Document filename: ITK Spine Mini Service – Common Client Requirements-v1.1.docx			
Directorate / Programme	HSCIC - Architecture	**Project**	Interoperability
Document Reference		HSCIC-ITK-ARCH-300	
Project Manager	N/A	**Status**	Final
Owner	George Hope	**Version**	1.1
Author	George Hope	**Version issue date**	18/12/2014

ITK Spine Mini Service – Common Client Requirements

Document Management

Revision History

Version	Date	Summary of Changes
1.0	22/07/2014	Draft version issued by HSCIC
1.1	18/12/2014	Amended requirement **MSCA-ORG-01** to generalise this document's Acceptable Use Policy reference, and to refer readers to AUP sections in related documents

Reviewers

This document must be reviewed by the following people: author to indicate reviewers

Reviewer name	Title / Responsibility	Date	Version
George Hope	ITK Architecture Lead	31/05/2014	1.0
Sanjay Paul	ITK Architect	31/05/2014	1.0
Richard Dobson	ITK Accreditation Manager	31/05/2014	1.0
David Barnet	ITK Communication and Messaging	31/05/2014	1.0
Nigel Saville	ITK Accreditation	31/05/2014	1.0

Approved by

This document must be approved by the following people: author to indicate approvers

Name	Signature	Title	Date	Version
Shaun Fletcher		Head of Architecture	31/05/2014	1.0
Rob Shaw		Director Operational Services	31/05/2014	1.0

Reference Documents

Ref no	Doc Reference Number	Title	Version
1	0405.04	0405.04 ITK 2.01 Additional Module Spine Mini Services Provider Requirements v2.1.pdf - (Deprecated)	2.1
2	0406.04	0406.04 ITK 2.01 Spine Mini Services Logical Interface Overview v2.1.pdf - (Deprecated)	2.1
3	0408.04	0408.04 ITK 2.01 Spine Mini Services Client Requirements v2.1.pdf - (Deprecated)	2.1

Note: The referenced documents that are marked as deprecated were used only to create this new document set shown as diagram in the section 1.2. Readers may not refer to those documents for any practical purposes.

Document Control:

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1 Introduction 4

1.1 Purpose of Document 4
1.2 ITK Documentation Set 4
1.3 Audience 5

2 High Level Overview 5

2.1 Level 0 view 5

3 Client Access Methods 7

4 Information Governance – Organisational 7

5 Information Governance – General 8

6 Audit 10

Appendix A – Detailed IG Compliance Requirements 13

1 Introduction

Spine Mini Services are a specification to enable suppliers of third party software to provide solutions that provide a greatly simplified interface for accessing a subset of Spine services. The intent is to thus lower the “barrier to entry” to the Spine.

This document forms part of the overall document set for the Interoperability Toolkit (ITK).

1.1 Purpose of Document

This document is a specification for the implementation of services that are expected to be provided by a Spine Mini Service Clients. There are also requirements in here for the design and assurance process. The implementation specification provides some requirements for some non functional behaviour of the SMSP as well as some guidance for implementation decisions.

Some of the requirements in this document will be assured using the Common Assurance Process and some will be assured using the ITK Accreditation process..

1.2 ITK Documentation Set

The position of this document in relation to the document set is shown below.

