|  |  |  |  |
| --- | --- | --- | --- |
| Document filename: HSCIC-FNT-TO-TAR-0113.01 IG Requirements V4 - 0.92-TC | | | |
| Directorate / Programme | Programme and Service Delivery | Project | GPSoC |
| Document Reference | | HSCIC-FNT-TO-TAR-0113.01 | |
| Project Manager | Melissa Ruscoe | Status | Published |
| Owner | Danny Solomon | Version | 0.92 |
| Author | Danny Solomon | Version issue date | 19/09/2014 |

GPSoC IG Requirements V4

Document Management

Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Changes |
| V0.1 | 12 Oct 2012 | First draft – modified from “NPFIT-FNT-TO-TIN-0427.10 IG Requirements for ESP Systems v5.0” |
| V0.2 | 19 Oct 2012 | Addressed comments from MC, TT and BM (first internal review); clarifications for consistency, revised numbering mechanism. Distributed for wider review. |
| V0.3 | 4 Jan 2013 | Updated to final draft in response to comments from Dr Alan Hassey, Phil Walker and IST. Includes section on data annotation, suppression and deletion. |
| V0.4 | 22 Jan 2013 | For approval. Minor updates based on comments received on previous draft. |
| V0.5 | 25 Feb 2013 | For approval. Updated title and document reference. Clarification to requirement GP-IG-2.1-1. |
| V0.6 | 10 April 2013 | Updated following comments received from supplier community. |
| V0.7 | 15 April 2013 | HSCIC branding |
| V0.8 | 19 June 2013 | Significant revision to section 5. Other updates to reflect comments received. |
| V0.81 | 23 June 2013 | Minor updates following comments received. |
| V0.82 | 3 July 2013 | Update to GP-IG-3-12; revision to section 5. |
| V0.83 | 5 August 2013 | Clean version for ITPD. |
| V0.84 | 23 Sep 2013 | Corrected intra-document references. No content change. |
| V0.85 | 17 Nov 2013 | Updates following bidder comments. Includes RTM with categorisation of each requirement as either “Entry” or “Standard”. Removed section on security testing as that is now covered elsewhere in the contract. |
| V0.86 | 20 Nov 2013 | Final updates prior to being made available to bidders. |
| V0.87 | 6 Dec 2013 | Update to Section 4 to clarify scope. |
| V0.9 | 4 Feb 2014 | Clarifications to section 10 and section 12 around display of user details in the context of provenance data. |
| V0.91 | 15 Aug 2014 | Migrated requirement from Patient Services, see GP-IG-5-7 |
| V0.92 | 19 Sept 2014 | Added reference to HSCIC Good Practise Guidelines for of Information Security and Information Governance in section 14. |

Reviewers

This document must be reviewed by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer name | Title / Responsibility | Date | Version |
| Mike Curtis | GP IT Lead Technical Architect |  |  |
| Andy Dickinson | IG SME |  |  |
| James Wood | Head of Infrastructure Security |  |  |
| Dr Alan Hassey | Senior Clinical Advisor |  |  |
| Phil Walker | Information Governance & Standards Policy |  |  |

Approved by

This document must be approved by the following people:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title | Date | Version |
| Mike Curtis |  | GP IT Lead Technical Architect |  |  |
| Kemi Adenubi |  | GP IT Programme Director |  |  |
| James Wood |  | Head of Infrastructure Security |  |  |

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 5](#_Toc372729197)

[1.1 Information Governance 5](#_Toc372729198)

[1.2 Applicability 5](#_Toc372729199)

[1.3 Scope 5](#_Toc372729200)

[1.4 Definitions 6](#_Toc372729201)

[2 Authentication 8](#_Toc372729207)

[2.1 NHS Smartcards 8](#_Toc372729208)

[2.2 Local authentication 10](#_Toc372729209)

[3 Role-based Access Control 12](#_Toc372729210)

[4 Legitimate Relationships 15](#_Toc372729211)

[5 Information Sharing outside the practice 16](#_Toc372729212)

[6 Additional Privacy Controls within the practice 18](#_Toc372729213)

[7 Workstation Access Controls 19](#_Toc372729214)

[8 Content Commitment 20](#_Toc372729215)

[9 Data Labelling 21](#_Toc372729216)

[10 Provenance 22](#_Toc372729217)

[11 Data Annotation, Suppression and Deletion 23](#_Toc372729218)

[12 Audit 25](#_Toc372729219)

[13 Alerts 28](#_Toc372729220)

[14 Information Security 29](#_Toc372729221)

[14.1 Time-stamping 29](#_Toc372729222)

[14.2 Secure Storage 29](#_Toc372729223)

[14.3 Secure Transmission 30](#_Toc372729224)

[14.4 Network Access Controls 31](#_Toc372729225)

[15 Subject Access Requests 32](#_Toc372729236)

[16 Requirements Traceability Matrix (RTM) 33](#_Toc372729237)

# Introduction

*Information Governance:   
Getting accurate and up-to-date information to the right people,   
at the right time, at the right place – but nowhere else*

## Information Governance

This document provides the Information Governance (IG) requirements that define the controls that are needed to ensure that the significant quantities of sensitive personal data processed by GP clinical IT systems are kept confidential, are available to authorised users when required, and are accurate.

Information Governance is a key aspect of the Authority’s requirements for systems, reflecting for example the public commitments made under the Care Record Guarantee[[1]](#footnote-1) and the NHS Confidentiality Code of Practice[[2]](#footnote-2).

## Applicability

GPSoC systems and modules process considerable amounts of sensitive, personally identifiable information, and the requirements in this document are intended to provide controls over the processing and use of that data.

The requirements in this document apply to all GP IT systems: systems that, as an integrated product, provide clinical IT services to a practice, or separate systems that provide a specific set of functionality to a practice. In general, therefore, these requirements are applicable to:

* principal systems, providing core functionality to manage clinical records;
* interfaces exposed by principal systems to enable integration with subsidiary modules and systems;
* subsidiary modules and systems providing alternatives to modules provided by principal systems, or additional functionality.

However, there are some requirements that are only applicable to principal clinical systems; where this is the case, those requirements are marked “applicable only to principal systems”.

## Scope

This document defines a number of system-level controls, but does not describe processes and controls that system suppliers, as organisations designing, building and deploying systems, need to meet, or non-system processes within practices. The GPSoC Contractor Security Policy includes the definition of these latter controls (for example around the need for organisations to implement a robust Information Security Management System (ISMS), including the use of security penetration testing as part of their development processes).

