Amendment History:

|  |  |  |
| --- | --- | --- |
| Version | Date | Amendment History |
| 0.1 | 17th Sep 2008 | First draft issued for comment. |
| 0.2 | 22nd Sep 2008 | Incorporated comments from Martin Tallis. |
| 0.3 | 23rd Sep 2008 | Corrected formatting issues, missing section title and modified elaboration for 1-click access. |
| 1.0 | 6th Oct 2008 | Incorporated final comments from Danny Ruttle and Mike Walker and changed status to approved. |
| 1.1 | 29-Apr-2010 | - Updated to align with RBAC database V26 with Areas of Work now deprecated, and many Activity descriptions updated.  - Activities B0168, and B8028 added.  - Activity B0088 removed.  Draft for review. |
| 1.2 | 08-Jul-2010 | (No changes to document body.)  Draft for Approval |
| 1.3 | 30-Jul-2010 | Revision of description of SCR Consent in section 1.3 |
| 2.0 | 11-Aug-2010 | Approved version – content as version 1.3 |
| 2.1 | 04-May-2011 | -Updated to align with RBAC database v27.1  -Activities B1680 and B0098 added |

Forecast Changes:

|  |  |
| --- | --- |
| Anticipated Change | When |
| Review/Revision for RBAC Database V28 | 2011-12 |

Reviewers:

This document must be reviewed by the following:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title / Responsibility | Date | Version |
| Mike Walker |  |  | 11-Jun-2010 | 1.1 |
| Steve Davison |  |  | 5-May-2011 | 2.1 |
| Nancy Pickering |  |  | 14-Jun-2010 | 1.1 |

Approvals:

This document must be approved by the following:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title / Responsibility | Date | Version |
| Richard Clay |  | Programme Manager – SCR Programme | 30-Jul-2010 | 1.3 |
| Nancy Pickering |  | Senior Technical Architect for Demographics and SDS | 10-Aug-2010 | 1.3 |
| Jim Lewis |  | Lead Technical Architect | 04-Aug-2010 | 1.3 |

Distribution:

NASPs, ESPs, LSPs

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in FileCM is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

|  |  |  |  |
| --- | --- | --- | --- |
| Ref no | Doc Reference Number | Title | Version |
| 1 | NPFIT-SHR-QMS-PRP-0015 | Glossary of Terms Consolidated.doc | <latest> |

Glossary of Terms:

List any new terms created in this document. Mail the NPO Quality Manager to have these included in the master glossary above [1].

|  |  |  |
| --- | --- | --- |
| Term | Acronym | Definition |
|  |  |  |

Contents

[1 About this Document 5](#_Toc269306860)

[1.1 Purpose 5](#_Toc269306861)

[1.2 Audience 5](#_Toc269306862)

[1.3 Content 5](#_Toc269306863)

[2 Activities Relevant to PSIS 6](#_Toc269306864)

[2.1 Information Governance Activities 6](#_Toc269306865)

[2.2 Clinical Activities 7](#_Toc269306866)

[3 Activities Relevant to PDS 10](#_Toc269306867)

[3.1 Information Governance Activities 10](#_Toc269306868)

[3.2 Demographic Activities 10](#_Toc269306869)

[4 Parent Activities and Base-lined Job Roles 20](#_Toc269306870)

# About this Document

## Purpose

This document provides guidance on the implementation of Role Based Access Controls for applications integrating with the Personal Spine Information Service (PSIS) and/or the Personal Demographics Service (PDS) in the Spine 2008B timeframe.

## Audience

The target audience for this document is information governance architects within supplier organisations including NASPs, LSPs and ESPs.

## Content

Sections 2 and 3 define the activities relevant to PSIS and PDS respectively.

Section 4 defines the parent activities for each activity listed in sections 2 and 3 along with the base-lined job roles.

The activities and baseline has been extracted from V26 of the National RBAC Database.

Access to the Summary Care Record is now governed by the SCR Consent Preference that is stored in ACS. The consent value held on PDS is no longer used for SCR, but continues to apply to the sharing of detailed care records across legal organisation boundaries.

