

Position based access control (PBAC)

A toolkit for implementing simpler and more secure management of access to the NHS Care Records Service

Preface

Why have 'access control positions'?

Strict control of access to patient care records is fundamental to the operation of the NHS Care Records Service (NHS CRS). Position Based Access Control (PBAC) provides a simple and effective mechanism for providing users the access they need in the course of their work, whilst also ensuring that these access rights are properly managed and appropriate for the job they are doing.

Instead of requiring case-by-case scrutiny for every person who requires access to care records, PBAC grants these rights according to the 'access control position' to which their job is assigned. Once the rights attached to each 'access control position' have been approved — along with the jobs included in these different positions — the process of granting access rights for staff becomes much simpler. This toolkit describes how these 'access control positions' can be designed.

Implementing PBAC is a key part of the strategy for Integrated Identity Management which aims to streamline the handling of identity information and integrate it more closely with access control. As well as making worthwhile efficiency savings, this will enable organisations to honour the commitments to patient data security made by the Information Governance Assurance Programme and the NHS Care Record Guarantee.



Contents

- 1.0 Introduction
- 2.0 Readership
- 3.0 Glossary
- 4.0 PBAC: What is it? Why do it? Why do it now?
- 5.0 Implementing PBAC: Step-by-step guide
- 6.0 Case histories
- 7.0 Appendices:
 - Mapping ESR Positions to Access Control Positions



1.0 Introduction

This toolkit will help NHS organisations to improve the way they grant and manage access for staff to the NHS CRS. Position based access control (PBAC) will help reduce the administrative load on Registration Authority (RA) sponsors responsible for approving access rights. Of equal importance, the new management system will enable more robust and timely governance of access — meeting public and staff concerns about who has access to personal clinical records, and why.

PBAC simplifies how access rights are initially granted to a new employee, or someone moving into a new job. Instead of these rights having to be identified and approved for each member of staff, they will be granted automatically according to the access position to which their job is assigned. PBAC builds on the existing, approved Role Based Access Control (RBAC) security model, which provides access for staff to NHS CRS compliant systems appropriate to the job that they do. PBAC links the job to the access rights it requires, thereby reducing the need for access rights to be assessed on an individual basis.

As a result, the workload and number of RA sponsors currently involved in approving access rights to individual members of staff will reduce. PBAC will also bring greater consistency within NHS organisations about how access to care records is controlled and managed.

2.0 Readership

The guidance is aimed at a range of audiences who will have different levels of detailed knowledge about the processes involved in access management:

- RA managers and agents who are familiar with the principles and current practice for access control
- IT staff who are aware of current data management systems and records deployment within their organisation
- HR and other staff responsible for the capture and use of identity information in the electronic staff record (ESR)
- senior managers with responsibility for Information Governance policy (including Caldicott Guardians)
- performance managers in PCTs and other commissioning organisations



- RA sponsors currently responsible for approving individual access rights to staff.

Not all of these readers need to read all of this guidance: some of the detail will be of most use to those tasked with implementing the new process. But it is important that all should have an understanding of the principles involved, because the issue of how access rights to care records are best granted and controlled is crucial to supporting patient confidentiality and meeting the demands of the NHS Care Record Guarantee.

Other toolkits have been produced to support further elements of the Integrated Identity Management programme:

- Developing a strategy for Integrated Identity Management
- Integrating identity management processes between Registration Authority and HR functions, and wider business processes integration
- Implementing the Integrated Identity Management approach

Together they set out a route for NHS organisations towards the goal of simpler, more efficient and more robust management of employee identity and control of access to patient care records.



3.0 Glossary

This document uses a range of terms, some of which have a specific meaning to the Registration Authority community. The following glossary should help the reader.

Access control position	An <i>access control</i> position contains a set of access rights which have been approved and granted through the RA process.
ESR position	An <i>ESR</i> position contains the organisational and financial details of each type of job performed in an organisation, including pay grade, job description, start date, etc. UIM will enable the mapping between <i>access control</i> and <i>ESR</i> positions so that a user moving into an <i>ESR</i> position will automatically be assigned the corresponding <i>access control</i> position.
Approve	The formal authorisation of access rights to an individual user or position. Must be undertaken by an RA sponsor who has been nominated by the organisation.
Grant	The physical allocation of approved access rights to an individual or position. Must be undertaken by an RA Manager or Agent.
Access control assignment	Within PBAC this means the allocation of approved access rights in an access control position to an individual performing a job.
ESR Assignment	The assignment in ESR provides the link between employee and position. Each employee will have at least one assignment but may have more if they do more than one job. The assignment holds contractual data such as the grade, hours worked etc.
Job	Staff perform jobs which are associated with positions or posts.
Job Role	In access control terms this is the mandatory Role Based Access Control attribute granted to individual users or positions. Each job role has associated access rights defined by the national baseline policy. These may be supplemented with other access rights according to local access policy. In ESR terms a job role is defined against the position and is based on a list of values. It is a sub field of the staff group and together these define the 'Job'.



UIM	New software which will provide the electronic management of access control which is replacing the current paper based registration process.
ESR	The Electronic Staff Record (ESR) is the integrated Oracle Human Resource Management System (HRMS) (including Payroll) in use by the vast majority of organisations within the NHS; hosted and maintained by McKesson plc.
Workstructures	The area of ESR that allows the definition and management of the structure and hierarchy within an NHS Organisation. Workstructures consist of organisational units, departments, locations and positions. A Workstructures administrator manages the hierarchy within ESR using a specific user responsibility profile (URP). This role usually sits within either HR or Finance.
Workgroups	A Workgroup is a collection of individuals (team) caring for an individual patient. All members of a Workgroup, subject to their Role Based Access Control (RBAC) profile, have access to the patient's clinical records where a legitimate relationship has been created with that Workgroup.