This document presents Information Governance requirements around:

* Authentication – integration with Spine services to support the use of NHS Smartcards, and local authentication
* Role Based Access Control (RBAC) – for authorising access to system functions and data
* Legitimate relationships – ensuring there is a valid justification for a user’s access to specific patient records
* Controls around sharing of personal sensitive information about a patient outside the practice
* Additional privacy controls that allowing patients to exercise choice about the level of visibility of their records within the practice
* Workstation access controls – minimising the risk that information may be viewable on unattended workstations
* Content Commitment – allowing the electronic equivalent of ink signatures
* Data labelling – ensuring that outputs from the system are properly marked to reflect their sensitivity
* Provenance – ensuring that the source of all clinical data is appropriately recorded and accessible
* Data annotation, suppression and deletion – ensuring that the accuracy of the clinical record is maintained
* Audit Logging – ensuring that all system actions are recorded, and accessible, providing an important control against the mis-use of systems
* IT Security – time stamping, storage, testing, communications and access controls
* Subject Access Requests

## Definitions[[3]](#footnote-3)

"personal data" means data which relate to an individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

"sensitive personal data" means personal data including but not limited to information as to:

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Typically, the Personal Demographics Service (PDS)[[4]](#footnote-4) holds personal data, whereas clinical systems for use in general practice hold sensitive personal data.

Where used in this document, the words “must” (or “shall”), “should” (or “recommended”) and “may” are to be interpreted as described in Schedule 2.1.

Note that Section 16 contains a Requirements Traceability Matrix (RTM) that includes, for each requirement, its categorisation as either “Entry” or “Standard”.

# **Authentication**

## NHS Smartcards

|  |  |
| --- | --- |
|  | Systems MUST support the use of NHS Smartcards, by integrating with the Spine SSB, Spine SAML service and the locally-deployed Identity Agent, as described in detail in this section, or as separately published by the Authority. |
|  | When a practice user carries out any system functionality that directly initiates a call to any Spine service, or causes information from the Spine to be displayed to the user, then that user must be authenticated using their Smartcard. |
|  | Any access to personal data or sensitive personal data within practice systems SHOULD be subject to NHS Smartcard authentication, and MUST be subject to authentication at least to standards described in section 2.2. |
|  | Systems shall ensure that, where users have been issued with an NHS Smartcard, those users are able to carry out all system activities (subject to their access rights) using Smartcard authentication, without the need for any additional authentication. |
|  | To allow for occasions when the Spine SSB service may be temporarily unavailable or inaccessible, the system MUST provide an alternative authentication mechanism. This mechanism SHOULD make use of the NHS Smartcard, relying on cached authorisation information, allowing users to continue to use their Smartcard and Passcode as normal. Such cached authorisation information shall expire after a fixed period of 14 days (or as separately agreed with the Authority) following the most recent SSB-based authentication. Systems MAY use the LAC (Local Authentication Component) available through the Authority for this purpose.  Suppliers will be aware that any fallback mechanism that relies on a local authentication mechanism where users will need a separate set of credentials (for example as described in section 2.2) will need to take into account (i) the irregularity of any SSB unavailability or inaccessibility and (ii) the need for passwords to periodically expire as described in GP-IG-2.2-3. |
|  | A fallback mechanism as described in GP-IG-2.1-5 that makes use of the NHS Smartcard must continue to provide access to available Spine services as well as local services, during the period of its use. Any other fallback mechanism must not provide access to Spine services, and mechanisms must be put into place to ensure that any Spine interactions that would otherwise normally be carried out are completed, once full SSB authentication becomes available. |
|  | The system shall integrate with Spine Security Broker mechanisms for notification of:  Session Timeout  Smartcard Removal  When notified of a Session Timeout event, the system will provide for a mechanism of allowing the user to re-authenticate and immediately return to their previous activity. However if the user does not respond within a defined period (to be configurable to be set as defined by the Authority, default being 2 minutes) then the system will lock as defined in requirement GP-IG-12-10, although without requiring any additional user action.  When notified of a Smartcard Removal event, the system will immediately lock as defined in requirement GP-IG-12-10, although without requiring any additional user action.  The system shall do this by registering a Token Listener (See External Interface Specification[[5]](#footnote-5) and GP-IG-2.1-8 in this document for further information).  Note that the session timeout values are set by the Authority and may be changed from time to time. |
|  | SSO Token Listener  To detect when a User’s session ends, as described above in GP-IG-2.1-7, the system must ‘listen’ for SSO Token events.  The Spine Security Broker (SSB) SSOTokenListener interface provides a mechanism for applications that need notification when an SSO token expires. The token will expire if it reaches its maximum session time, or maximum idle time, or if an administrator terminates the session.  The system shall invoke the addSSOTokenListener method using the SSOToken interface; this method implements the SSOTokenListener interface. A call-back object will be invoked when the SSO token expires. Using the SSOTokenEvent (provided through the call-back), the system can determine the time, and the cause of the SSO token expiry.  In the destruction of the Session Token, the SSB invokes the registered call-back. The call-back is a HTTP POST request that transmits XML data to a servlet in the system; the system receives the HTTP Post and uses the information contained therein to take action as appropriate. |
|  | The system shall provide a mechanism to link a user’s Smartcard to their user record within the system. As a minimum this shall include the SDS UserID but may include other IDs (e.g. role profile IDs) if required. The assignment of a SDS ID shall be through a restricted access system function and shall be done programatically (see pseudo code below). All such assignments shall be recorded in the appropriate system audit trail. Removal or change of such assignments shall similarly only be accessible through a restricted access function and all records of the change shall be recorded in the appropriate system audit trail.  Actors  Operator – person using the system who will assign a new Smartcard to a system user  User – the person whose (new) Smartcard is being linked to their user record in the system  Pre-condition  The operator must have access to the secure Smartcard assignment function. They should be authenticated by SSB, otherwise must be authenticated locally.  BEGIN  IF operator is authenticated by SSB THEN BEGIN  Prompt Operator to remove their Smartcard  Allow Operator to continue using system (i.e. do not log Operator out because they have removed their Smartcard or because a token listener event message is received because of this Smartcard removal)  END  Prompt for User’s Smartcard to be inserted  User authenticates themselves (entry of PIN)  IF authentication successful THEN BEGIN  System retrieves the SAML assertion and programmatically extracts the SDS user ID and any required RoleProfileIDs  If appropriate, the operator should select any required RoleProfileIDs for storage  System stores the SDS User ID and any required RoleProfileIDs  END  IF operator was authenticated by SSB THEN BEGIN  Prompt Operator to insert their Smartcard and reauthenticate  Allow Operator to continue using system  END |
|  | Users whose Smartcard is not recorded on the system (see previous requirement) can only use local authentication and will not therefore be allowed access to system functions for which Smartcard access is required. |
|  | Periodically (at least every 30mins, but no more frequently than every 10 minutes, or to a frequency separately agreed with the Authority) the application shall check for the presence of the local ticket to ensure an authenticated smartcard remains present, unless the application is performing a valid exception in allowing the smartcard to be removed for receiving another smartcard. |
|  | 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:  Access to this computer/system and any information it contains is limited to authorised users only.  Legal action may be taken against unauthorised use of, or unauthorised access to, this computer/system and/or any information it contains, including pursuant to the Computer Misuse Act 1990.  If you are an authorised user, by proceeding to access and use this computer/system and/or the information it contains, you are accepting any terms of use, notices and policies which are contained or referenced within it or which have otherwise been drawn to your attention as an authorised user.  Note that this wording may be updated from time-to-time. |
|  | The application shall make it possible – by clearly and continually displaying the user’s name, role and organisation – 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. |
|  | All activities associated with requirements in this section must be recorded in the system audit trail. Such audit trail entries should also include end-user device (or system) identification information. |