The RBAC activity ‘View when permission could not be requested’ (B0168) now applies to Summary Care Record access. The RBAC activity ‘Gain Temporary Access to Patient Data With Permission from Dissenting Patient’ (B0088) no longer applies to Summary Care Record access.

Where useful, diagrams illustrate any differences in behaviour when an application is not connected to the Spine and the following symbols are used:



# 

# Activities Relevant to PSIS

| **Code** | **Activity** | **Includes** | **Description** |
| --- | --- | --- | --- |
| Information Governance Activities | | | |
| B0082 | Legal Override of Consent |  | Allows a user to view a patient’s records (both Summary Care Record and detailed) without patient consent where legally justifiable. Example reasons are public interest and statute.  Such access will cause an alert which will not be repeated for the duration of the temporary access. |
| B0168 | View when permission could not be requested | B0360 | Where a patient has positively chosen, or has a default consent setting of “ask me first”, the user should normally ask the patient for permission before their Summary Care Record is viewed. However, this activity enables viewing without permission in specific circumstances such as a medical emergency where it is not possible to ask the patient. This access is subject to the user's other access rights.  Note that the specific circumstances referred to above are distinct from those justifying a legal override of consent (see activity B0082). However, in both cases, an alert is raised and notifications can be received by users with activity B0015.  Includes:  B0360 View Detailed Health Records |
| B0083 | Gain Temporary Access to Patient Sealed Data Without Patient Permission | B0070 | Allows a user to access sealed (but not locked) data when the patient has not consented to this access and the user does not have access through the team they work in or their authoring rights e.g. public interest, statute. Such access will cause an alert which will not be repeated for the duration of the temporary access.   Includes: B0070 Access Patient Sealed Data |
| B0070 | Access Patient Sealed Data |  | Allows a user to access information that is patient sealed (or locked) for which they have access permission (e.g. as a result of the team they work in or their authoring rights).  Also allows a user to access information that is patient sealed (but not locked) for which they do not have access permission (e.g. as a result of the team they work in or their authoring rights) but do have express Patient permission to do so.  Such access will cause an alert which will not be repeated for the duration of the temporary access.  In either case the scope of their access is controlled by their other relevant RBAC rights. |
|  |  |  |  |
| Clinical Activities | | | |
| B0256 | View ETP Clinical Data within CSA |  | The CSA does not currently display ETP messages. This should no longer be granted and where previously granted it should be removed. Any users with this activity will be presented with a blank screen within CSA which may cause confusion and lead to unnecessary service desk calls. |
| B0257 | View non-ETP Clinical Data within CSA |  | Allows the viewing of all clinical data within the Summary Care Record application with the exception of ETP messages. With one exception (discussed below) the activity 'B0264 Access CSA (Perform Patient Trace)' must also be granted in order for this activity to be effective.  THIS ACTIVITY MUST NOT BE GRANTED UNLESS YOUR RA HAS BEEN AUTHORISED TO DO SO BY THE SUMMARY RECORD EARLY ADOPTERS PROGRAMME.  For those applications which support ‘1-click access’ this activity by-passes the requirement for the gateway activity B0264 only where the patient has already been traced in the application.  **Elaboration**  With one exception (SCRa 1-click access) this activity is only relevant to SCRa (previously called CSA) and should not be used by other applications requiring access to PSIS. Use ‘B0370 View Summary Health Records’ instead. |
| B0370 | View Summary Health Records |  | Allows user to view summary health information using the local application, i.e. not via the national Summary Care Record application.  This activity does not provide 1-click access to the Summary Care Record application (refer instead to B0257).  **Elaboration**  This activity should be used on the assumption that the patient is registered on and being viewed within the application, i.e. not via CSA (see B0257 for note on 1-click access).  It supports the following PSIS queries:   * PSIS Document List Query * PSIS CRE List Query * PSIS Document Query (may be used in conjunction with Synchronisation List query for system synchronisation purposes) |
| B0380 | Perform Detailed Health Record | B0790 B8011 B0069 | Allows user to enter information in detailed clinical records including clinical coding, patient medication, clinical alerts, health issues, comments, contact events, assessments, care plans, conditions, dependency levels, birth (delivery and CDS details).  Also allows user to change the consent to treatment flag and upload information to the Summary Care Record as defined by the CRS programme board.  This does not allow viewing of sealed information or sealing, which are separately controlled.  Includes:  B0069 Record Patient Medication;  B0790 Perform Clinical Coding;  B8011 Perform Clinical Documents. |