4.0 PBAC

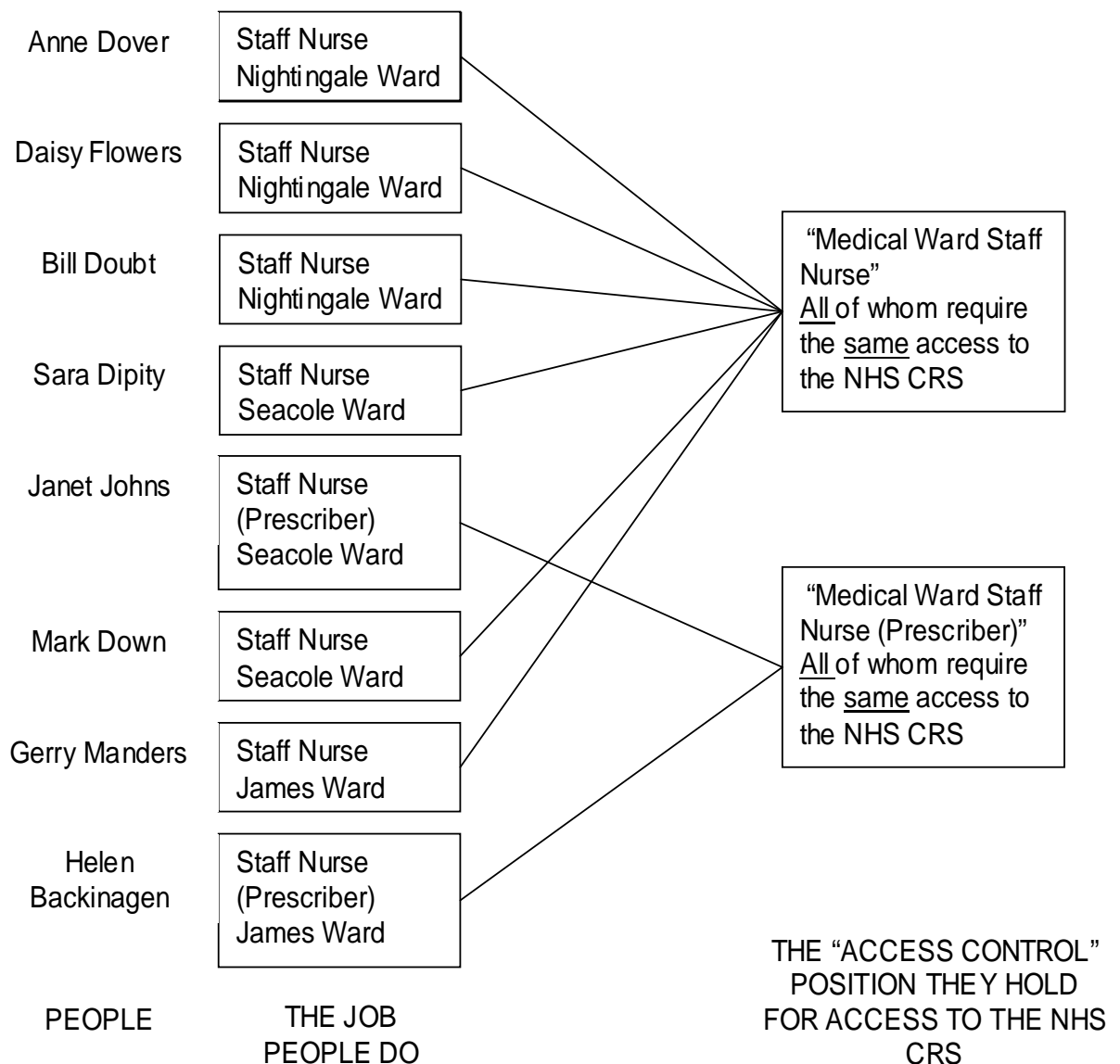
4.1 What is it?

PBAC simplifies the way that access rights to the NHS CRS are provided. Instead of the access rights for each job being ascribed individually every time someone starts work or moves into a new job, jobs are assigned to access control positions that carry a set of approved access rights. These rights are assigned automatically to staff as they move into a job, and rescinded as they leave. If staff move to jobs associated with a different access control position, their access rights are altered accordingly.

Individual employees will also be governed by Professional and Local Codes of Conduct, and local terms and conditions of employment. These are not affected by PBAC and provide important supplements to the security of the NHS CRS.

The following diagram demonstrates how individuals, jobs and access control positions relate within PBAC:





4.2 Why do it?

Implementing PBAC will reduce the workload of RA sponsors who currently have to approve access rights for individual members of staff, usually within their department or team. Some 28,000 people across NHS act as RA sponsors and have to be trained in their responsibilities. At present, they may be called on at any time to approve individual access rights. PBAC will largely remove this responsibility and reduce the number of sponsors needed. With PBAC, a decision need only be made once as to the access rights required for the access control position which is associated with each job.



PBAC will also ensure greater consistency and improve the quality of RA processes. A simpler system and fewer sponsors will decrease differences in interpretation and practice around which access rights are appropriate.

Anecdotal evidence indicates that many NHS organisations are already using PBAC-like solutions. For example:

- When a new system is being deployed there is a review of the jobs people perform, and agreement on which access rights they need. While there is an investment in time to set this up, a quicker and more efficient process is established that ensures access control operates without unnecessary delay.
- Other organisations assess at the time of when recruiting to a vacancy or filling a post an assessment is made as to whether the requirements for access to the NHS CRS have changed. If not the new recruit is approved, via a sponsor and granted, via an RA Agent, the same access rights as the previous post holder .

Adopting a PBAC approach both improves the governance of these informal processes and prepares the organisation for the changes to the electronic systems of registration that are due later this year.

4.3 Why do it now?

New registration software — User Identity Management (UIM) — is being introduced in 2009 which will replace the current paper-based systems for registration of staff who require access to NHS CRS. The UIM system will enable a direct interface between this list of staff (the Spine User Directory of NHS CRS) and the Electronic Staff Record (ESR): the world's largest HR and payroll system carrying job details and employment and pay records for more than 1.2 million people working in the NHS. ESR is also being enhanced to facilitate this interface. Even where a significant number of NHS CRS users are not directly employed staff and do not appear on ESR, PBAC will enable organisations to derive optimum benefit from the new UIM system.



