.2.13 All tiered storage management SHOULD be fully audited in line with the requirements documented in the PACS RIS Core Statement of requirements in section 4.5.

9.2.14 The Service SHOULD provide storage virtualisation. Storage virtualisation refers to the provision of an abstraction layer between the requesting servers and the storage components themselves.

9.2.15 The storage virtualisation layer SHOULD permit the migration of data between heterogeneous storage appliances with no interruption of service to end users.

9.2.16 The storage virtualisation layer SHOULD be used to optimize utilisation by ensuring that the multiple file systems supporting the individual application components that make up the Service can be managed onto a small number of individual storage components.

9.2.17 Storage virtualisation SHOULD be delivered outside of the server infrastructure delivering the Service.

9.2.18 Storage virtualisation SHOULD be provided as “in-band”. In-band storage virtualisation means that the flow of data to and from the storage subsystem all passes through a virtualisation appliance.

9.2.19 Storage virtualisation SHOULD be integrated with the chosen Enterprise Management solution.

9.2.20 DICOM data MUST be stored as received, as specified in part 10 of the DICOM standard.
9.2.21 DICOM standard transfer syntax MUST be used.

9.2.22 All database schemas and structures MUST be open, accessible and documented and made available to the trust when requested, for example to support data migration and system integration.

9.2.23 All changes to DICOM data and metadata MUST be versioned so that a complete history of versions is held by the Service.

9.2.24 The Service MUST support DICOM standard PS3.4 Annex I (Media Storage) and Annex S (media creation).

9.2.25 Information stored by an individual trust MUST be logically separated and independent from information stored by other trusts. Therefore many trusts SHOULD be able to store information with the same identity, for example UID for study, totally independent of each other.

**DICOM Interface Service**

9.2.26 The DICOM interface Service MUST provide integration of the Service with external DICOM consumers and producers for both receiving and sending DICOM objects.

9.2.27 The Service MUST support the Storage Service Class as defined in the DICOM standard PS3.4, Section 5 and SHOULD support storage of all Information Object Definitions (IOD) defined in the DICOM Standard PS3.4, Annex A. Suppliers MUST list any Annex A IODs which the Service will not support for storage.

9.2.28 The Service MUST support Storage Commitment as defined in DICOM Standard PS3.4, Annex J.

9.2.29 The Service MUST also support the following Service Classes from PS3.4 of the DICOM standard:

- Annex C: Query/Retrieve;
- Annex N: Softcopy Presentation States; and

9.2.30 The Service MUST support non-blocking access to data stored.

9.2.31 All DICOM objects MUST be stored “as-is” with no changes or manipulations to content.

9.2.32 The Service MUST provide DICOM WADO.

9.2.33 DICOM connection MUST be made using virtualised TCP/IP addresses that are recorded in an N3 DNS entry.

9.2.34 The Service MUST be easily extensible to allow new imaging transport protocols such as the Medical Imaging Network Transport (MINT) to be added in the future.

9.2.35 All DICOM messages sent and received MUST be logged for audit and service management purposes.

9.2.36 The Service MUST provide the ability to delete DICOM data.

**HL7 Interface service**

9.2.37 The HL7 interface Service MUST provide integration of the Service with external HL7 message consumers and producers for both receiving and sending HL7 messages.
9.2.38 The Service SHOULD provide a HL7 message translation service that allows HL7 message formats and contents to be changed internally within the Service, so that external systems can talk to the Service in their local dialect of HL7. This SHOULD be implemented as a message broker within the Service.

9.2.39 The HL7 interface MUST support HL7 versions from 2.3 up to 2.7.

9.2.40 The HL7 interface MUST be used by the Service to update demographic information stored within the archive.

9.2.41 All HL7 messages sent and received MUST be logged for audit and service management purposes as defined in PACS RIS Core Statement of requirements section 4.5.

9.2.42 All demographic information updates MUST be logged for audit and service management purposes as defined in PACS RIS Core Statement of requirements section 4.5.