## Local authentication

|  |  |
| --- | --- |
|  | The system MAY provide a local authentication model to provide an alternative method of authentication for users who do not wish to use NHS Smartcards. No access to Spine services can be available for users authenticated in this way. |
|  | Any local authentication MUST be based on a unique user identity which is then authenticated at least through the use of a separate password. |
|  | Local authentication MUST satisfy the password strength and password management requirements set out in “Password Policy for Non-Spine Connected Applications”[[6]](#footnote-6) |
|  | Where passwords are stored in system databases, they MUST be stored salted and hashed, using algorithms and strengths recommended in “Approved Cryptographic Algorithms Good Practice Guideline”[[7]](#footnote-7). |
|  | Successful login, unsuccessful login attempts, logouts and 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 (to the second)   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. |
|  | New users MUST be automatically assigned a system generated password matching password-strength requirements. |
|  | Upon first use of the system by the new user using local authentication, they MUST be required to set their own password. |
|  | Password-reset facilities must be provided; the system must store additional information associated with each user so as to allow newly-generated passwords to be provided securely to devices previously known to be associated with the user (such as mobile number or NHSmail email address). Any such newly-generated passwords must not be made visible to system-administration staff, and following first use of such passwords, the user MUST be required to set their own password. |

# **Role-based Access Control**

|  |  |
| --- | --- |
|  | Role Based Access Control (RBAC) is used to control user access to system functions; it determines which areas of system functionality individual users are authorised to access, based upon their business needs.  All systems must implement RBAC to authorise a user’s actions, based upon his/her authenticated identity. Where a system provides SSB-supported authentication, the specific RBAC requirements relating to the national RBAC model that are provided in this section apply.  Where a system provides local (non-SSB) authentication, RBAC controls are still required, but will be provided using local mechanisms.  Where a user has a registered NHS Smartcard but retains credentials for local authentication, there can be no greater rights associated with their local credentials (to avoid any incentive to bypass strong RA and authentication processes).  The nationally-defined list of Job Roles and Activities – together with the harmonised mapping of Job roles to Activity Baselines – is documented in the National RBAC Database (NRD)[[8]](#footnote-8). This represents the “reference data” that supports the Spine-supported RBAC, and as such will be updated from time to time by the Authority. This reference data information is also available on the SDS. For an overview and further guidance in this area, see “IG Guidance Note for ESP Suppliers – RBAC” NPFIT-FNT-TO-IG-DES-0159.  Members of Registration Authorities are responsible for registering users and providing NHS Smartcards, and for assigning User Role-Profiles to those users: details of organisation, Job Roles, and, where necessary, individual Activities that may be appropriate for those users.  These assignments are communicated through User Role Profiles which are stored as part of the *People* branch of the Spine Directory Service.  The structure and attributes of a role profile are defined in the Spine *External Interface Specification* (EIS) [[9]](#footnote-9)  Applications are responsible for authorising user access to functions based upon information obtained from the user’s allocated User Role Profiles.  Applications must grant access to application functions on the basis of Activities (also known as Business Functions) identified implicitly (through the baseline policy) and explicitly through additional Activities in a URP.  Applications are responsible for maintaining a local cache of baseline policy reference data in order to map Activities to Job Roles.  Access MUST NOT be granted on the basis of Job Role alone.  All Activities must be mapped to a consistent set of underlying Application Functions based on the description of the Activity.  One Activity may include the functionality of one or more other Activities, i.e. access rights can be granted in a hierarchy. This hierarchy is mapped explicitly in the NRD.  Where the user has multiple Role Profiles, s/he selects one to be used as the default profile for the login session. When initiating a particular application, a user may select a different profile to use with that application.  The interfaces provided by the Spine to access user profile information are defined in the Spine *External Interface Specification* (EIS). |
|  | The system shall implement role-based access control to authorise users’ access to the system’s functions and data. |
|  | Systems which integrate with the Spine RBAC framework shall obtain information about a user’s allocated Role Profiles; this should be achieved by using the SAML interface provided by the Spine for this purpose, as defined in the Spine External Interface Specification (EIS). Alternatively, SDS lookup may be used. |
|  | Systems MUST NOT call the Spine SAML interface more than once per user session, unless the user is explicitly changing their role-profile selection. |
|  | Systems which integrate with the Spine RBAC framework shall allow the user to select which of the applicable User Role Profiles (ie where the organisation from the URP matches an organisation supported by the system) allocated to the user is to be applied to that user’s session with the application. Any default URP selected by the user on the most recent Smartcard authentication to the workstation shall be used to present a default suggestion for this choice, without mandating its selection. Where there is a single applicable URP, the system shall apply that URP without requiring any user selection or confirmation. Where there is no applicable URP, the system shall not allow the user to proceed. |
|  | A System which integrates with the Spine RBAC framework shall establish a user’s entitlements based on allocated Job Roles and Activities obtained from the chosen User Role Profile (URP). Systems shall use the baseline information as defined within the NRD to expand the Job Role from the URP into a set of activities, and add to that set any additional activities explicitly added to that URP.  The system shall use only those entitlements to authorise access to the system’s functions. |
|  | The system shall implement a process for incorporating updates to the nationally-defined mapping from Job Role to Baseline Activities as published by the Authority from time to time. |
|  | Where the system supports users who have not been allocated an NHS Smartcard, the system shall implement local role-based access controls which support the allocation of access rights in line with the nationally-defined Job Roles and Activities. Those local RBAC mechanisms must:   * Restrict users’ use of the system to specific functions, assigned 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, at least:   * 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) |
|  | Where systems provide non-Smartcard-based authentication that can be used by users who have been allocated Smartcards, any local access rights must automatically reflect the access rights associated with the user as defined on Spine, ie without any manual update mechanism being required. |
|  | Where systems provide non-Smartcard-based authentication that can be used by users who have been allocated Smartcards, no increased access rights can be locally associated with the non-Smartcard-based authentication. |
|  | 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). |
|  | The system must ensure that the organisation context of the system matches the selected role-profile. Where the system supports a single organisation, that organisation must match the organisation from the selected role-profile for any user access to proceed. Where a particular system supports multiple organisations, the system shall set the organisational context to that of the selected role-profile (and thus influencing the control as to which patients the user has access).  There may be specific circumstances where a user requires access across organisational contexts using the same or different systems (where it would be impracticable for that user to explicitly manually change their role-profile selection). Examples would include where more than one general practice (with their own ODS code) shares a physical location and may share administrative staff where:   * The same instance of a system is used by all practices, thus the need to switch organisational context without re-authentication, or * Separate instances of the same, or a different, system are used by each practice, thus the need to be authenticated in the context of multiple organisations simultaneously.   In such circumstances, the system MUST provide facilities for the user’s organisational context within the system(s) to be transparently set according to the patient being accessed, subject to all of the following:   * The user must have separate role-profiles (with equivalent rights) for each organisation to which these arrangements apply; * The system must be specifically configured to allow defined users to have “roaming” access across a specifically configured group of organisations; * The system must at all times make clear to the user which organisational context is in force; * The system’s audit trail must accurately reflect the organisational context. |
|  | Suppliers must provide details of the mapping of their local system functions to activities from the National RBAC Database, using a defined template[[10]](#footnote-10). This is to support the RA process (to ensure that RAs have information to enable them to correctly define positions and allocate users to such positions, or by allocating users individual URPs containing appropriate job roles any additional activities) and also to support the compliance process. |
|  | Where a User has been allocated an NHS Smart Card the system MUST ‘link’ the User record to the SDS record using the User’s UUID from their Smart Card. |
|  | The User record MUST inherit the role(s) and activities as configured in SDS and available via their SAML assertion or by direct retrieval from SDS. |
|  | The system MUST support the concept of a user having more than one role, each with its own activities. |
|  | The system MUST ONLY support the activities associated with the role that the user has logged in under. The system MUST NOT combine activities from multiple roles for the purposes of controlling a user’s access to the system. |
|  | The system MAY support roles (e.g. GP, Practice Nurse) and activities that are not part of the National RBAC Database but which extend or elaborate the National RBAC Database. Any such roles or activities MUST NOT contradict or conflict with the National RBAC Database and SHOULD only be used for specific purposes. |
|  | The system MUST support the notion of specific professional status for users, to support areas of functionality where there may be, for example, statutory reasons to restrict such functionality to certain professional groups (for example where fitnotes can only be issued by GPs). |
|  | Where a user does not have a Smart Card, it MUST be possible to assign roles and appropriate activities to the user. These roles and activities MUST be taken from the latest National RBAC Database (see also previous requirement) and it MUST be possible for a user to have different access rights for each of their roles. |