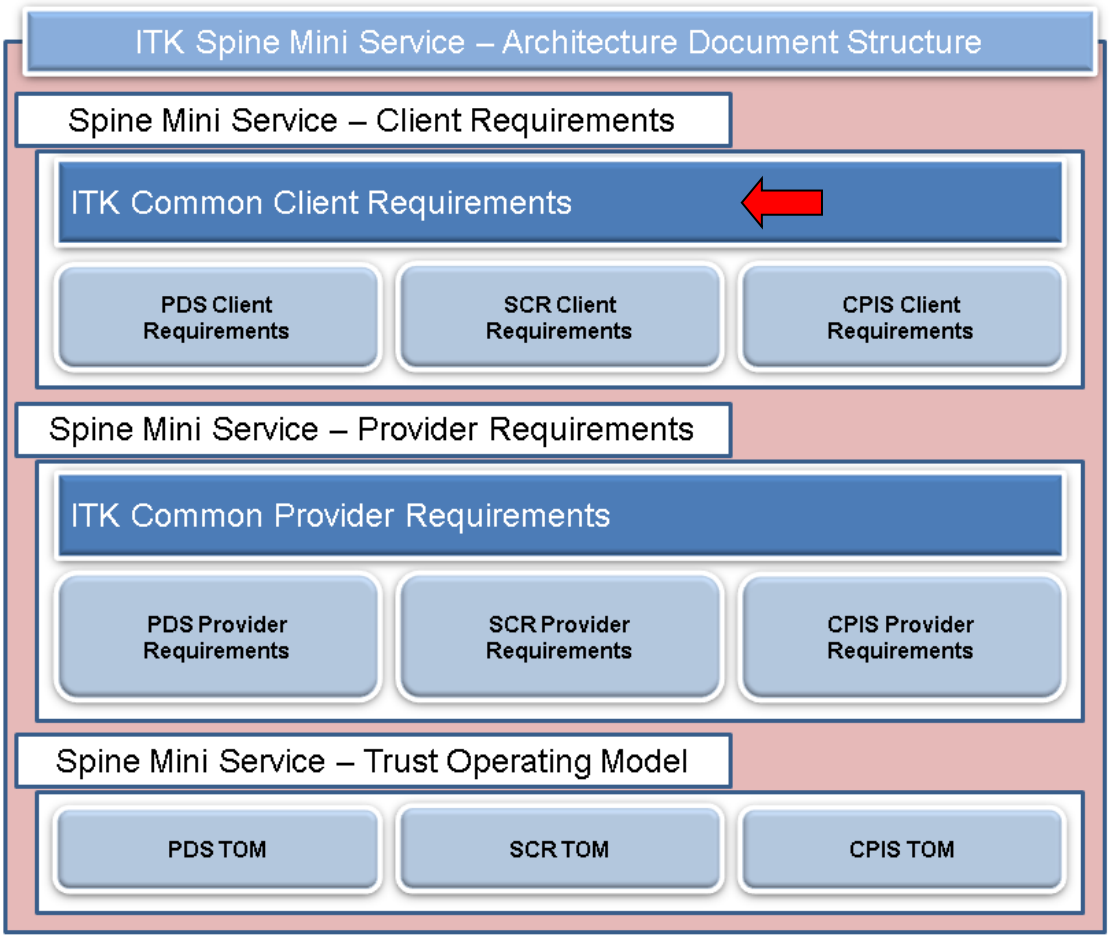

Figure 1 – The ITK Spine Mini Services Architecture Document Set.

1.3 Audience

The primary audience for this document are the developers (analysts, architects, developers) working on the ITK Component of the Spine Mini Service being developed. Within a Trust, the Project Manager and technical team will find the entire document set relevant.

These requirements are common/generic to all ITK Spine Mini Service Provider implementations.

2 High Level Overview

2.1 Level 0 view

A SMSP is an application which handles the complexity of dealing with the Spine TMS boundary yet provides a simplified interface to its clients. The complexity saving can be expressed both in terms of relaxed requirements for certain system calls and or syntactically and semantically more concise messaging.