| B8028 | Verify Detailed Health Records | B0380 | Allows user to verify the contents of detailed clinical records entered by a third party including clinical coding, patient medication, clinical alerts, health issues, comments, contact events, assessments, care plans, conditions, dependency levels, birth (delivery and CDS details).  Also allows user to change the consent to treatment flag and upload information to the Summary Care Record.  Includes: B0380 Perform Detailed Health Records. |
| B8029 | Manage Detailed Health Records | B8028 | Allows user to remove (mark as deleted in database and make non visible to end user) or alter the contents of detailed clinical records entered by a third party including clinical coding, patient medication, clinical alerts, health issues, comments, contact events, assessments, care plans, conditions, dependency levels, birth (delivery and CDS details).  This does not allow viewing of sealed information or sealing, which are separately controlled.  Also allows user to change the consent to treatment flag and upload information to the Summary Care Record.  Includes: B8028 Verify Detailed Health Records.  **Elaboration**  This activity allows PSIS documents to be withdrawn.  This activity also allows update of PSIS by contributing (via indirect include of B0380 Perform Detailed Health Record). |
| Activities Relevant to PDS | | | |
| Information Governance Activities | | | |
| B0020 | Control Consent Status |  | Allows a user to change the value of the national flags indicating a patient’s preferences for restricting viewing of their Summary Care Record and detailed records. This activity must only be granted to users who are able to explain to the patient the consequences of these choices.  This activity controls access to sensitive personal data which includes clinical and administrative information, i.e. it does not apply to demographic data. |
| Demographic Activities | | | |
| B1611 | Access Sensitive Records |  | The National Back Office can flag patient records as ‘Sensitive’, indicating that local systems may restrict access to a subset of users. This activity gives permission to access the local records, including local location details and any other local records according to their other RBAC access rights in the same User Role Profile as this activity. It does not provide access to the location information held on PDS. |
| B1680 | Manage Patient Duplicate Records |  | Allow user to search for potential duplicates and perform a merge of the records including administrative, episodic and clinical data. |
| B0098 | Perform Extended Person Trace |  | Allow user to search for a patient against the Personal Demographics Service (PDS) using a postcode or Postal Address File (PAF) key only trace. Permits the viewing of full demographic data, but does not provide access to sensitive personal information.   This activity must only be allocated to a limited number (3 to 4) of correctly trained demographics staff working in a local back office environment either at a Trust or national level. Its use should be monitored locally on a regular basis.   Note that this activity is only effective in the SCR Application when used in combination with activity B0264 Access CSA (Perform Patient Trace).   Note that this activity is only effective in the DSA when used in combination with the activity B0089 Access DSA. |
| B0820 | View Patient Demographics |  | Allow user to search for and view local instance of patients' demographic records. No direct PDS access.  Also allows the user to execute demographic reports such as death notifications (patients who have either died or been undeaded on PDS).  **Elaboration**  This activity is not to be used by applications for access to PDS – B0264 Access CSA (Perform Patient Trace) should be used for this instead. Any access to the PDS data is only indirect as a result of synchronisation using B0825 Amend Patient Demographics. |
| B0825 | Amend Patient Demographics | B0820 | Allow user to amend local instance of patient demographics and synchronise with PDS (where the application is able to synchronise with the record on PDS, differences detected can be accepted or rejected).  Also allows the user to import patient identified on PDS into local instance (where not already registered) using PDS simple trace (forename, surname, DOB or sex).  The user cannot register a patient locally when there is no connection to the Spine.  When used in conjunction with the gateway activities 'B0089 Access DSA' or 'B0264 Access CSA (Perform Patient Trace)' allows user to update demographic data on the Personal Demographics Service (the national demographic database) for the patient they have selected EXCLUDING the Civil Registered birth and death data.  Includes: B0820 View Patient Demographics.  **Elaboration**    The user can search on PDS and import a patient identified using the Simple Trace query.    The user can search on PDS using the Simple Trace query and choose to resolve any discrepancies found.  The user cannot register a patient locally when there is no connection to the Spine. |