# Legitimate Relationships

|  |  |
| --- | --- |
|  | In addition to being authorised to access sensitive person data, users shall only have access to sensitive data within the records of patients with whom they have a legitimate relationship. The system shall enforce this constraint such that consent to the access could be reasonably demonstrated, i.e. the user being a member of the patient's care team, or the patient being registered at the user's practice.  This may be a result of the patient being an active registered patient at the user’s practice (as defined, for example, as the organisation part of the user’s User Role Profile). |
|  | Controls must be in place to prevent normal access to records (ie access governed by authentication credentials and access rights by registered users) that may exist within the system that refer to patients that are no longer actively registered with the practice. |
|  | Access to the records of non-active patients can be provided within a grace-period following inactivation (such a period to be configurable per organisation, default 4 weeks). Access to records during such a period must generate a notification (a warning, rather than alert) to the user designated as the organisation’s Privacy Officer (see section 13). Access to records beyond such a period must only be possible after the user has provided a reason for access, and must generate an alert to the user designated as the organisation’s Privacy Officer (see section 13). If such access is provided to multiple patients as a result of running a report, a single notification must be provided (rather than one per patient). |
|  | The act of making a patient record active (from an inactivated or archived state), when carried out without a formal patient re-registration, must generate an alert to the user designated as the organisation’s Privacy Officer (see section 13). |
|  | Where the system provides the ability to view information managed in separate organisations, these controls must ensure that information is only made available from the general practice if it concerns patients with a currently active registration. For example, any cross-organisational data sharing should not take place for inactivated, or archived, patients. |

# Information Sharing outside the practice

*“safe and appropriate sharing in the interests of the individual’s direct care should be the rule, not the exception”*Caldicott review: information governance in the health and care system, <http://www.caldicott2.dh.gov.uk/>

There are different ways in which information is commonly shared outside the practice; for example[[11]](#footnote-11):

* Providing information to accompany, for example, routine referrals of the patient to other care settings; in such circumstances, providing information is an essential part of the process. Systems must support this type of scenario; requirements are defined as part of the GP Systems Requirements.
* Allowing information from within the practice to be accessible in other care settings; this might follow an explicit referral (for example, the clinician within an outpatient clinic may feel it is helpful to review parts of the patient’s general practice record that have not been included in an original referral letter) or might be as a result of a patient’s attendance at an unscheduled or urgent care setting. Whilst the Information Governance Review “Information: to share or not to share?”[[12]](#footnote-12) encourages the sharing of information in these scenarios, systems are not mandated to support such information sharing. However, where they do, irrespective of the technical implementation of such information sharing[[13]](#footnote-13), the requirements in this section apply.

The requirements in this section are intended to recognise that:

* There is a national system for recording patients’ expression of their “consent-to-share” (a flag held on PDS), but this is a global setting and does not allow patients to specify which information they consent to share, nor in which circumstances.
* Some patients have previously expressed their dissent to information sharing, which is recorded using that mechanism.

Note that:

* Consent requirements for the Summary Care Record are contained in that programme’s requirements documentation[[14]](#footnote-14), and are not affected by any of the requirements in this section;
* These requirements do not affect any secondary uses of data (controls around consent for such scenarios are described separately.