**Connectivity service**

9.2.43 The Service MUST be connected to N3, or its successor NHS network.

9.2.44 The network connection MUST be resilient so that it is always available.<Trust to define level of resilience>.

9.2.45 N3 is considered to be a “private but not secure” network; therefore all network connections between trusts and the Service MUST be secured.

9.2.46 The Service MUST support IPv4.

9.2.47 The Service MUST support IPv6.

9.2.48 All externally visible IP Service addresses MUST be virtual IP addresses that are mapped to physical network addresses within the Service. The external virtual network addresses MUST be a configuration item within the Service.

9.2.49 All Service externally visible IP addresses MUST be registered with the NHS DNS.

9.2.50 The Service MUST support Secure Socket Layer / Transport Layer Security (SSL/TLS). Valid server certificates (bound to the fully qualified domain name (FQDN)) will therefore be needed.

9.2.51 The Service MUST support IPsec for application protocols that cannot use SSL/TLS.

9.2.52 The Service MUST detect, alert and manage “denial-of-service” (DoS) attacks.

9.2.53 N3 usage MUST be fully monitored and reported. Configurable capacity alert triggers MUST be provided. On exceeding a trigger an operational alert MUST be generated. Usage data collected MUST be decomposable by:

- End-Point or Client IP; and
- Archive Service.
- Monitoring data for the rolling last 12 months MUST be retained.

9.2.54 N3 connection availability MUST be fully monitored and reported. Configurable availability alert triggers MUST be provided. On exceeding a trigger an operational alert MUST be generated. Monitoring data for the rolling last 12 months MUST be retained.

9.2.55 An N3 capacity model MUST be maintained that, based on historical monitoring data, allows the supplier to maintain suitable bandwidth to keep the Service operational.
9.2.56 The Service MUST support unpredicted usage demands by either standards based QOS or a bandwidth throttling process that can selectively degrade or enhance network throughput and response for specific End-Points and archive services.

9.2.57 The Service MUST provide functionality to schedule and control throttling at the application level.

9.2.58 The Service MUST provide functionality to schedule transfers, e.g. Out of Hours.

9.2.59 The Service SHOULD provide functionality within the application to prioritise specific transfers; prioritised transfers SHOULD be identifiable at network/QoS level.

9.2.60 The Service MUST provide functionality to differentiate between image request and transfer traffic at a network/QoS level, e.g. transaction and bulk types.

9.2.61 The supplier MUST provide evidence of the Service working in a WAN environment.

9.2.62 The supplier MUST provide bandwidth, latency, jitter requirements per QoS level for data centre/s and small, medium and large endsite/s.

9.2.63 Volumetric data references MUST differentiate between both active and concurrent users and explain how these are derived.

9.2.64 Volumetric data referenced MUST clearly state the length of any sample periods provided.

9.2.65 The supplier MUST provide maximum, minimum and average transmission times per image type.

9.2.66 The supplier MUST provide a monthly report per trust which includes RX/TX for total bandwidth, image type, maximum, minimum and average transmission times.

**Information lifecycle service**

9.2.67 The Service MUST support storage of both compressed and uncompressed data.

9.2.68 The Service MUST support compression and decompression of data to be transported.

9.2.69 The Service MUST support file and block based compression/decompression transfer syntaxes.

9.2.70 The Service SHOULD support the following compression transfer syntaxes:

- JPEG Lossless;
- JPEG Lossy (basic – 8 bit);
- JPEG Lossy (extended – 12 bit);
- RLE (lossless run length);
- JPEG 2000 (lossless);
- JPEG 2000 (lossy);
- JPEG LS;
- MPEG-2; and
- MPEG-4.
9.2.71 The Service SHOULD allow addition (in a plug and play method) of new compression transfer syntaxes.

9.2.72 All compression activity MUST be fully audited and retained as defined in PACS RIS Core Statement of requirements section 4.5.