| B0830 | Perform Patient Demographics | B0825 | Allow user to register patients on the local instance where a patient is not found on PDS or where PDS is unavailable (when applications re-connect they should perform a PDS lookup, compare the records and, where they match on the patient, allow synchronisation as described for 'B0825 Amend Patient Demographics').  Also allows the user to register patients anonymously or pseudonymously on local systems to protect patient confidentiality when the patient is receiving sensitive treatment or advice, for example relating to sexual health matters.  This does not allow new patients to be registered on PDS (see B1610).  Includes: B0825 Amend Patient Demographics.  **Elaboration**    Allow user to search on PDS and import a patient identified as above (because of included activity) when connected to spine.    When disconnected the user can register a patient on the local system.  When the system re-connects to spine it should perform a PDS lookup, compare the records and, where it exists, allow synchronisation. This does not allow new patients to be registered on PDS (see B1610). |
| B0835 | Manage Patient Demographics | B0837 B0830 B1680 | Allow user to delete patients entered or imported in error on the local application. Any local deletion will not affect PDS.  When disconnected the user can register a patient on the local system and delete (make not visible to the end user) patients registered on the local system. When applications re-connect they should perform a PDS lookup, compare the records and, where they match on the patient, allow synchronisation as described for 'B0825 Amend Patient Demographics').  This does not allow new patients to be registered on PDS (see B1610).  Includes:  B0830 Perform Patient Demographics;  B0837 Decease Patient;  B1680 Manage Demographic Duplicate Records  **Elaboration**    Allow user to search on PDS and import a patient identified as above (because of included activity) when connected to spine.  Allow user to delete (make not visible to the end user) patients registered on the local system.    When disconnected the user can register a patient on the local system and delete (make not visible to the end user) patients registered on the local system. Any local deletion should not affect PDS.  When the system re-connects to spine it should perform a PDS lookup, compare the records and, where it exists, allow synchronisation. This does not allow new patients to be registered on PDS (see B1610). |
| B0065 | Undecease Patient |  | Allow user to reverse the recording of a patient as deceased on a local solution. This does NOT synchronise with PDS. |
| B0837 | Decease Patient | B0820 | Allow user to record a patient as deceased. This will allow synchronisation with PDS.   Includes: B0820 View Patient Demographics. |
| B0264 | Access CSA (Perform Patient Trace) |  | Allow user to search for a patient against PDS with using wider search criteria than 'B0825 Amend Patient Demographics' including blank fields and wildcards.  This activity also acts as a gateway activity for the Summary Care Record application (previously known as the Clinical Spine Application) for patient tracing.  Permits the viewing of full demographic data, but does not provide access to sensitive personal (clinical and administrative) information.  See also 'B0098 Perform Extended Person Trace'.  **Elaboration**    Note that the Clinical Spine Application has been renamed the Summary Care Record application, which is abbreviated to SCRa.  This activity supports access to PDS using the following queries:   * Simple trace and NHS number * Advanced Trace (with algorithmic or alphanumeric search and use of wildcard characters) * Cross check   Note that the following queries are system initiated and are therefore not controlled through RBAC.   * Batch tracing (cross check) * Batch tracing (advanced trace)   Note that B0098 Perform Extended Person Trace is not relevant to applications other than SCRa and DSA. |
| B1610 | Allocate NHS Number | B0264 | The user may request a new NHS number for an un-registered patient and the number will be generated and returned automatically by PDS, effectively adding the new patient to PDS. IT IS STRONGLY RECOMMENDED THAT LOCAL PROCESSES ARE PUT IN PLACE TO ENSURE THAT DUPLICATE REGISTRATIONS ARE NOT PERFORMED.  A user can also search for a patient against PDS with wider search criteria than 'B0825 Amend Patient Demographics', including blank fields and wildcards (because of the included activity 'B0264 Perform Patient Trace').  Includes:  B0264 Perform Patient Trace. |
| B8009 | Register Patient with Primary Care Provider on PDS |  | Allows user to change the patient’s registered primary care provider on PDS.  Also allows user to run reports to support GP registration activities.  **Elaboration**    Allow user to allocate a new NHS number and register patients on the local instance where a patient is not found on PDS or where PDS is unavailable.  User can change the patient’s *registered* practice on the Spine. |