Employee information held in ESR does not include their access rights to NHS CRS. Now, the direct interface between the two systems will — through the use of PBAC — allow access rights to be managed from ESR. This will create more secure, responsive and efficient access control. Implementing PBAC is therefore critical to the operation of the ESR interface to UIM.

5.0 Implementing PBAC: Step-by-step guide

This toolkit contains ideas and advice on how NHS organisations can implement PBAC. The content draws on experience from several pilot projects representing different sectors with varying mixes of directly-employed and non-employed staff: acute trusts, PCTs and mental health trusts. The case histories provide practical examples of how individual trusts set about the exercise.

How you begin implementing PBAC will depend on where you are starting from, and your strategic goal for identity and access management within your organisation (see [Developing a strategy for Integrated Identity Management](#)). There are broadly two different approaches to designing access control positions:

1. Group together bundles of existing access rights which are shared across a number of jobs, e.g. allied health professionals or general administrative staff (see step 3 A 'bottom up' approach).
2. Review access rights across the organisation and look to see how these can be combined into a number of 'access control positions' which cover the access requirements of a range of similar jobs (see step 3 A 'top' down approach).

Which approach you choose will be influenced by:

- whether you will shortly have to review access management in anticipation of new or updated patient care records systems
- the mix between employed (ESR-listed) and independent contractors and their staff¹(not ESR-listed)
- the make-up of the team conducting the exercise.

¹ Independent contractors cover the full range of primary care services including GPs, pharmacists, dentists, opticians, etc. and the staff that they employ.



Within the step-by-step guide, the amount of technical detail has been kept to a minimum in the interests of the wider readership. More detailed information for the team conducting the PBAC programme is contained in the appendices.

Further information is also provided on the following websites which should be referred to when using this toolkit. They will provide updates which may become relevant as your project develops. It is important that all staff involved in PBAC are kept up to date with any changes in requirements, both during the project and after its completion.

For information governance:

<https://www.igt.connectingforhealth.nhs.uk/>

For Registration Authority issues:

<http://www.connectingforhealth.nhs.uk/registrationauthorities>

For ESR:

<http://www.esrsolution.co.uk>



5.1 Step 1

Gain board level endorsement for PBAC implementation

Board members will be aware that robust and efficient control of access rights to care records will be a significant element in how the overall performance of their organisation is judged. It is not essential that board members have a detailed understanding of how access is managed; but they should be asked to endorse the PBAC process as part of an overall strategy for identity management and access control within their organisation (see [Developing a Strategy for Integrated Identity Management](#) toolkit).

A report to the board from the access control lead should cover the following points:

- how many staff currently have access to care records and how access rights are granted
- how many RA sponsors are involved in approving access
- how PBAC will simplify the process for granting access
- the reduced administrative load on sponsors
- the greater security (particularly removing access rights when someone leaves a job) and clarity of access control
- the 'fit' of PBAC within the wider integration of identity and access management
- the marginal impact on staff (those who need to create and manage the positions).

Checklist

Report presented to board, setting out the high level case for PBAC

Outline proposal of how PBAC is to be implemented

Proposed terms of reference for the group

Proposed membership of project team and any implications for workload and staff resourcing (see Step 3)

Outline of timescale and projected outcomes

Communication with senior managers and wider staff audience

Timeline:

Month one - endorsement for the project given after presentation at the board meeting



Tips:

- 1.** The board should be made aware that PBAC will have minimal cost implications to implement and offers worthwhile (though difficult to quantify) cost savings in terms of reduced administrative load.
- 2.** Detailed scrutiny or input from board members is not required during the project, but the PBAC solution will have to be signed off by them before being implemented.
- 3.** The report should contain some criteria by which progress can be measured (see Step 6).
- 4.** The report should make clear that PBAC implementation will have little or no effect on most staff in terms of their day-to-day work.



5.2 Step 2

Establish project team including representatives from RA, information governance, IT and operation of ESR. Staff group representatives may be invited to participate, and will be consulted as the project develops.

The report to the board in Step 1 must have included a proposal for who the project team will comprise. This is likely to include:

- the manager responsible for RA processes and policies and agents who carry out allocation of access rights
- an appropriate individual to advise on the technical detail of PBAC implementation and interfaces between different systems, this person is likely to have an RA and/or IT role
- a manager engaged in operation of the ESR system within the organisation (if the organisation is seeking to use the UIM/ESR Interface to manage their identity and access management). Participation of an ESR manager is not required for organisations where most staff accessing care records are not direct NHS employees (i.e. independent contractors and their staff and therefore not on ESR) and the strategic decision has been taken to use UIM alone for access control.

The Caldicott Guardian/clinical director etc. will be aware of the team's brief and must be kept informed of progress. Representatives from clinical staff groups will need to be consulted on access requirements as the project unfolds, and agree the details of access rights that affect them.

Checklist:

Project team members identified and recruited
Project team terms of reference in place and agreed
Project plan with timeline and objectives
Communication plan prepared and distributed

Timeline:

Month two - set up the team and arrange first team meeting

Months three to four - subsequent team meetings scheduled as



members have progress to report

Tips:

1. Briefings to staff and managers should emphasise that the objective is to improve efficiency and control of access rights, not change existing rights.
2. Awareness among the team of current access control procedures is essential.

5.3 Step 3

Design and implement the access control positions

A range of factors will influence how you set about developing a PBAC system for your organisation:

- a) The existing deployment of patient care records systems in the organisation, and the systems for access control.
- b) Whether a new or updated care record system is soon to be introduced
- c) Are most staff who have access to patient care records directly employed (and therefore present on ESR)?
- d) The make-up of the team undertaking the project.

The variations in approach hinge principally on how far the exercise can travel before wider staff consultation is involved: does it require a fundamental re-appraisal of what access rights are needed and how they are granted to various jobs or is it a rationalisation of existing, person-by-person control procedures?

Tips:

1. The eventual goal for many organisations will be a direct link between managing access rights and operation of the ESR. Designing your positions should anticipate this linkage. Even where your main user base is independent contractors and their staff, you should consider in designing your positions how they will be utilised in UIM.
2. The main aim of the exercise is to simplify the procedure for granting access rights to staff and to be confident in its security.