9.2.73 The Service MUST manage data assets lifecycle states, which MUST include:

- Submitted;
- Updated;
- Approved;
- Deprecated;
- Un-deprecated; and
- Removed.

9.2.74 Within the image archive appropriate service behaviours SHOULD be controlled by a policy. A policy is defined as a set of imperative rules that define the actions to carry out based on a set of possible input values.

9.2.75 Policies SHOULD be definable for:

- Compression – compression format for different categories of data assets;
- Storage – storage location for different categories of data assets; and
- Retention – retention period for different categories of data assets.

9.2.76 A policy SHOULD be definable at a system level. The Service SHOULD provide a default set of policies at a system level.

9.2.77 A policy MUST be definable at individual trust level. A trust level policy SHOULD override a system level policy.

9.2.78 A web based policy designer tool SHOULD be provided that allows an authorised end user a means of easily and intuitively designing policy rules for their trust.

9.2.79 Where feasible, an industry standards based method of representing and presenting policy rules SHOULD be used.

9.2.80 All policy management activities MUST be monitored and fully reported.

9.2.81 The Service MUST provide appropriate master data and reference lists management to support operational aspects of the Service.

9.2.82 Master data SHOULD be sourced and kept synchronised from external providers.

9.2.83 Master data coding SHOULD adhere to standard code sets and coding formats mandated or approved by the NHS.

9.2.84 All changes to master data MUST be fully audited.

**Security service**

9.2.85 Refer to Section 4, para 4.4 Information Governance

**Management service**
9.2.86 The Service MUST provide a full enterprise management solution that both monitors the operational state of the Service and all its components and provides a comprehensive reporting service to users. This will monitor:

- Environmental services;
- Power;
- Network – LAN and WAN;
- Storage Network (where separate from the Network, otherwise managed as part of the LAN);
- Network services – time, name services, authentication services;
- Physical systems – servers, routers, switches, storage devices;
- Operating systems;
- File systems; and
- Application services, functions and components.

9.2.87 The enterprise management solution MUST be used pro-actively to ensure that the required levels of resilience, and hence availability levels are achieved.

9.2.88 The enterprise management solution MUST use an industry standard management protocol.

9.2.89 The enterprise management solution MUST provide suitable management agents (where applicable) for all hardware and software components used within the Service.

9.2.90 Any bespoke software components within the Service MUST be fully instrumented to provide both exception alerts and continuous performance monitoring compatible with the enterprise management solution.

9.2.91 All COTS components within the Service MUST be fully instrumented to provide both exception alerts and continuous performance monitoring compatible with the enterprise management solution.

9.2.92 The configuration and operation of the enterprise management solution SHOULD be from a web browser based console, which can if required be made available for access outside of the Service hosting environment for use by the supplier or authorised third party.

9.2.93 A web based service operational status dash board MUST be provided that displays in a concise presentation the real time values of the Service Key Performance Indicators (KPI). This should be accessible to the supplier, authorised third parties and trusts.

9.2.94 The Service MUST provide fixed parameterised reports for audit, capacity, availability and performance of appropriate functions of the Service. These SHOULD include:

**Audit reports**

- N3 connectivity;
- HL7 I/O;
- DICOM I/O;
- Tiered storage management;
- Authentication;
- Access control;
- Master data management;
- Policy management;
- Information lifecycle management; and
- Compression.

**Capacity reports**
- N3 connectivity;
- HL7 activity;
- DICOM activity;
- Tiered storage management;
- Physical storage;
- Master data management;
- Policy management;
- Information lifecycle management; and
- Compression.

**Performance reports**
- N3 connectivity;
- HL7 activity;
- DICOM activity;
- Tiered storage management;
- Physical storage;
- Master data management;
- Policy management;
- Information lifecycle management; and
- Compression.