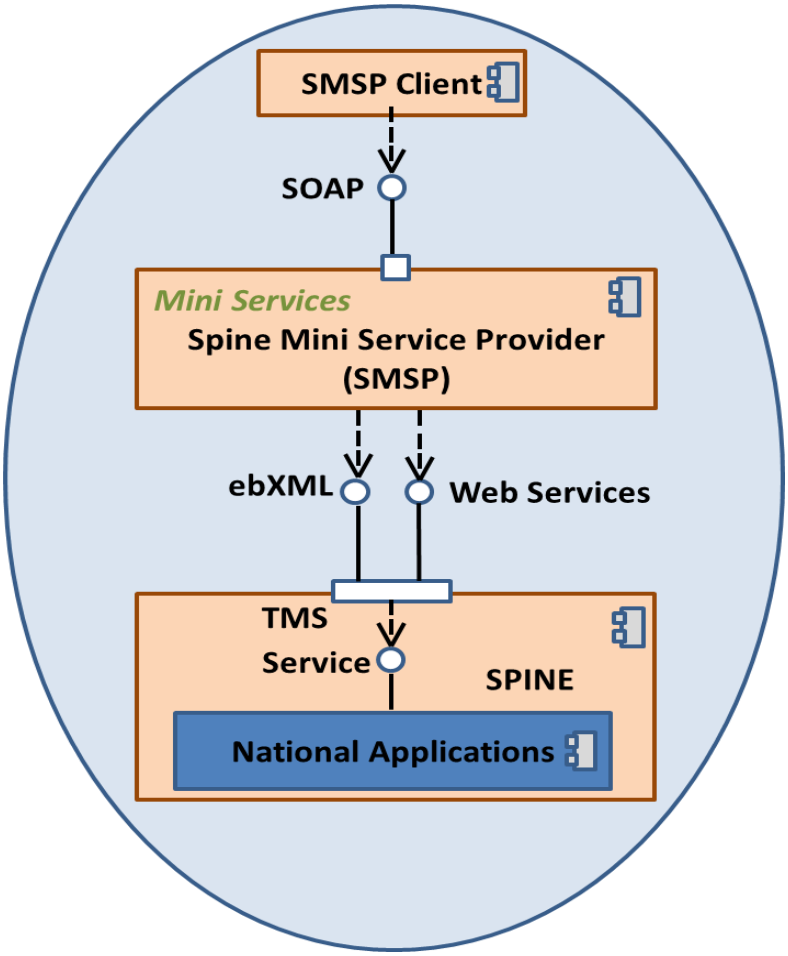

Figure 2: High Level view of an ITK Spine Mini Service

This version of this document is related to the appropriate ITK Mini Services Interface Specification document described in the Scope section.

A SMSP MAY (and indeed, in some cases MUST) provide internal business logic above and beyond simple adaptor logic (e.g. filtering, protocol translation etc.). The following sections in the document are logical groupings of related principles of the architecture of an SMSP that must be considered and have some additional requirements.

3 Client Access Methods

The type of connection Clients use when connecting to Spine Mini Service Providers is dependent on the National Service being accessed. That is PDS (Personal Demographics Service) requirements may be different to the requirements of SCR (Summary Care Record).

There are 4 types of connection:

1. **Unattended SMS Client Calls** –are not initiated by an individual, they are typically initiated by an automated function within software e.g. on admission into hospital a patient will be allocated a local identifier.
2. **Attended SMS Client Calls to SMS Provider – (Without Smartcard**) -In this case the ITK audit identity contains a SMSP provided code to identify the user. It is essential that this code is sufficient to uniquely identify the individual user involved, and that it is written to the SMSP audit trails to provide an end-to-end link from the spine bound call back to the local user.
3. **Attended SMS Client Calls to SMS Provider – (With Smartcard)** - In this case the ITK audit identity contains the Spine identity fields from the smartcard, identified by their standard OIDs, which are then passed through directly to be used in the Spine message. The User Role Profile ID and User ID MUST be provided, and the Role ID MAY optionally be provided.
4. **Attended SMS Client calls to SMS Provider Session Authenticated (With Smartcard)** - builds upon the previous attended access method with a Smartcard, but differs in that the spine mini service provider must authenticate the Smartcard session before calling spine i.e. ensuring the smart card is currently being used (inserted in the card reader) by the authorised user (with card pin code).

Each of the above methods has an impact on the ITK message structure and the ebXML message structure(s) when communicating with the Spine.

Details can be found in the Mini Service documentation associated with the National Service being accessed and the ITK Accreditation team can also provide further guidance.