3. Ensure that a sensible and consistent means of naming access control positions is defined. Names should reflect the job roles that each access control position covers and should be easy to understand from the title alone.



5.4 Option 1 – A ‘bottom up’ approach

In this option the project team use their knowledge of the access rights already granted to individuals to develop sensible ‘groupings’ from which to derive a series of access control positions.

The starting point is to review the documentation that exists in relation to current access rights. This information will come from the [RA02](#) forms. The suggested steps are:

1. Group RA forms into those that have similar RBAC job roles – e.g. those with ‘Hospital Doctors’ or ‘GP’ access. You could also refer to your ESR positions and the hierarchy that the ESR system uses since it can provide valuable information in relation to how individual jobs are grouped together.
2. Review the differences between the [RA02](#)’s in these groupings. Where most of the RA02 jobs have an access right consider adding to all or vice versa (e.g. remove an access right if only one or two jobs have it). There is a need to be pragmatic in this exercise.: You should take into account ‘the way your organisation does things’, the other non-technical controls that govern inappropriate access, and the fact that just because someone has the ability to do something in relation to an electronic record, this doesn’t mean they have to. As a result you may end up with groupings that include access rights that only one or two people currently have and apply them to a larger population.
3. Once you have agreed what these groupings are, they become your access control positions. You then complete the RA06 form for each position.
4. These [RA06](#) forms and the positions they relate to should be approved formally by the organisation. It is recommended that this sign off is completed under the auspices of the organisation’s governance structure – this may mean that a sub-group of the board, main group of the board or a delegated group undertake this role.
5. When UIM is implemented these approved [RA06](#) forms will form the basis for inputting positions into the system.



Timeline:

Month three - produce a first draft set of access positions to cover most staff. Detailed consideration of the access positions before sharing with clinical leads and managers

Month four - clinical leads and managers to review the impact on access rights for their own staff groups

Month five - resolve any variations between existing and proposed access rights

Tips:

- Use [RA02](#) forms, ESR and other local sources of data to develop groupings
- You should aim to create a number of positions that amount to no more than 20 or so in a large NHS organisation. In a smaller organisation, such as an independent contractor, the aim to should be to have less than ten positions.



5.5 Option 2 – A ‘top down’ approach

The deployment of a new system, such as Lorenzo or RiO, allows the opportunity to review who needs access to that system, and for what purpose. From this it is a short step to identifying which jobs have similar access requirements and arranging these into groupings for access management purposes. The suggested way forward is:

1. Best practice suggests that the review should involve discussions with clinical staff and managers to verify and agree access requirements. A collective briefing on patient care records and access management may be needed as a prelude to these discussions. Where practical, bank staff should be included in this review.
2. The starting point should be to review the 23 rationalised job roles contained in the [National RBAC Database²](#). These roles have been widely consulted upon and represent a set of nationally approved baseline access rights appropriate to the jobs people do.
3. Because not all NHS organisations work in the same way, some organisations will want staff to have additional access rights to those in the RBAC Database. One way of clarifying what these are might be to map the patient journey through episodes of care, and establish any additional access rights that staff may require as the journey proceeds. Many organisations undertake these sort of mapping sessions as part of their process improvement and service redesign work.

² To be found at

<http://nww.connectingforhealth.nhs.uk/registrationauthorities/access-control/rbac>



Timeline:

Month three – briefing / discussions / patient journey mapping sessions with clinical heads and managers to agree required access rights

Month four – review of RA02 forms / mapping sessions outcomes and first draft of access positions with shared access rights

Month five - refinement of access positions and agreement with clinical leads and managers on modified access rights

Tips:

1. This approach is suitable for any NHS organisation and especially relevant where a new or updated patient care records system is soon to be introduced
2. Review of RA02 forms will be time intensive. A team of up to four staff may be needed for a period of up to six weeks.
3. For consistency, use RBAC access codes to describe access rights where possible.



5.6 Step 4

Preparing access control positions for uploading into UIM

Access control positions can be created, and the efficiency gains achieved, prior to the introduction of UIM and the ESR interface. However you need to consider preparing your positions for uploading into UIM.

UIM will be a paperless system that will also introduce improved governance into the RA process. Part of this will be the ability of a manager to 'assign' individuals to 'positions' that they are responsible for. This reflects real life where managers often redeploy staff to cover illness, emergencies and annual leave.

When the initial design of positions is undertaken it is important to consider these managers as separate positions. In UIM these separate managerial positions will have the ability to 'assign' people to other positions.

UIM will support a hierarchy of positions with 'higher level' positions being able to assign individuals only to those positions that they are responsible for.

Further 'technical' guidance on how to upload positions into UIM will be made available once system development has been completed.

Timeline:

This step can be undertaken in combination with the previous step in order to minimise the effort required. However, whether undertaken in parallel or separately, the additional effort is likely to be small (less than a week).



5.7 Step 5

Linking access control positions to ESR positions

This section is aimed at those organisations which intend to use the UIM/ESR interface. This step can be planned prior to creating positions in UIM, but the technical linking can only take place after positions are uploaded into UIM.

User Identity Management (UIM) will replace the paper-based administration of access control with electronic forms and signatures. Through the UIM system, an interface can be established between ESR and information held on the Spine User Directory of the NHS CRS. Once this is in place, access to NHS CRS can be managed with data captured and stored in ESR and shared for RA and HR purposes (see *Integrated Identity Management Implementation Approach* toolkit).

The mapping of access control positions to ESR positions is a prerequisite for the interface with the UIM system. Positions in UIM will define the access rights needed by staff to do their job. In ESR employees are associated with a position which defines the job that they perform from an HR perspective. Linking the two types of position will enable the automatic assignment of access rights for staff using NHS CRS.

The benefits are in the streamlining and simplification of process flow between HR and RA, ensuring that data is entered only once and that all employees in similar jobs will have the same set of access rights. It also enables prompt allocation and withdrawal of access rights for starters and leavers and when someone changes their job.

It is recommended that the mapping exercise is conducted concurrently with implementing PBAC. You can use data from ESR to inform your decision making on access requirements and save revisiting these decisions later on.