|  |  |
| --- | --- |
|  | Systems must provide the capability to record a patient’s expressed preferences as to how clinical information about them, held within the GP system, can be accessed from other care settings, for their direct care.  Where systems are directly used in other care settings, it is expected that such preferences can be managed at the level of individual operational units or settings in which patients would reasonably expect their information to be shared without hindrance, in order to support their direct care. |
|  | Practice structures change over time, for example as practices merge or split. In such circumstances, every patient’s expressed preferences must be carried forward into the new organisational structure, on the basis that patients had been made aware of the implications of any such proposed change, prior to it taking place, and that patients had the opportunity to amend their expressed preference. |
|  | The practice must have control as to whether information sharing (access to information from other care settings) for any patients is enabled, so as to allow alignment with any practice-wide information campaigns. |
|  | The system must respect any such recorded preferences, having effect on the sharing of information that might otherwise be technically possible. |
|  | Patients must be provided with the opportunity to determine whether any information about them from the general practice is made available to other organisations for the purposes of direct care; if the system also supports access to information from other care settings, then it must also support the recording (and respect of) expressed preferences whether information about them from specific other organisations can be viewed from within the general practice.  It must not be necessary that an explicit consent to such sharing be recorded within the system prior to any such sharing taking place, other than the exception condition described in requirement GP-IG-5-6. |
|  | Some patients have an “express dissent” setting (value 2) on the consent-to-share flag held nationally on PDS, to be interpreted that the patient has previously expressed concern about potential information sharing for their direct care across different care settings.  For such patients, making their GP record available to other care settings must be on an “opt-in” basis, rather than the default “opt-out”. Therefore, in that situation, systems must prevent any access to information from other care settings (both access to data from the general practice from other settings, and if applicable, access within the general practice to information from other care settings), unless the patient has explicitly consented to such sharing in the local system through facilities provided in requirement GP-IG-5-5.  In circumstances where both (i) the patient has an ”express dissent” (value 2) setting nationally, and (ii) the system has not recorded any expressed decisions from the patient, the system must provide a prompt to the clinician as part of an encounter with the patient, to provide an opportunity to confirm the patient’s intentions through the facilities described in requirement GP-IG-5-5.  The system must support the amendment of the patient’s consent-to-share status held on PDS:   * If the status is not “express dissent” (value 2), but the patient has chosen to determine that, using facilities provided under requirement GP-IG-5-5 no information is to be made available for their direct care outside the general practice, then the consent-to-share flag must be automatically set to “express dissent” (value 2), which will have the effect of flagging any concern nationally. * If the status is “express dissent” (value 2), and the patient has chosen to take advantage of facilities as described in requirement GP-IG-5-5 to allow access to information from the General Practice, the facility should be provided to support the setting of the consent-to-share flag to “express consent” (value 1). The suggested wording of the prompt to change the setting is:   *“It has previously been recorded on a national system that you have expressed concern about information sharing for your direct care. You may leave this in place, in which case you may be asked again for your explicit consent in other care settings, or if you move practice in the future. Alternatively, you can have it changed, indicating that you no longer wish to record any concerns about information sharing nationally for your direct care. Would you like to confirm this?”* |
|  | The provision of online services to patients inevitably requires the exposure of sensitive personal data outside previous controls; whilst clinical record systems have been, and will continue to be, hosted within the controlled environment of N3 or its successors, there will be additional vectors of attack due to the availability of internet-facing services.  The technical architecture of the interface mechanism and any supporting infrastructure to satisfy the requirements in this document must therefore:  • Satisfy the requirements of IGSoC or equivalent successor agreements  • Be subject to periodic penetration testing  • Continually incorporate best-practice monitoring and intrusion-detection mechanisms |

# Additional Privacy Controls within the practice

|  |  |
| --- | --- |
|  | It MUST be possible to restrict access to a patient’s entire clinical record. It MUST NOT be possible, over and above the use of RBAC in general, to restrict access to any part of a patient record. |
|  | Such restrictions MUST ONLY be applicable at the level of user roles but MUST NOT be applied to the role representing GPs. It MUST NOT be possible to restrict such access to either groups of users or to specific individuals. |
|  | All restrictions MUST be as a result of an explicit, audited, action by an authorised user. Local practice policy may suggest specific records where restrictions may be appropriate, but restrictions MUST NOT be automatically applied by the system |
|  | Restrictions applied to records MUST NOT interfere with their inclusion in data transfers (for example as a result of a patient changing practice, or as part of a data migration between systems). It is expected that in these circumstances, as described in published guidance, any locally-applied restrictions will be removed. |

# Workstation Access Controls

|  |  |
| --- | --- |
|  | The system shall provide controls to protect unattended workstations from being accessed by unauthorised person(s), with automatic timeout after a period of user inactivity; this SHOULD be achieved by application-level locking, requiring a legitimate user to re-authenticate. It MAY be achieved by the use of operating-system desktop locking, but only when workstation authentication controls are at least as strong as application-level authentication.  Automatic timeout will be preceded by a warning that timeout is about to take place (this warning to be a configurable period before timeout, default being 60 sec). |
|  | The system shall provide a facility for the user to lock the system with a single action, this action hiding any patient-identifiable data from view and ensuring that re-authentication is required for the application to be resumed. |
|  | When access is denied due to the requirements in this section, the same user can return to their session by re-authenticating, or any other user can log off the previous session (without returning to it) in order to be able to proceed with a new session. Where another user has logged off the previous session, the system need not retain the previous session. |
|  | The system MUST provide a mechanism for hiding/removing all clinical data from display whilst retaining any patient demographics/non-clinical data. |

# Content Commitment

|  |  |
| --- | --- |
|  | Some kinds of information system interactions require the electronic equivalent of a signature in ink; this act of content commitment is provided by the use of advanced digital signatures, supported by certificates stored on the user’s NHS Smartcard.  The current need for content commitment is in the area of prescriptions within the Electronic Prescribing Service (EPS) Release 2.  Detailed requirements for the use of content commitment at the point of prescribing (within GP systems) and at the point of dispensing (within pharmacy systems) are provided separately as part of the EPS Release 2 compliance baseline. |

# Data Labelling

|  |  |
| --- | --- |
|  | All personal data about a patient which are output to hard-copy by the system MUST be 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, or for any other outputs that are subject to separate requirements.  Further guidance is available at: <http://systems.hscic.gov.uk/infogov/security/risk/nhsinforiskmgt> |
|  | The Service shall provide for the protective labelling of information (as described in GP-IG-9-1), which is output to screen rather than hard-copy, to be made known to each user either:   1. by being shown on any screen displaying the information; or 2. by being displayed to the User upon logging into the system (for example as part of an acceptable use policy). |
|  | Where alternative (a) in requirement GP-IG-9-2 above is chosen, the protective labelling of information MUST be shown in a standardised location and manner on any screen displaying the information. |
|  | 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. |
|  | The Supplier shall ensure that the system provides a means for users to verify that hardcopy print-outs are complete (e.g. "page 3 of 5" annotations). |

# Provenance

|  |  |
| --- | --- |
|  | The system must record the following provenance details of all personal and sensitive personal data recorded within the system:   * Author details (identified through unique ID), including name and role * Data entered by (if different from author) * Date & time (to the second) entered * Originating organisation * Encounter context (see the Encounter Management section in the GP Systems Requirements v2) |
|  | The system must make it possible to record provenance details of information being sent to the practice, together with provenance details of information that might be entered into the system from within the practice, but based on incoming information. For example, a document from a separate organisation may be sent into the practice, and some summarisation activity may then take place within the receiving practice. The system must enable the recording of:   * The provenance of the incoming document, and * The provenance of any information entered locally as a result of the incoming document, and * The linkage between the locally-entered information and the incoming document. |
|  | The system must make access to provenance information available to users. Whilst some details (such as name, role) associated with individual users are likely to change over time, the display of user information must reflect the state of such information as it was at the time of the associated event (such as data entry). |
|  | Where data is being displayed from outside the organisation, it must be made immediately clear to the user which items of information are from other organisations. Such visual indications should be the means by which users can access the provenance data for those items. |