**Availability reports**
- N3 connectivity;
- HL7 activity;
- DICOM activity;
- Tiered storage management;
- Physical storage;
- Master data management;
- Policy management;
Information lifecycle management; and
Compression.

A trust MUST only be able to report on their own activities within the Service.

9.2.95 Reports SHOULD be generated on-demand or as scheduled reports. Scheduled reports can be configured to be generated at specific times by the trust.

9.2.96 Reports MUST be created in both Excel and PDF format, which can be both viewed within the Service or downloaded via a web portal by authorised users.

9.2.97 The Service MUST keep a library of historical reports which can be accessed by authorised users. The library can be both browsed and searched. Only reports that the user is authorised to view and/or download will be visible within the library.

9.2.98 Historical reports within the library MUST be kept on-line for a configurable period of time. After this period reports must be archived but MUST be restorable to the library on request.

9.2.99 Historical “N3 utilisation” reports MUST be kept on-line indefinitely.

9.2.100 Historical “N3 availability” reports MUST be kept on-line indefinitely.

9.2.101 Authorised users MUST be able to subscribe to be notified of the availability of scheduled reports by email. The notification email will contain a URL to the report which can be viewed/downloaded from the Service web portal. Authorised users can also subsequently unsubscribe to any notification.

9.2.102 Ad-hoc reporting MUST be available to authorised users within a trust through a report writer application. This SHOULD allow a user to visually build report templates, store them for future use and/or amendment, and run them. The report writer SHOULD be web based and easily used from within the Service web portal.

9.2.103 Although there is currently no direct requirement for a Business Intelligence capability using an appropriately structured store (such as a multi-dimensional data mart/warehouse), bidders SHOULD indicate how the relevant information within the Service could be extracted, transformed and loaded into such a capability if required in the future.

9.2.104 Access to reports MUST be fully audited.

9.2.105 To support „utility pricing” functionality, the Service MUST support a billing management solution.

9.3 Non Functional requirements – image archive services

9.3.1 Data MUST be able to be kept for a period of not less than 30 years without loss.

9.3.2 Data MUST be recovered to the requesting system within 48 hours.

9.3.3 Storage virtualisation where used MUST not impact the performance of any other functions of the Service.

9.3.4 Tiered storage management where used MUST not compromise any other functions of the Service.

9.3.5 The Service SHOULD be scalable to support all NHS trusts in England concurrently using DICOM I/O.

9.3.6 The Service SHOULD be scalable to support all NHS trusts in England concurrently using HL7 I/O.
9.3.7 The capacity of the N3 connection for the Service SHOULD be scalable to support the capacity demands of all NHS trusts in England using the Service over N3 concurrently.

9.3.8 The Service SHOULD be scalable to support all NHS trusts in England concurrently defining and using policies.

9.3.9 Authentication MUST be robust and reliable.

9.3.10 Authentication sign on times MUST be within 3 seconds.

9.3.11 Authentication SHOULD be scalable to support 1,000 concurrent users.

9.3.12 Access control MUST be robust.

9.3.13 Access control permission checking times MUST be less than 0.5 seconds.

9.3.14 Access control SHOULD be scalable to support 1,000 concurrent users.

9.3.15 The audit process MUST not adversely affect the performance of the Service.

9.3.16 The enterprise management solution MUST not adversely affect the performance of the Service.

9.3.17 The production of reports MUST not have an adverse impact on the performance of the Service.

9.3.18 Service performance MUST be measured in terms of the speed and effectiveness of data transfer into and out of the Service, and the response time of end user and end-point interfaces. These SHOULD be measured in terms of the average and maximum response times for specified data volumes being transferred, both as upload data and results from queries.

9.3.19 The Service MUST handle system and data errors in a controlled manner. Input, output and system errors MUST not have a detrimental effect on system performance, availability or the integrity of data stored within the Service.