The process for linking access positions to ESR positions is described in detail in Appendix 1.



Timeline:

Where ESR positions mapping is done concurrently with the definition of access control positions then the exercise should fit within the timeline for Step 3, either option 1 or 2.

Where the mapping exercise is conducted later the timing will depend on a number of factors including the size and complexity of the organisational set up in ESR, the number of access control positions agreed, the ease of correlation between the two, and the number of staff on the team. On average you should allow 3 – 6 weeks to conduct the mapping exercise if done subsequent to Step 3.

Tips:

1. Use this exercise as an opportunity to revisit the existing set-up within ESR: consistency of information, correct employee assignment to job etc
2. Expect a 'many-to-one' relationship between ESR positions and access positions
3. Ignore ESR positions which require no access to NHS CRS



5.8 Step 6

Improvement performance criteria

The deployment and use of patient care records presents a very varied picture across the NHS. But for most organisations using NHS CRS, the current management of access control typically requires individual identity checking and assignment of rights conducted by RA agents and sponsors. These processes take place separately from HR and other processes relating to identity capture and management.

Though robust, this existing approach has significant flaws:

- duplication of activities between HR and RA staff
- a heavier-than-necessary workload on RA agents and sponsors
- possible inconsistencies in the rights granted to different staff doing the same job
- no guarantee of timeliness in granting and withdrawing access rights.

The success of implementing PBAC can be measured by:

1. Consistency

Once the access control positions have been agreed and approved at senior level, access rights can be assigned automatically by staff whose own position provides this ability. The workload of RA sponsors is reduced.

2. Timeliness

ESR, UIM and the interface between them ensures prompt granting of access to new staff, and timely modification or withdrawal of rights as people change jobs.



6.0 Case histories

6.1. Designing access positions for broad staff groups Nottingham University Hospitals Trust

Nottingham University Hospitals Trust employs almost 14,000 staff working across the full range of acute sector services. At the start of this PBAC exercise 3,500 staff held NHS CRS Smartcards, and the intention is to roll out card usage more widely. RA and IT decided to examine PBAC as a means of managing existing users and facilitating the addition of new ones.

A small team was formed, bringing together people with experience of RA and access processes along with knowledge of the recently introduced ESR system and broader awareness of the use of IT systems across the organisation. The team was headed by an IT manager with responsibility for maintaining approved information governance within the trust. Authority for the exercise came from the trust's policy to improve and extend NHS CRS Smartcard usage.

The aim of the team was to reduce the administrative load on RA managers and sponsors involved in granting access rights. Taking the example of the 500 or so junior doctors moving into the trust every August — all starting with almost identical access rights — the team set out to devise a small number of staff groups with common access needs. Choose and Book, PACS and PAS are the three national systems used within the trust, and the team were able to define seven group positions where the same access rights applied for the majority of staff. The detailed access rights were defined from this table.

	Group	Required Access
P1	Senior Clinician (Clinical Directors, Consultants, Professors, ST2s)	Standard PC Access (PC, Internet, Email)
		Choose & Book
		PACS (IMPAX)
		PACS (Web1000)
		PAS (Drs Orders, Results, Bedstates, Transfers and Discharges, Tracking, View Documents)
P2	Clinician (F1,F2,ST1)	Standard PC Access (PC, Internet, Email)
		PACS (IMPAX)
		PACS (Web1000)
		PAS (Drs Orders, Results, Bedstates, Transfers and Discharges, Tracking, View Documents)
P3	Nursing Level 1 (Registered Nurse, Matron, Sister, Ward Manager)	Standard PC Access (PC, Internet, Email)
		PACS (Web1000)
		PAS (Nuring Orders,Results, Bedstates, Transfers and Discharges, Tracking, View Documents)
P4	Nursing Level 2 (Unqualified Nursing Staff)	Standard PC Access (PC, Internet, Email)
		PAS (Blood Orders, Results, Bedstates, Transfers and Discharges, Tracking, View Documents)
P5	Allied Health Professionals	Standard PC Access (PC, Internet, Email)
		PACS (Web1000)
		PAS (Results, Bedstates, AHP Ordering)
P6	Medical Sec	Standard PC Access (PC, Internet, Email)
		Choose & Book
		PAS (Bedstates, Transfers and Discharges, Tracking, Create Documents)



P7	General Admin	Standard PC Access (PC, Internet, Email)
		PAS (Tracker)

Although the team did look at RA roles and business functions and at national job roles within ESR as a method of classifying staff, they found too many role complexities and inconsistencies in title usage. These seven positions were developed using their own combined experience and knowledge of access management, ESR and IT usage — starting with groups requiring highest levels of access.

The team acknowledged from the start that these group positions would need further individualisation, particularly for access to local systems, but were confident that the majority of access rights could be controlled and granted in this way. The hierarchy of the seven positions relates solely to levels of access rather than levels of seniority within the organisation.

Their next step was to look for pre-defined fields in ESR which could be used in association with the group positions to facilitate management of access. The team took three fixed fields — Occupational Code, Role and Staff Group — and ran the 13,982 individual staff records through spreadsheet filters to produce 642 staff categories. These 642 categories were manually cross-referenced to the seven access group positions. Most fitted clearly into one of the seven groups, but 51 fell into more than one. These are being looked at individually to ensure that correct access rights are granted.

Darren Dovey, ICT Services Manager for the trust, did most of the detailed work involved in developing the seven access group positions and linking these to ESR positions: “Because of the different strands of experience and knowledge we brought to the exercise, we were able to work as a small team without calling on other staff resources. It took us about a week of proposal and discussion to arrive at the seven group positions, and producing the 642 categories from ESR was done using filters in Microsoft Excel once we had decided on which fields to use.”

“We are confident that the system we have developed will grant and manage the large majority of access rights appropriate for most staff. The UIM interface being developed nationally will refine this still further, and we are doing more work on departmental and local systems to see how best to relate these to the whole system. At that stage we will be talking to clinical leads and others to ensure appropriate access rights continue to be granted. But if the system works well, individual members of staff should notice no difference. The gains are all to do with reducing the administrative load on sponsors, and enhancing the security of access management.”