4 Information Governance – Organisational

Ref	Description
MSCA-ORG-01	**The deploying organisation MUST conform with the Acceptable Use Policy for Spine Mini Services**
(1)	For individual domain-specific acceptable use policies, refer to relevant client specifications, e.g.: • PDS Client Requirements • CP-IS Client Requirements

MSCA-ORG-02	**The deploying organisation MUST put in place back-office data quality processes to handle any discrepancies which the use of Spine Mini Services reveal**
(1)	Spine Mini Services provide access to National Systems. This is likely to lead to discrepancies being discovered with local records. Back office data quality

	processes MUST be put in place to handle this, including: • Process for front-line staff to notify back-office of a potential discrepancy • Back-office investigation process to decide what to do • Back-office process to request an update to National Systems where necessary

MSCA-ORG-03	**The deploying organisation MUST consider the impact of rolling out Spine Mini Services on staff and job roles**
(1)	Typically the use of Spine Mini Services will increase the role of front-line staff in confirming that demographic details are entered correctly at the point of capture. Whilst this has many advantages, it is essential that any implications of this additional activity are considered, and any necessary training is provided. Piloting and a phased rollout would typically be used as part of this approach.

MSCA-ORG-04	**The deploying organisation MUST put in place a process for handling Subject Access Requests**
(1)	This may be needed in order to follow up on audit enquiries about use of Spine data. Note that where the SMSP is hosted by an external supplier, then this may include organising back-to-back agreements with the supplier regarding audit enquiries.

5 Information Governance – General

Ref	**Description**
MSCA-IG-01	**The Mini Services Client Application MUST provide RBAC control over access to its features**
(1)	The Mini Services Client Application MUST protect is functionality with RBAC controls sufficient to meet IG Requirements for a system accessing Spine data. This includes: • Implementing role-based access control to authorise users' access to the system's functions and data. • Restricting access to view audit trails • Protecting RBAC configuration data Note that the use of local RBAC is acceptable

NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA-IG-02	**The Mini Services Client Application MUST provide authentication control over access to its administration and other features**
(1)	Authentication MUST be based on a user identity which is then authenticated at least through the use of a separate password. • The use of two-factor authentication mechanisms (eg Smartcard) is encouraged but not mandated • Where passwords are used then password management processes and policy enforcement are essential. The guidance documentation referenced in the Trust Operating Model ("Password Policy for Non-Spine Connected Applications") therefore applies.
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA-IG-03	**The Mini Services Client Application MUST display basic security context information to the user**
(1)	This includes: • Computer misuse warning on start-up • Confirmation of the logged on user's current role and organisation
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA-IG-04	**The Mini Services Client Application SHOULD ensure appropriate labelling of personal data**
(1)	This includes protective labelling of personal data both on-screen and in printed output.
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA-IG-05	**The Mini Services Client Application MUST be hosted in a managed and secure environment**
(1)	The capability and responsibility of the deploying organisation, and acknowledgement of the risk ownership, is to be demonstrated through the maintenance of an approved IG Statement of Compliance (IGSoC1)

6 Audit

Ref	Description
MSCA-AUD-01	**The Mini Services Client Application MUST provide a secure audit trail**
(1)	The Mini Services Client Application MUST provide a secure, tamper-proof audit store sufficient to meet IG Requirements for a system accessing National Systems data. This includes protecting the audit store from deletion or modification, and ensuring that audit trails are enabled at all times. Audit data MUST be stored for periods as defined by DH policy and described in the NHS Records Management Code of Practice Parts 1 and 2. (see https://www.gov.uk/government/publications/records-management-nhs-code-of-practice)
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA- AUD-02	Events that MUST be audited
(1)	The Mini Services Client Application MUST audit all relevant events, sufficient to meet IG Requirements for a system accessing National Systems data. This includes: • All information exchanges with NHS CRS, including messages sent and received via Spine Mini Services • Changes to reference and configuration data • Successful login, unsuccessful login attempts and logouts, password changes
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA- AUD-03	Data Items that MUST be audited
(1)	The Mini Services Client Application MUST capture relevant data items in the audit store sufficient to meet IG Requirements for a system accessing National