9.3.20 The supplier will be responsible for management and maintenance of the Service. This will include planned upgrades, performance/integrity checks, regular statistical reporting and the implementation of fault corrections. The Service MUST ensure that management and maintenance activities can be performed with a minimum of cost, in terms of time and effort required, and have no impact on the availability of the Service.

9.3.21 The Service SHOULD be designed with the „Greening Government ICT” agenda in mind, as documented in the Greening ICT paper, available from: http://www.cabinetoffice.gov.uk/resource-library/greening-government-ict

10 Sharing services

10.1 Functional requirements

Registry/repository service

10.1.1 The Service MUST provide a data registry that holds a master index of stored data and their associated metadata.

10.1.2 The data registry SHOULD hold references to data assets that are not stored in the Service. These external data assets SHOULD be stored in local or shared trust systems. The Service will have no control over these external data assets.

10.1.3 The data registry MUST ensure full data integrity.
10.1.4 The data registry MUST maintain explicit versions of all data items. If a data item is changed, the previous version must be maintained and a new version created.

10.1.5 Unless explicit reference is made to a version of a data item, all access to a data item MUST use the most current version.

10.1.6 For DICOM data items the data register MUST record as a minimum:
- Object name;
- Object size;
- Object owner;
- Object permissions (for instance read only, loss-less only);
- Object creation date;
- Object service ingest date;
- Object last referenced date;
- Object total references;
- Compression algorithm used ("none" being acceptable);
- Encryption algorithm used;
- Current Storage Tier;
- UID for study;
- UID for series; and
- UID of Service Object Pair (SOP) instance.

10.1.7 The data registry MUST allow references to external repository items.

10.1.8 The data registry MUST provide SOAP and HTTP bindings.

10.1.9 All data registry activities MUST be monitored and fully reported.

10.1.10 The Service MUST provide a data repository that stores all the data within the Service.

10.1.11 The physical storage and location of data both at a file and block level MUST be managed separately by the Storage Services. The data repository only provides a logical storage interface.

10.1.12 All data assets are considered to be discrete objects and as such MUST be logically stored as discrete entities within the data repository.

10.1.13 Logical and physical storage MUST be decoupled. Moving a data asset to a different location within physical storage MUST not change the logical location as recorded in the repository.

10.1.14 All data repository activities MUST be monitored and fully reported.

10.1.15 The Service MUST provide an XDS-b interface to allow external systems to act as both XDS-b consumers and providers.

10.1.16 The Service MUST provide an XDS-Ib interface to allow external systems to act as both XDS-Ib consumers and providers.
10.1.17 The Service MUST provide registry federation through XDS federation. This MUST include:

- Inter-registry Object References;
- Federated Queries;
- Local Caching of Data from Another Registry; and
- Object Relocation.

10.1.18 The Service MUST support membership of multiple federations.

10.1.19 The Service SHOULD provide a throttling and quota function that allows a system administrator as a configuration item to limit both the amount of outgoing and incoming federation operations between the Service and specific registry peers.

10.1.20 All federation activity MUST be monitored and fully audited.

**Patient index service**

10.1.21 The Service MUST maintain a Master Patient Index (MPI) for all data stored in the data repository and all data referenced by the data registry that resides in external trust systems or other external federated repositories/registries.

10.1.22 The common identifier MUST be verified NHS number.

10.1.23 The master source for NHS number MUST be verified NHS numbers from the Patient Demographic Service (PDS) from the NHS SPINE.

10.1.24 The service MUST support HL7 v3 NHS SPINE messaging to connect to PDS or its successor.

10.1.25 All NHS SPINE activities MUST be fully monitored and audited.

10.1.26 Updates to the MPI SHOULD be propagated, where appropriate, to associated data assets stored within the Service.

10.1.27 The Service MUST support the IHE PDQ profile.

10.1.28 All MPI activities MUST be fully monitored and audited.

**DICOM viewing service**

10.1.29 The Service MUST provide a diagnostic quality, web based DICOM viewer.

10.1.30 The DICOM Viewer MUST work with all mainstream web browsers.

10.1.31 The DICOM Viewer MUST provide server side rendering or streaming rendering. For the latter any web browser client streaming components MUST be compatible with the mainstream web browsers and their supported operating systems.