# Parent Activities and Base-lined Job Roles

In order to map the relevant access rights to all activities and job roles it is vital that the baseline policy is modelled as well as the activity hierarchy of included activities.

The baseline policy describes the mandatory access rights for each job role and it is possible to model this in two main ways:

1. As a static table held locally by the application and uploaded on demand using information exported from the national RBAC database.
2. As a dynamic table populated automatically by performing LDAP queries on the SDS.

The slight advantage of the former approach is that the solution provider has more control over when a particular baseline is made live but given that the changes are not frequent this is not significant. The current process involves annual reviews. If the latter approach is used it would be very sensible to create a local cache rather than perform LDAP queries when each user logs in.

The other feature to take into account is the include relationships between activities. For example, when decoding the access rights associated with an activity such as B0380 Perform Detailed Health Records it is vital to map the same access rights to all parent activities which in this example includes:

* B8028 Verify Health Records
* B8029 Manage Detailed Health Records

where B0828 includes B0380, and B8029 includes B8028.

Like the baseline policy, this information can be gleaned from the national RBAC database or looked up using LDAP queries on the Spine. The included activity information is held as free text in a standard format at the end of each activity description but is not ideal for machine reading. Most suppliers, particularly LSPs have chosen to model the information statically.

Therefore in order to fully map relevant access rights to each User Role Profile (URP) received from the Spine Security Broker (SSB) it is necessary to follow these steps:

1. Decode the activities associated with the job role from the national baseline policy. As of V26 all areas of work have been deprecated and it is no longer required to take them into account when decoding the baseline. However, where support for areas of work was provided previously, it is vital that trusts are provided with clear guidance in sufficient time so that any affected profiles can be updated by adding explicitly any missing area of work baseline activities.
2. For each activity determine which are its parent activities and map the same access rights (as a minimum) to each one.
3. For each parent map any additional rights that are specific to that activity and its parents and so on.

In order to facilitate this process the following table lists each activity described in the previous sections and for each one lists the parent activities and base-lined job roles. In the case of the job role baseline policy, where a job role acquires the activity directly, it is listed on its own.

For further information on the national baseline policy please refer to:

* RBAC Harmonisation across the NHS, v4.0, **NPFIT-FNT-TO-IG-0030.05**
* RBAC Knowledge Map, v5.0 or later, NPFIT-FNT-TO-IG-IGCOM-0090