	Systems data. This includes: • User Identity (see MSCA-AUD-04 below for more about what this must contain) • Timestamp (synchronised from the national time service) • Audit event details • Identity of associated data (e.g. patient's NHS Number) • A sequence number to help protect against tampering • The originating system identifier • Message ID of any messages sent to the Mini Services interface
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA- AUD-04	**The Mini Services Client Application MUST provide an Audit Identifier for the initiating user when calling Spine Mini Services**
(1)	The ITK Distribution Envelope provides an "Audit Identifier" field for the purpose of allowing the client application to pass an identity for the end user initiating the Mini Services request. • This Audit Identifier field MUST be populated by the Mini Services Client Application. • It MUST contain an ITK format of Audit Identity (see example below) • Additionally if an SMSP client system is smartcard enabled then the User Role Profile and User ID MUST both be supplied, and the Role ID MAY be supplied. • If the Mini Services Client Application is not smartcard enabled then an alternative local unique identifier for the user MUST be presented in the Audit Identifier field.
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic A typical itk audit identity may look like this. <itk:auditIdentity> <itk:id type="**2.16.840.1.113883.2.1.3.2.4.18.27**" uri=" **urn:nhs-uk:identity:ods:REC:localOrgID** " /> </itk:auditIdentity>
MSCA- AUD-05	**Audit entries MUST be available on a queryable interface**
(1)	The Mini Services Client Application MUST provide an interface for interrogating the audit log sufficient to meet IG Requirements for a system accessing National Systems data. Searchable parameters MUST include user identifier, Message ID, Patient ID, date/time.
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA- AUD-06	**The Mini Services Client Application MUST utilise a Stratum 3 time source as a minimum**
(1)	The Mini Services Client Application MUST utilise a Stratum 3 time source as a minimum however implementers SHOULD consider the use of Stratum 2 or above. This enables meaningful comparison and sorting of messages based on timestamps. It is particularly important to enable an end-to-end trace of events to be established all the way from the Mini Services Client Application, through the SMSP.
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

MSCA- AUD-07	**Audit timestamps generated by Mini Services Client Application MUST comply with issued guidance on time zones**
NB:	See Appendix (A) for full details of relevant IG Requirements on this topic

Appendix A – Detailed IG Compliance Requirements

MSCA-IG-01: The SMSP MUST provide RBAC control over access to its administration and other features

3.3.2	The system shall implement role-based access control to authorise users' access to the system's functions and data.
3.3.7	Where an Existing Systems Supplier is not required to support SSB authentication, the system shall 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. Those local RBAC mechanisms must: • Restrict users' use of the system to specific functions, assigned by the system manager(s) and only by the system manager(s); • Not allow any user access to their allocated functions until they have entered their user identity and password Access controls must include the ability to segregate access to the following functions: • Viewing the audit trail • Accessing inactive staff details • Accessing the records of patients that are not normally accessible to system users (for example in the case of GP systems, to the records of patients that are not currently registered at the practice)
3.3.8	The system shall ensure that, when stored locally, user profile information which supports RBAC mechanisms is protected from unauthorised access (including view, modify, or delete).
3.9.5	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. Suppliers 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.

MSCA-IG-02: The SMSP MUST provide authentication control over access to its administration and other features

3.15.2	Any local authentication should be based on a user identity which is then authenticated at least through the use of a separate password.

MSCA-IG-03: The Mini Services Client Application MUST display basic security context information to the user

3.1.11	The application shall prominently display the following message upon application start-up to remind users of their responsibilities and the legal constraints on the use of the system: Computer Misuse Act 1990 – Unauthorised access to this system is an offence Note that this wording may be updated from time-to-time.
3.1.12	The application shall make it possible for Users to validate the role and organisation relevant to the access they are being granted so as not to be able to claim ignorance of that role or organisation, or otherwise justify a lack of awareness of the significance of their actions.

MSCA-IG-04: The Mini Services Client Application MUST ensure appropriate labelling of personal data

3.17.1	The Supplier shall ensure that all Personal Data about a patient which are output from a healthcare application provided as part of this Agreement is labelled "NHS Confidential: Personal Data about a patient" and the Supplier shall also comply with such labelling requirements as may be reasonably specified by the Authority, e.g. to reflect changes in relevant legislation. Note that requirements in this section are not intended to affect the printing specifications for prescriptions or dispensing tokens as specified by the EPS requirements. Further guidance is available at: http://systems.hscic.gov.uk/infogov/security/risk
3.17.2	The Service shall provide for the protective labelling of information, which is required pursuant to this Section 3.17, to be made known to each User either: a) by being shown on any screen displaying the information; or b) by being displayed to the User upon logging into the system (for example as part of an acceptable use policy).
3.17.3	Where alternative (a) in Section 3.17.2 above is chosen, the Contractor shall ensure that the protective labelling of information is shown in a standardised location and manner on any screen displaying the information.
3.17.4	The Supplier shall ensure that the protective labelling of the information is shown in a standardised location and manner on any hardcopy output displaying the information.
3.17.5	The Supplier shall ensure that the system provides a means for users to check that hardcopy print-outs are complete (e.g. "page 3 of 5" annotations).