6.2. Introducing PBAC across two primary care trusts North Mersey Health Informatics Service (HIS)

North Mersey HIS provides information systems and technology support for two neighbouring PCTs: Liverpool PCT and NHS Sefton. It launched the Lorenzo care records service across the trusts' podiatry departments in 2005 and has been steadily rolling out its use. Some 4760 staff for Liverpool PCT and 1020 staff for NHS Sefton now carry NHS CRS Smartcards.

As usage of the NHS CRS Smartcards spread, North Mersey HIS and the Trusts' RA teams wanted to achieve greater consistency among sponsors in the allocation of individual access rights. So they proposed a review of generic job roles, developing process maps of the patient journey through care and identifying the access rights needed at different stages by administrative and clinical staff. The proposal was approved by the National Care Records Service Implementation Boards for the two Trusts, who were responsible for ensuring safe and effective deployment of the new system.

The project manager and a co-ordinator involved in RA work set out to review access requirements. They did this through process mapping sessions with different staff groups set up across community services. The sessions tracked the patient journey from referral into their service to discharge. From this the sequence of activities were defined. Groups of up to twelve staff attended these sessions — rolls of wallpaper and post-it notes were used to create and refine the maps during discussion. Once agreed, these maps enabled the project team to identify the access rights and role-based access codes needed by different staff as treatment progressed. The access varied in accordance with what each member of staff actually did.

The team then referred this information to the activities and access rights attributed by the existing RBAC programme to 17 generic job roles (eg community nurse, all AHPs, clerical staff...). Starting from the baseline access rights generated by the RBAC programme, they were able to allocate additional activities which the process map indicated might be needed by different staff within each job role. These became the access positions for the generic job roles. Not all staff included in these broader positions will need all the access rights granted to them, but no rights are granted in any position which would compromise the overall security of patient records.

The proposed position access rights for each job role were presented to clinical leads for comment and approval. These positions were then reviewed and signed off by the Implementation Board.

Kathy Simons, NPFIT project manager with North Mersey HIS, has been involved with the PBAC initiative from the start. "It took about 12 months for us to get from when we went "live" with our first Community Team back in 2005 to where we now have access rights granted generically across 17 job roles. Creating the generic role profiles allowed us to make the process of identifying the appropriate role profile a lot easier, quicker, and more transparent. The profiles were discussed and agreed with the service leads so they could see how we had come to the decision about which role profile would "best fit" their particular service. Obviously, it is only when staff themselves are actually using the position profile that we can see whether it is the most appropriate, and service leads/RA sponsors are encouraged not to change access rights without first consulting with our team. Any changes might mean that we



need to review our profiles and either update or create new ones that are more appropriate.

“I have since mapped the identified RBAC roles within the profiles to actual ESR job roles and these are all contained in a single spreadsheet. The aim of this document is to control access rights for almost all NHS CRS Smartcard holders, although individual adjustments can be made and approved by an RA sponsor at department level and the North Mersey HIS Implementation Board. As work processes change, so the generic access rights may have to be adjusted. Things don't stand still, but I'm confident that PBAC gives the trusts a simpler and more consistent method of access management.”

6.3. Introducing PBAC alongside the London-wide RiO system West London Mental Health NHS Trust

West London Mental Health NHS Trust provides a full range of mental health services for a population of nearly 700,000 adults and children in Ealing, Hammersmith & Fulham, and Hounslow. It employs 4,000 staff across 32 sites, including high secure services at Broadmoor Hospital.

In mid-2007 the Trust embarked on the process of enabling NHS CRS Smartcard access to the NHS CRS for some 1,700 staff. This anticipated the implementation of Version 5 of the RiO information system, co-ordinating community and mental health care records across London. Introducing the latest version of RiO meant that a new process of role-based access mapping would be needed. The Trust decided to use this opportunity to develop this mapping into position-based management of access.

The project was led by a team comprising leads from Clinical Transformation, RA and Information Management within the Trust, supported by a consultant with previous experience of introducing new NHS CRS-related programmes. Taking the work already done on role-based access, the team set out to define a series of access profiles that would cover all positions in which staff require access to the system. From almost 30, they got down to 18 and eventually 12 distinct profiles. These access rights were then attributed to positions, documented in a spreadsheet, and presented to the Trust RA group for approval.

At every stage — the project team set-up, the role and position mapping, and the RA sign off — clinical staff have been closely involved. The whole project goes 'live' in early 2009, but within the overall 18 month timeline, the PBAC design took only three months after completion of the role-based mapping.

Denise Butterfield provided the project management expertise to guide the implementation. “In this instance, position-based profiling was the lesser part of a much larger project to introduce Smartcards for staff across the Trust. Looking forward, taking the PBAC approach will reduce the load on RA sponsors as individual staff move or change their jobs. Our aim was to minimise the number of different access profiles to keep management of the system as simple as possible whilst retaining a high level of information governance as required by the NHS Care Record Guarantee. With the involvement of clinical and other staff who will actually be using the new system, we were able to get these down to a sensible number that still covers all the different access rights that staff need.”



6.4 Hertfordshire Health Community Using PBAC to strengthen and simplify access control

Hertfordshire Health Community comprises two PCTs, an acute hospital trust, and a mental health care trust. It already had a well-developed NHS CRS Smartcard system in place covering a huge diversity of staff in both primary and secondary care — from GP practice receptionists and admin staff through the full range of community health practitioners to trust executives and hospital consultants. As of late-2008, 7,000 staff within the Health Community held NHS CRS Smartcards including staff in all local GP practices accessing the CRS system.

Introduction of a new community health and primary care system (TPP release 3) during 2008 meant that existing access rights would have to be revisited and checked for all current cardholders as well as new joiners. This would involve referring to all the role-based access rights granted to each job. The RA team was faced with the challenge of completing this re-assignment within less than six months across the whole Health Community.

The task was to add a host of business functions to each role for correct access to the clinical product, whilst keeping control of who had what access. When RA02 forms were used to examine each role, it soon became clear that access was not that much different for differing types of users i.e. admin, clinical staff, clinical managers etc. So after looking at different roles over a period of three meetings, it was decided that the number of profiles could be reduced whilst still providing sufficient coverage of access rights.