# Data Annotation, Suppression and Deletion

This section provides requirements for systems to support, in particular restricted circumstances, the ability for information in a clinical record to be annotated, suppressed or deleted. There are several related mechanisms, compared in the following table:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Req ID** | **MUST/ SHOULD/ MAY** | **Typically initiated by** | **Actioned by** | **Reversible?** | **Visible marker of use?** | **Example / use case** |
| Annotation | GP-IG-11-2 | MUST | User | User | Yes, by user | Yes | Previous clinical entry now known to be untrue, or no longer true. |
| Logical Deletion | GP-IG-11-3 | MUST | User (during data entry)  User or Patient for previously-committed data | User | Yes, by back-office | Yes, for previously-committed data | i) clinician discovers error during data entry ii) patient wishes damaging information to be hidden from all future users; clinician agrees that this will not impact future care. |
| Physical deletion | GP-IG-11-4 | MUST | Patient | Back-office | No | No | Patient wishes damaging information to be hidden from all future users; court so orders. |

|  |  |
| --- | --- |
|  | Other than in the specific circumstances described in subsequent requirements in this section, the system MUST NOT allow any user to remove information from the clinical record (whether that be a “logical delete / soft delete” causing information to be hidden from view, or a “physical delete / hard delete” causing information to be physically deleted from the clinical data repository). |
|  | The system MUST support (multiple) annotation of entries in the clinical record, for example to allow a user to indicate their disagreement with information entered by others, or to indicate that they no longer hold a clinical view that was previously expressed. It MUST be possible for the user to remove annotations.  Such annotations MUST capture details of the user creating the annotation, when, with a reason being recorded. It must be possible for annotations and associated reasons to consist of least 255 characters.  Where such annotations are made, it MUST be immediately visible on all subsequent views of the record that relevant entries have been annotated, and it MUST be possible for the user to discover the associated details of the annotation.  The system SHOULD support a specific reason of “withdrawn”, for example to be used to withdraw a stated diagnosis, and in such circumstances the system MUST ensure that any secondary uses to which the clinical data is put (such as QoF calculations or clinical audit activities) exclude any such “withdrawn” entries. The system MUST also provide a mechanism to allow any such “withdrawn” entries to be filtered from the view of the clinical record, in which case it MUST be clearly visible that the view of the record is a filtered one. The system default view SHOULD be filtered.  Any such annotations must be retained with associated clinical data if that data is accessed externally, for example by a subsidiary system through an exposed interface mechanism. |
|  | The system MUST provide facilities for users to “logically delete” entries in a record: ie resulting in the underlying data being marked in such a way that it is no longer visible to any user of the record.  The requirements associated with this functionality vary, according to whether the information being deleted has been able to be viewed by other users (or accessible by system processes).  If such data has not been viewable (for example where a user discovers during the recording of a consultation that they are entering data in the record of a different patient, or where the user recognises they have made an error):   * the audit trail must record the sequence of events in such circumstances * the record MUST be able to be re-constituted to show entries that have previously been logically-deleted, but such functionality MUST only be available as part of a back-office task, for example to support forensic investigation * the system MUST ensure that the system ignores all logically-deleted data for any secondary uses to which clinical data is put (such as QoF calculations or clinical audit activities)   Alternatively, where data is being logically deleted that has previously existed in the record, and has been accessible to other users (for example where a patient feels that information in the record is damaging, that an annotation is not sufficient, and requests that information from the record is deleted; note that this is most likely to be true where information has been previously entered into the record in error):   * the record MUST be able to be re-constituted to show entries that have previously been logically deleted, but such functionality MUST only be available as part of a back-office task, for example to support forensic investigation * the normal view of the record MUST show the fact that information has been logically deleted; it MUST be possible for the user to access details of who authorised the logical deletion (including date/time, authoriser, reason) * an alert – as described in section 13 of these requirements – MUST be generated whenever this functionality is used; where there are multiple uses of this functionality for a particular patient’s record, within the same user session, there SHOULD only be a single alert generated * the system MUST prompt the user to confirm that the patient has requested such a logical deletion, that the user has considered the impact on future uses of the record, and has concluded that the benefits to the patient of having information logically-deleted outweighs any potential risk associated with an incomplete record * the system MUST store details – including the user’s acceptance of the request and risk-assessment – of the logical deletion in the audit trail * the system MUST ensure that the system ignores all logically-deleted data for any secondary uses to which clinical data is put (such as QoF calculations or clinical audit activities) |
|  | The system MUST support the physical deletion of records or parts of records in response to court orders or other legislative circumstances. This functionality MUST NOT be made available to normal users of the system, and local system administrators MUST NOT be able to grant access to such functionality to normal users.  Such physical deletions are expected to be rare – the functionality described in requirement GP-IG-11-3 is expected to satisfy the great majority of scenarios. Therefore, physical deletion shall be initiated through a supplier’s service desk facilities, but shall only be carried out in response to a specifically authenticated and validated request from an organisation’s Caldicott Guardian or Privacy Officer, co-signed by a senior clinical representative. Such requests shall be audited and retained by the supplier.  In such circumstances it MUST NOT be possible for any user, or back-office process, to reconstitute the state of the record to that prior to any such physical deletion.  This functionality MUST NOT modify the system audit trail, other than is necessary to support this requirement. The fact of a physical deletion (without referring to data content) must be recorded in the system audit trail but such entries must not be visible to normal users of the system. |

# Audit

|  |  |
| --- | --- |
|  | Systems must provide audit trails, sufficient to support the following purposes:   * to enable and support investigations, e.g. into system misuse * to monitor whether access controls are operating as intended * in support of the Care Record Guarantee, to enable fulfilment of requests from patients as to who has accessed or modified their Sensitive Personal Data or Personal Data; when that access or modification occurred and the nature of the information output (that is, displayed or printed).   Application level audit trails must be considered to be subject to the same level of controls as the electronic patient record. |
|  | 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, and when and by whom information was entered into the record.  The system shall also ensure that Audit Trails are kept which record information about all information exchanges with external systems and organisations, 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 * All data access or presentation from separate organisations or systems   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, taking into account the requirements stated in GP-IG-11-4. |
|  | 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 inactivation 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[[15]](#footnote-15).  Such facilities to include the ability to display, filter and sort parts of the audit trail based on at least the following parameters (both individually and in combination): patient id (normally expected to be the NHS Number), user id, organisation id, date & time, sequence number.  Whilst some details (such as name, role) associated with individual users are likely to change over time, the display of user information must reflect the state of such information as it was at the time of the associated event (such as data entry). |
|  | 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, URP id when Smartcard authenticated)* attribute values, obtained from the user’s Session structure; * a record of the identify 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. |
|  | 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. |
|  | 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, to ensure the integrity of the audit trail, and protect against attempts to tamper. |
|  | All Audit Trails shall be enabled at all times and there shall be no means for users, or any other individuals, to disable any Audit Trail. |
|  | All Audit Trails shall be included as part of the routine system backup. This shall include:   * Application-level audit log files – the events defined above. * Operating-system security audit logs – containing events relating to security at the workstation/server level, e.g. login events, changes to security settings, etc. |
|  | The audit trail may be moved to archive storage as required for efficient system operation, but shall be retained in accordance with the audit retention policy as specified by the authority, to allow access as specified above in requirement GP-IG-12-4. In summary, audit trail entries that describe changes to personal or sensitive personal data shall be kept for the same time as the data it describes (typically life plus 30 years).  Where audit data has been previously archived, it must be made clear in audit viewing tools or other arrangements that some audit data may not immediately available, but that it can be retrieved (with an indication of steps to take to make such archived data visible).  Details of message exchanges should be kept similarly, however the payload of messages may be subject to a shorter retention period (not shorter than one year), and may be archived such that access times to data older than one month may be lengthened to one working day rather than being immediately available, (as would otherwise be the case) to online tools. |
|  | Copies of the audit trail should only be made to support the following:  For forensic purposes, a separate copy of the audit trail (in the original live environment format) must be used from the version in the live environment  For other reporting and querying purposes, a different separate copy of the audit trail should be used from the version in the live environment |
|  | Audit trails must include details of any configuration (e.g. a spine service being switched on), system updates, data backups and other system maintenance activities or reference data changes (e.g. an update to the clinical coding scheme data, drug databases) applied to the system. |
|  | In a system where any patient records are archived (made inaccessible to normal system access) then a link must be maintained between the archived records and the audit trail, to ensure that the audit records associated with archived records remain accessible. |
|  | Suppliers must ensure that during upgrades to systems, any manual steps are documented in advance and any automated steps must involve the production of one or more logs which describe each step being taken and whether or not it has been processed successfully.  Logs that cover a sequence of steps must also indicate whether the overall sequence has been a success or failure. |
|  | The timestamps in Audit Trail entries shall be stored in UTC(GMT), to the nearest second. When displaying audit entries to authorised users, they shall be displayed by default in local time (with clear indication how this may differ from UTC). |