MSCA-AUD-01: The Mini Services Client Application MUST provide a secure audit trail

3.9.6	The system shall ensure that records in the audit trail can only be deleted by a privileged user under specific conditions; such as court orders. Note that such deletions are expected to be very rare, and it is important that access to such functionality must be stringently controlled. It must not be possible for any local user to have such rights as a matter of course, and it must not be possible for any local administrator to be able to grant such rights to any local user. Any attempts to manually update or add to the audit trail must be prevented as far as is practicable.
3.9.7	All Audit Trails shall be enabled at all times and there shall be no means for users to disable any Audit Trail.

MSCA-AUD-02: Events that MUST be audited

3.9.2	The exact nature of the data to be captured in the Audit Trails shall be sufficient to monitor whether access controls are operating as intended and to meet requests from patients as to who has accessed (eg displayed on-screen, printed, downloaded) or modified their Sensitive Personal Data or Personal Data, when and what was displayed / printed. The system shall also ensure that Audit Trails are kept which record information about all information exchanges with NHS CRS, including but not limited to: • All attempts to use an SSO Token ID to access to an application – including both successful and failed attempts. “use of a token” is interpreted to mean a call to the SSOTokenManagement API to validate a token. • All message interactions – sent and received • All interactions with the Spine SDS.

	Such Audit Trails shall provide a security record for use in analysing breaches of security and policy that may be used as evidence for use in disputes. A means of viewing or reconstructing any individual patient record as it was on any previous date must be supported.
3.9.11	Audit trails must include details of any configuration (e.g. a spine service being switched on) or reference data changes (e.g. an update to the clinical coding scheme data, drug databases) applied to the system.
3.9.15	Systems must ensure that outbound and inbound messages are tracked such that information in the audit trail can provide a complete end-to-end view of each transaction in terms of sent messages and received acknowledgments and responses.
3.15.4	Successful login, unsuccessful login attempts and logouts, password changes must be recorded in the system audit trail. Data to be included in such an audit trail entry: Successful login, logout: • User id • Date and time Unsuccessful login: • Number of attempts • Date and time • Access point (if available) • User id (if available) Password changes: • User id • User whose password was changed • Date and time **Such audit trail entries should also include end-user device (or system) identification information.**

MSCA-AUD-03: Data Items that MUST be audited

3.9.4	The Audit Trail records shall include the following minimum information: A record of the user identity. This is the User ID, Name, Role profile (including Role and Organisation) attribute values, obtained from the user's Session structure; A record of the identity of the authority – the person authorising the entry of, or access to data (if different from the user); The date and time on which the event occurred; Details of the nature of the audited event and the identity of the associated data (e.g. patient ID, message ID) of the audited event; A sequence number to protect against malicious attempts to subvert the audit trail by, for example, altering the system date. Audit trail records should include details of the end-user device (or system) involved in the recorded activity.

MSCA-AUD-05: Audit entries MUST be available on a queryable interface

3.9.3	The system shall provide facilities to allow Authorised Users (e.g. a Caldicott Guardian or privacy officer) to view Audit Trails and to analyse Audit Trails to allow the identification of all system users who have accessed or modified a given patient's records over a given period of time (such modification to include, for example, the archiving of a patient record in a GP system when that patient is no longer registered at the practice). All such access shall also be recorded in an appropriate Audit Trail. This is to support commitments made in the Care Record Guarantee. Such facilities to include the ability to display parts of the audit trail based on: patient id (normally expected to be the NHS Number), user id, authority id, date & time, sequence number.

* * * End of Document * * *