The Information Governance access group supported this approach and so the team developed generic profiles to attach to different types of role codes. In the few cases where no appropriate access codes existed, brief descriptions were written to ensure control of access to the clinical system in certain critical areas.

Once profiles had been developed that granted appropriate bundles of access rights to different staff, these were circulated and discussed with staff groups, GP practices and an Information Governance Group comprising clinical representatives, information management, HR and Trust managers. The initial exercise produced some 90 profiles, many of these covering different administrative staff within GP practices.

By focusing on which areas of the records system these administrative staff would need access to, and grouping them broadly together with restricted rights, the number of profiles was reduced to 19.

These profiles were discussed again with different staff groups for approval before sign off on the final set. These were then documented within a spreadsheet that matches jobs to the bundled access rights, and acts as the control mechanism for access across all the organisations.

Pam Lumsden, RA & NACS re-organisation project manager led the project. "This approach both simplifies and strengthens access control across our different organisations. Setting it up did involve a major mapping exercise. We had to list business functions within the NHS CRS system, link them to the TPP mapping document, and make it more conducive to explanation by adding new descriptions



where no RBAC codes existed for the TPP-described function. Then we created the spreadsheet which grouped jobs according to the access rights they needed. I had a team of three extra staff for a six week period to do that work. But the effort is worth it in terms of more robust information governance and a more easily managed process in the future. I'd now like to link this list of profiles with the ESR, which could deliver further efficiencies in managing Smartcard access.

"Time has gone on and overall PBAC is working well. But as new units and services join the community we have to revisit profiles and add access rights for different needs, i.e., path lab, CSA etc. In most cases I have been able to explain the situation by email to the RBAC access group and get agreement on changes — with the provision that if there is any conflict we will meet to discuss.

"The thing to remember is that once you have a profile it is not set in stone: it will need regular updating for clinical changes within the systems or because of new spine applications. So we must be able to change templates easily, and keep on top of any new products coming in that can affect certain profiles.

"Linking these profiles to ESR, you are matching an occupational role to a clinical access role. In some cases where people need access to two different applications they may have two roles matched to them, to enable them to do their job. This is not a problem but does create queries from users sometimes because they think we have their organisation role wrong. For this reason, careful consideration must be given to the naming of the profiles, as well as resourcing the ongoing update work."

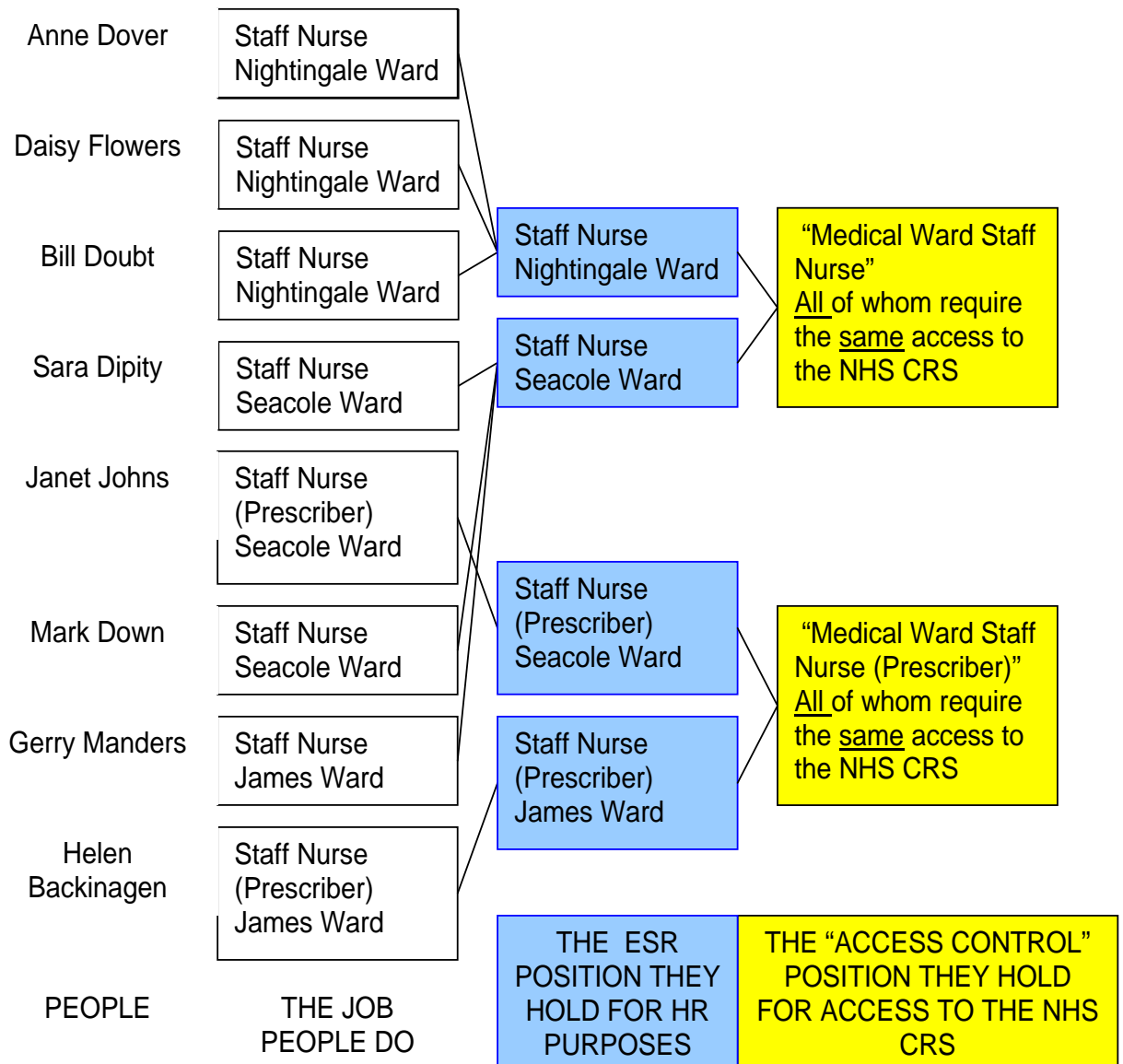


7.0 Appendix 1

7.1 Mapping ESR Positions to Access Control Positions

How do ESR positions relate to access control positions?