# Alerts

|  |  |
| --- | --- |
|  | There are a number of requirements elsewhere in this document (which reference this alerts section) where it appropriate for specific actions to be permitted, but an alert to a privacy officer will be raised to ensure appropriate governance of actions can be maintained. In such circumstances, the system shall ensure that the user is made aware that an alert will be raised, and is provided with the ability to enter a reason for their action. |
|  | In such circumstances, an alert containing the following information must be made available to the individual within the organisation designated as Privacy Officer:   * Date and time (to the second) * User * Context of the system at the time the alert was raised (including patient identification) * Reason entered by the user   This alerting mechanism should use the Task and Workflow mechanism within the GP system. |
|  | The alerting mechanism shall support at least two levels of alerts: notifications (warnings) and full alerts. Notifications are for occasions when there is a legitimate, but unusual, activity taking place (such as the access to a record of a newly-archived patient) whereas alerts are for exceptional conditions. |
|  | The system must provide functionality to allow the designated Privacy Officer to receive notification of each alert, as it is raised, in a timely manner (within 10 minutes), and to view the details (including level, date, time, context, reason) of the alert. |
|  | The system must provide functionality to allow the designated Privacy Officer to view all alerts, to change the status of alerts (eg new, in-progress, completed), to record the actions carried out associated with each alert, and to filter and/or organise the view of alerts according to (either individually, or in combination) level, date/time, user involved, patient involved, status. |
|  | The system must not allow go-live for a specific organisation without a Privacy Officer being configured within the system. It is important that there is at least one individual user per organisation designated as Privacy Officer at all times; the system shall enforce this, for example by ensuring that an individual designated as the Privacy Officer cannot be removed from the system prior to another individual being so designated. |

# Information Security

The HSCIC publishes a series of Good Practice Guidelines (GPG) which are a series of informational documents providing good practice advice in technology-specific areas of Information Security and Information Governance. Each Good Practice Guideline is intended to support Department of Health Policy and Information Governance requirements for NHS organisations and suppliers alike. As Information Security is an evolving discipline the library documents will be updated regularly and where they exist for a particular area of Information Security should be followed.

The Good Practice Guidelines can be found at <http://systems.hscic.gov.uk/infogov/security/infrasec/gpg>

## Time-stamping

|  |  |
| --- | --- |
|  | Systems MUST ensure that all parts of their solution synchronise any internal time clocks to within 250 milliseconds, using the NTP protocol. This enables meaningful comparison and sorting of, for example, messages based on timestamps, and of audit entries. |
|  | All messaging must be time-stamped using UTC(GMT). Whilst applications may display local time when displaying message details, message timestamps shall contain UTC(GMT) values. |
|  | All audit entries, and other timed entries into the clinical record, shall be based on the synchronised time-system as described in this section. Applications must display local time when displaying audit and timed information to users. |
|  | Systems may synchronise any internal time clocks with N3 Network DNS Servers – currently at cns0.nhs.uk & cns1.nhs.uk – using the NTP protocol. Alternatively, the system MUST utilise a Stratum 3 time source as a minimum however suppliers SHOULD consider the use of Stratum 2 or above. |

## Secure Storage

|  |  |
| --- | --- |
|  | The confidentiality and integrity of personal and sensitive personal data must be protected from unauthorised access and modification while stored within compliant systems, and in backup and archive storage.  **These requirements also cover the circumstances w**here devices or services offered by the Supplier result in the transfer of patient identifiable data through electronic means or by removable media and devices. Examples of removable media and devices to which the requirements apply include but are not limited to: CD, DVD, tape, USB memory stick, removable hard drives, laptops and PDAs.  These requirements also cover where services offered by the Supplier result in the storage of patient identifiable data in inherently difficult-to-secure environments. Examples of this include servers or desktops in a Practice.  Note that prior to any transfer patient identifiable data taking place, full consideration must be given to the business need for the transfer, and for any opportunity to de-identify the data. |
|  | The system shall ensure that all personal and sensitive personal data about a patient, and audit logs, are protected from unauthorised access and modification when stored within the system’s databases and/or files. This applies wherever such data is being processed or stored. |
|  | While being processed, stored, and in backup and archive storage, all personal data and sensitive personal data and audit logs shall be physically protected from loss or theft in line with the security policy published by the authority. |
|  | Archive copies of personal data and sensitive personal data and audit logs shall be retained in line with the retention policy published by the authority. |
|  | The location of physical storage of Personal or Sensitive Personal data shall abide by published DH guidelines. |
|  | The system shall ensure all data is stored for periods as defined by DH policy and described in the NHS Records Management Code of Practice Parts 1 and 2, or as subsequently amended. |
|  | When no longer required to support services, all media and any infrastructure components that have stored data shall be subject to secure deletion to standards described in “Destruction and Disposal of Sensitive Data – Good Practice Guideline”[[16]](#footnote-16) |