10.1.32 The DICOM Viewer MUST correctly interpret and present any DICOM object stored in the Service.

10.1.33 Where the DICOM Viewer cannot interpret a data element it MUST annotate this clearly in the presentation.

10.1.34 The DICOM Viewer MUST be capable of displaying one or more DICOM images using a variety of hanging protocols.

10.1.35 The DICOM Viewer MUST be capable of displaying all DICOM data including multi-frame Ultrasound, Angio Cine or any other imaging data that currently requires a non-radiology specialist viewer.
10.1.36 The DICOM Viewer MUST also support the display of reports and other unstructured data in various formats; such as PDF and JPEG files.

10.1.37 All DICOM Viewer activities MUST be fully audited.

**DICOM Transform service**

10.1.38 The Service MUST provide a DICOM Transform service, which is a means of transforming a DICOM object from one vendor’s DICOM format to a different vendor’s DICOM format (often termed DICOM tag morphing). The transformation MUST include all specific presentation states and overlays.

10.1.39 The Service SHOULD provide a web User Interface that is simple to use that allows an authorised user to setup a mapping from one set of DICOM tags to another set of DICOM tags.

10.1.40 A DICOM transformation SHOULD be invoked implicitly or explicitly.

10.1.41 An implicit DICOM transformation SHOULD be based on a DICOM end-point requesting a DICOM C-GET. The DICOM end-point can be registered with the DICOM transform service as understanding a specific vendor’s DICOM format, which implicitly invokes a DICOM transformation if required.

10.1.42 An explicit DICOM transformation SHOULD be based on an appropriate interface protocol that allows a DICOM end-point to:

- Directly query the available DICOM mappings;
- Request a transformation of a specific DICOM object using a specific DICOM mapping; and
- Get the transformed DICOM object.

10.1.43 DICOM mappings SHOULD be exportable and importable as XML files in a standard XML schema.

10.1.44 All DICOM transformation activities MUST be monitored and fully audited.

**Management service**

10.1.45 The Service MUST implement the management service requirements defined for the Image Archive Services.

10.1.46 The Service MUST provide additional fixed parameterised reports for audit, capacity, availability and performance of appropriate functions of the Service. These SHOULD include:

**Audit reports**

- DICOM transformation;
- DICOM viewing;
- Patient index;
- Data registry;
- Data repository; and
- Federation.
- Capacity reports
- Patient index;
- Data registry;
- Data repository; and
- Federation.
- Performance reports
- Patient index;
- Data registry;
- Data repository; and
- Federation.
- Availability reports
- Patient index;
- Data registry;
- Data repository; and
- Federation.

**10.2 Non functional requirements**

10.2.1 The Service SHOULD be scalable to support all NHS trusts in England concurrently using the data registry.

10.2.2 The Service SHOULD be scalable to support all NHS trusts in England concurrently using the data repository.

10.2.3 The Service SHOULD be scalable to support all NHS trusts in England concurrently using the XDS/XDS-I interface.

10.2.4 The Service SHOULD be scalable to support HL7 v3 NHS SPINE messaging for a fully populated MPI, i.e. potentially containing all known patients in England.

10.2.5 The Service SHOULD be scalable to support all NHS trusts in England concurrently using the MPI.

10.2.6 Data uploads and downloads to operational storage are likely to occur outside normal office hours, and search and discovery access may occur at anytime. Therefore the Service MUST provide continuous real-time access to authorised users within a trust for operational storage data uploads, downloads and queries.

10.2.7 The Service SHOULD be scalable to support all NHS trusts in England concurrently using the DICOM Viewer.

10.2.8 The Service SHOULD be scalable to support all NHS trusts in England concurrently using the DICOM Transform service.