The following diagram illustrates how jobs map onto to ESR positions and how these then map onto access control positions.



In this diagram each person has a single job though in practice a person could perform more than one. ESR positions (blue boxes above) are defined as part of the workstructure hierarchy within ESR. Identical jobs are mapped onto the same ESR position so, for example, there are three people assigned to the ESR position “Staff Nurse Nightingale Ward” and three other people assigned to the ESR position “Staff Nurse Seacole Ward”.

Different groups of ESR position are shown next to each other. Each group is then mapped to the appropriate access control position in UIM. In this case the two ESR positions just discussed map onto a single access control position “Medical Ward Staff Nurse” because this group of ESR positions has the same access control requirements. The fact that in ESR they require separate cost codes (for example) has no bearing in access control terms.

As this example shows, there will usually be more jobs than ESR positions and more ESR positions than access control positions. The task of managing access control positions via ESR requires the building of a mapping table between ESR positions and the corresponding access control positions.

7.2 Before Beginning the Mapping Exercise

A few points to bear in mind whilst conducting the mapping exercise:

1. This is an opportunity to review the set up within ESR. The structure may not have been assessed since implementation and it is possible that certain changes are required to bring it up to date. You should ensure that:
 - Workstructures correctly reflect the organisational hierarchy
 - There is consistency of information held in the position title and grade description fields. Both of these are free text and it is possible that — either due to inaccuracies in the legacy system from which the data was migrated when implementing ESR, or subsequent lack of procedural control over data entry — that there are inconsistencies which will make analysis for mapping purposes difficult.
 - All employees are assigned to the correct position for the job that they perform. Many organisations, especially PCTs, either have remodelled or plan to remodel their workstructures due to mergers/demergers and the change to commissioning and provider services. The two exercises could be conducted at the



- same time to save revisiting the same information at a later stage.
2. It is expected that there will be a 'many to one' relationship between positions in ESR and access control positions.
 3. A number of positions in ESR will have no need for access to care records systems and therefore mapping will not apply. Examples might include purely administrative functions such as HR, Payroll and Finance.
 4. Conversely there may be certain access control positions which have no match in ESR because they relate to not directly employed staff. Examples include Pharmacists and GPs for PCTs and students, locums and consultants for acute trusts.



7.3 Suggested Mapping Methodology

Steps:

1. Follow the steps in the main part of this toolkit to define an initial small set of access control positions. Allocate each one a unique name and reference³ to make it easier to assign to an ESR position. It is possible that you will need to amend the initial list of access control positions as a result of the information from ESR and the mapping exercise.
2. Use the 'ESR Organisation Positions Analysis' report or equivalent to produce a table containing a complete listing of all positions defined in ESR for your organisation.
3. Analyse the data by key fields in order to map the potentially 1,000s of ESR positions to a few access control positions.
 - Whilst position title or grade description may appear to offer the easiest way to group ESR positions this will not be possible unless these have been entered consistently, because they are free text fields. Instead use of the job role, staff group or occupation code may be more advisable as these are validated against a nationally defined list of values. A further alternative is to use the financial cost code although this will be unique to your organisation.
 - Group the data by one of the above fields in order to identify the significant distinct groups of ESR positions. This should significantly reduce the list of ESR positions to one which contains an ordered list of different position types. As an example an acute trust has over 13,000 employees, some 3,000 ESR positions but only 650 unique types.
4. As you conduct this exercise you may notice discrepancies in the data in terms of consistency of the free form fields and in the correct allocation of staff group, occupation code and job role to each position. Where corrections are necessary they must be made in ESR after which it will be necessary to re-run the 'ESR Organisation Positions Analysis' report.

³ Once UIM is deployed it will automatically generate a unique ID but for now just adopt your own numbering



5. Where a user has links to multiple positions within UIM or ESR (through assignments) it will be important to map ALL relevant ESR positions for that user to the corresponding access control positions. This arises because once an ESR position is mapped to an access control position and is assigned to a user, any preexisting access rights stored in the Spine User Directory will be replaced with those corresponding to the ESR position. Unless all the relevant ESR positions are mapped the user will not have the complete set of access rights they require.
6. Map the smaller number of ESR position groups to the appropriate access control position from the set defined in step 1 above. The expectation is that for the majority of ESR positions one of the access control positions should match.
7. Where there is a match add your access control position reference to each ESR position record within the table. This reference should be added to all ESR positions within the matching category to ensure that every ESR position has a mapping.
8. Where there is no direct match or more than one match, a number of options are available:
 - For unusual situations where more than one access control position applies to the ESR position consider the following options:
 - a) Merge the access control positions into a single position.
 - b) Split the position in ESR by creating a new position and reassigning the employees to the new positions.

Each case will have to be assessed on its own merits to find a solution but the outcome needs to be the mapping for each ESR position to only one access control position. This is because the ESR/UIM interface will only permit one position to be linked.

- For situations where there is no equivalent access control position to the ESR position either:
 - c) The ESR position may require no NHS CRS access in which case no mapping is necessary; or
 - d) You will need to define a new access control position, possibly basing it on an existing one.



9. Once the mapping table has been completed it must be reviewed by those responsible for Information Governance to ensure that it accurately defines the requirements for access to NHS CRS systems for each ESR position. A consultation with each department head may be required either during the mapping exercise or subsequent to the first draft being defined.
10. Finally, a senior sponsor within IG and/or HR must sign off the mapping, recording their name and UUID. This sign-off is essential to ensure that there is auditability and accountability of the automated inheritance of access rights that will be driven via the interface between ESR and UIM.

Acknowledgements

The suggested methodology described above has been compiled with the co-operation and input from three PBAC pioneer NHS organisations: Liverpool PCT, West Hertfordshire PCT and Nottingham University Hospitals.