## Secure Transmission

|  |  |
| --- | --- |
|  | The Supplier shall demonstrate that it has limited any patient identifiable data (including personal data and sensitive personal data) transferred to portable media to the minimum required. |
|  | Where devices or services offered by the Supplier result in the transfer of any patient identifiable data on any portable media, such media shall be encrypted. The level of encryption used shall conform to the Approved Cryptographic Standards published by the Authority. |
|  | Where devices or services offered by the Supplier result in the transfer of any patient identifiable data outside the local physical or virtual network (VLAN), including transfers across VLAN boundaries within a single local network or exporting data to removable data, encryption shall be used. The level of encryption used shall conform to the Approved Cryptographic Standards[[17]](#footnote-17). |
|  | The encryption, decryption, transport, storage and destruction of data which is transferred shall be auditable with the media logged and tracked to ensure all instances are accounted for. |
|  | The Supplier shall ensure that the encryption product used is accredited to FIPS 140-2 and should have received Augmented Grade Commercial Product Assurance (CPA) accreditation[[18]](#footnote-18). |
|  | The supplier shall ensure that the encryption key for each archive is of an appropriate strength and complexity as detailed in the Approved Cryptographic Standards. |
|  | Where encryption keys are generated by the system automatically for transfer of data by portable media, the system shall provide the encryption key to the Data Controller for each encryption operation. In such circumstances, cryptographic keys must not be generated by the use of an algorithm or other shared secret that solely combines known or accessible environmental or other context-specific information, without the inclusion of unique, context specific secret information as provided by the user or supplier. Such encryption keys shall be generated using existing libraries. Context specific, secret information should be controlled and managed in line with key management good practice principles (ie with audited access controls in place). |
|  | The Supplier shall ensure that any encryption keys generated by the system are stored securely to enable data recovery in the event of key loss or corruption by the Data Controller. |
|  | The supplier shall ensure that the encryption key for each archive is unique to that data archive. |
|  | Where the Supplier system provides a mechanism for sending encryption keys to a recipient, either electronic or manually, there must be processes in place to ensure that the encryption keys are sent following a separate communication mechanism to the encrypted data or posted separately from the encrypted media. |
|  | Where a service offered by the Supplier requires the transfer of patient identifiable data by portable media the media shall be encrypted to the level required by the Approved Cryptographic Standards and transported in a secure manner. The transfer of Patient Identifiable Data shall be conducted using Secure Courier services following Department of Health Encryption Guidance guidelines. |
|  | Where a service offered by the Supplier requires the transmission of patient identifiable data by electronic means, the data shall be transmitted in an encrypted form to the level required by the Approved Cryptographic Standards. This encrypted data can be transmitted via a secure email service such as NHS Mail or over an approved network such as N3. |
|  | The system shall protect the confidentiality and integrity of Personal Data and Sensitive Personal Data about a patient in transit across un-trusted networks, including (but not limited to):   * between data centres, * between data centres and deployment site LANs, * between N3 customers and remote access devices, * between data centres and remote access devices. |

## Network Access Controls

Note that additional guidance can be found at <http://systems.hscic.gov.uk/infogov/igsoc/links>

|  |  |
| --- | --- |
|  | The requirements in this section apply where a supplier provides a hosted service (outside of the practice premises) supporting deployments – such as a hosted application service or a shared message handling service.  Any requirement stated in this section does not absolve the supplier from adhering to the Authority’s Statement of Compliance obligations. |
|  | The supplier shall ensure that all connections to remote servers and applications are authenticated.  This requirement includes connections via the Internet. |
|  | The supplier shall ensure that access to diagnostic ports for network and server components is securely controlled. |
|  | The supplier shall segregate the networks and servers that support services under these contractual arrangements from deployments relating to other, unrelated services. |

# Subject Access Requests

|  |  |
| --- | --- |
| **Applicable only to principal systems** | |
|  | The Supplier shall ensure that the system maintaining personal data or sensitive personal data to be capable of responding to subject access requests, in accordance with the Data Protection Act 1998. Note that any historical data about the patient, that may be linked to the current active record (for example as a result of a GP2GP transfer) although not normally available to system users, falls within the scope of a subject access request. |
|  | The Supplier shall ensure that the system enables the patient's electronic records to be screened by Authorised Users for data that could be detrimental to a patient if viewed and/or third party information before responding (with such information being redacted) to a subject access request. This ability to be subject to the requirements described in section 4. |
|  | The Supplier shall ensure that the system enables a user to record a subject access request. |
|  | The supplier shall ensure that the system provides that the data that can be recorded about a subject access request includes, as a minimum, the date the request was received, the identity of the subject, the identity of the person making the subject access request, the identity of the User and organisation responsible for responding to the request, the identity of the healthcare professional consulted before the Personal Data were released, whether the request was refused, a free-text reason for a refusal, a classified reason for a refusal and the date of the response to the request and such other information as the Authority shall reasonably specify. |
|  | Where a subject access request is refused, the system shall require that at least one reason for refusal be selected from a pre-defined list (to be able to be configured within the system), which will be the subject of a national standard (as issued by the Authority from time to time), and that an alert is raised as described in section 13. |
|  | The system shall enforce RBAC controls to control access to functionality described in this section. |
|  | The system should provide functionality for monitoring SAR requests in progress and for reporting on targets for fulfillment. |

# Requirements Traceability Matrix (RTM)



1. <http://www.nigb.nhs.uk/guarantee/> [↑](#footnote-ref-1)
2. <http://www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550> [↑](#footnote-ref-2)
3. See also <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx> , from where these definitions were sourced [↑](#footnote-ref-3)
4. <http://systems.hscic.gov.uk/demographics/pds> [↑](#footnote-ref-4)
5. NPFIT-NCR-PMG-REP-2584 External Interface Specification [↑](#footnote-ref-5)
6. published at <http://systems.hscic.gov.uk/infogov/security/infrasec/gpg> [↑](#footnote-ref-6)
7. Ibid. [↑](#footnote-ref-7)
8. http://nww.connectingforhealth.nhs.uk/iim/ra/rbac/nrd [↑](#footnote-ref-8)
9. NPFIT-NCR-PMG-REP-2584 [↑](#footnote-ref-9)
10. NPFIT-FNT-TO-IG-IGCOM-0129 Application RBAC Compliance Template [↑](#footnote-ref-10)
11. This is not intended to be an exhaustive list [↑](#footnote-ref-11)
12. http://www.caldicott2.dh.gov.uk/ [↑](#footnote-ref-12)
13. There are a number of ways in which such sharing may be implemented; for example, through the use of a single system across care settings, through facilities for systems in other settings to query the GP system, or where extracts of data may be taken into other systems [↑](#footnote-ref-13)
14. See <http://www.nhscarerecords.nhs.uk/optout> [↑](#footnote-ref-14)
15. http://www.nigb.nhs.uk/guarantee [↑](#footnote-ref-15)
16. Published at http://systems.hscic.gov.uk/infogov/security/infrasec/gpg [↑](#footnote-ref-16)
17. See also <http://systems.hscic.gov.uk/infogov/security/encryptionguide.pdf> [↑](#footnote-ref-17)
18. http://www.cesg.gov.uk/servicecatalogue/CPA/Pages/CPA.aspx [↑](#footnote-ref-18)