| **Activity** | **Parent Activities** | **Baselined Job Roles** |
| --- | --- | --- |
| B0082 Legal Override of Consent |  |  |
| B0168 View when permission could not be requested |  | R8000 Clinical Practitioner Access Role R8001 Nurse Access Role R8003 Health Professional Access Role |
| B0083 Gain Temporary Access to Patient Sealed Data Without Patient Permission |  |  |
| B0070 Access Patient Sealed Data | B0080 Establish Sealing Controls B0083 Gain Temporary Access to Patient Sealed Data Without Patient Permission | R8000 Clinical Practitioner Access Role R8001 Nurse Access Role R8003 Health Professional Access Role R8014 Social Worker Access Role R8016 Midwife Access Role |
| B0370 View Summary Health Records | B0360 View Detailed Health Records B0168 View when permission could not be requested B0790 Perform Clinical Coding B0380 Perform Detailed Health Record B8028 Verify Health Records B8029 Manage Detailed Health Records B0800 Manage Clinical Coding B1693 View Mental Health Functions B1694 Perform Mental Health Functions B0064 Manage Mental Health Functions B1690 View Sexual Health Functions B1691 Perform Sexual Health Functions B0072 Manage Sexual Health Functions | R8000 Clinical Practitioner Access Role R8001 Nurse Access Role R8003 Health Professional Access Role R8004 Healthcare Student Access Role R8005 Biomedical Scientist Access Role R8006 Medical Secretary Access Role R8007 Clinical Coder Access Role R8014 Social Worker Access Role R8016 Midwife Access Role |
| B0380 Perform Detailed Health Record | B8028 Verify Health Records B8029 Manage Detailed Health Records | R8000 Clinical Practitioner Access Role R8001 Nurse Access Role R8003 Health Professional Access Role R8006 Medical Secretary Access Role R8016 Midwife Access Role |
| B8028 Verify Health Records | B8029 Manage Detailed Health Records | R8000 Clinical Practitioner Access Role |
| B8029 Manage Detailed Health Records |  |  |
| B0020 Control Consent Status |  |  |
| B1611 Access Sensitive(S) Flagged Records |  |  |
| B0820 View Patient Demographics | B0096 Amend Patient Demographics (National Back Office) B0825 Amend Patient Demographics B0830 Perform Patient Demographics B0835 Manage Patient Demographics B0837 Decease Patient B8012 View Patient Administration B0360 View Detailed Health Records B0168 View when permission could not be requested B0790 Perform Clinical Coding B0380 Perform Detailed Health Record B8028 Verify Health Records B8029 Manage Detailed Health Records B0800 Manage Clinical Coding B1693 View Mental Health Functions B1694 Perform Mental Health Functions B0064 Manage Mental Health Functions B1690 View Sexual Health Functions B1691 Perform Sexual Health Functions B0072 Manage Sexual Health Functions B8013 Amend Patient Administration B0560 Perform Patient Administration B8015 Perform Clinically Restricted Administration B8016 Perform Management Restricted Administration B8017 Manage Patient Administration | R0001 Privacy Officer R5110 Demographic Administrator R8000 Clinical Practitioner Access Role R8001 Nurse Access Role R8003 Health Professional Access Role R8004 Healthcare Student Access Role R8005 Biomedical Scientist Access Role R8006 Medical Secretary Access Role R8007 Clinical Coder Access Role R8009 Receptionist Access Role R8010 Clerical Access Role R8012 Information Officer Access Role R8013 Health Records Manager Access Role R8014 Social Worker Access Role R8016 Midwife Access Role R8024 Bank Access Role |
| B0825 Amend Patient Demographics | B0830 Perform Patient Demographics B0835 Manage Patient Demographics | R5110 Demographic Administrator R8000 Clinical Practitioner Access Role R8001 Nurse Access Role R8003 Health Professional Access Role R8006 Medical Secretary Access Role R8007 Clinical Coder Access Role R8010 Clerical Access Role R8013 Health Records Manager Access Role R8014 Social Worker Access Role R8024 Bank Access Role |
| B0830 Perform Patient Demographics | B0835 Manage Patient Demographics | R5110 Demographic Administrator R8006 Medical Secretary Access Role R8013 Health Records Manager Access Role |
| B0835 Manage Patient Demographics |  | R5110 Demographic Administrator R8013 Health Records Manager Access Role |
| B0065 Undecease Patient |  | R5110 Demographic Administrator |
| B0837 Decease Patient | B0835 Manage Patient Demographics | R5110 Demographic Administrator R8013 Health Records Manager Access Role |
| B0264 Access CSA (Perform Patient Trace) | B1610 Allocate NHS Number | R5110 Demographic Administrator R8016 Midwife Access Role |
| B1610 Allocate NHS Number |  | R5110 Demographic Administrator R8016 Midwife Access Role |
| B8009 Register Patient with Primary Care Provider on PDS |  | R5110 Demographic Administrator |