

## **Developing a Strategy for Integrated Identity Management**

### **1.0 Preface**

This paper is jointly agreed by the NHS Central ESR team and the NHS CFH Access Control team and its purpose is to support NHS organisations develop a strategy for Integrated Identity Management. Further documentation will be available which will support detailed implementation.

Since April 2008 new NHS Employment Check Standards have been required of the NHS. Their adoption enables trusts to declare their compliance with the relevant Healthcare Commission core standards as part of the annual health check 2008 / 09.

Similarly, robust identity checks (using the same identity management standards) are carried out by each NHS organisation's Registration Authority (RA) to verify an individual's identity before allowing access to Smartcard enabled IT applications within the NHS Care Records Service (NHS CRS), such as Choose & Book, and the Electronic Prescription Service.

Combining these two parallel activities into a single integrated identity management process will result in improved safety and productivity – saving both time and money.

A joint project between the Department of Health, NHS Connecting for Health, NHS Employers and the Electronic Staff Record (ESR) project has already helped organisations tackle some of the issues in this area, and has worked with over 100 NHS trusts in England to deliver improvements. Significant benefits have been gained by trusts through establishing a single integrated identity management process, providing more robust governance around data security, and doing things only once. Work is currently underway to encourage this practice across the NHS.

To further support this initiative, two new technical solutions are being developed to deliver further benefits to NHS organisations; User Identity Manager (UIM) and the ESR Interface.

UIM will replace the current registration software and will remove the paperwork involved in the current RA processes. It will also electronically record Position Based Access Control (PBAC). PBAC provides a simple and effective mechanism for allocating users the access they need in the course of their work, whilst also ensuring that these access rights are properly managed and restricted for the job they are doing.

HR functions currently update ESR when changes are made regarding an employee's assignment to an established position. The ESR interface will be triggered by such changes and will automatically update an individual's access rights to NHS CRS compliant systems, reflecting the requirements of their new position. It will enable the management of access control via a single point of data – the change to the employee's position within ESR.



All organisations will benefit from examining their identity management processes with a view to integration where these are duplicated. Depending on their composition, each NHS organisation will need to decide which implementation model to deploy to exploit the benefits of the two new technical solutions, centred either on UIM or ESR plus interface, or a combination of both.

The benefits will include:

- better assurance to the board that identity management is robust in respect of employees and access to data
- the productivity gains to be realised by reducing the duplication of activity in relation to identity assurance
- improved governance and timeliness of updates.

This toolkit shows a variety of approaches to achieving and implementing effective Integrated Identity Management. They reflect the typical scenarios encountered by the 100 NHS organisations, but are not exhaustive.

## 1.1 Readership

This toolkit is aimed at board-level management within NHS organisations. It assumes awareness of the NHS Employment Check Standards and the objectives of the NHS CRS, along with an understanding of the information governance issues surrounding personal data.

Further toolkits will be available that deal in more detail with specific areas of operational support for the strategy:

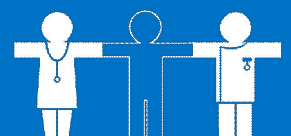
- HR and RA business process integration for identity capture and management, along with the possible further integration of related business processes
- a position based system of access control
- Integrated Identity Management Implementation Approach .

These supporting toolkits are aimed primarily at HR, RA, IT and Information Governance managers and staff. They are also accessible to a wider audience looking for a better understanding of how Integrated Identity Management and access to NHS CRS must be managed to minimise risk to patient privacy whilst ensuring appropriate user access.



## **2.0 Contents**

- 3.0 Introduction: Doing it once, and in the best place
- 3.1 Why do it?
- 3.2 Designing your Integrated Identity Management strategy
- 4.0 Step 1: Where are we now?
- 5.0 Step 2: Where do we want to be?
- 6.0 Step 3: How are we going to get there and what strategy are we going to adopt?
- 7.0 Tips for taking this forward



### 3.0 Introduction: Doing it once, and in the best place

This toolkit is designed to help NHS organisations move towards closer integration of the currently separate processes involved in capturing and managing staff identity, and controlling access to the NHS Care Records Service (NHS CRS).

There is a responsibility under the NHS Employment Check Standards for NHS organisations to assure themselves of the identity of all individuals providing NHS services. There is also a responsibility to prove identity beyond reasonable doubt for access to the NHS CRS. HR departments conduct checks for directly employed staff and a range of temporary or voluntary staff. Primary care support functions in PCTs conduct checks for independent contractors; and Registration Authority staff conduct checks for anyone requiring access to the NHS CRS. Clearly there is huge potential for duplication, and in most organisations this is the case.

The aim is, wherever possible, to eliminate duplication of activity in different functions, and locate information management where it can be used most effectively for purposes such as identity verification and access control.

To realise these security and efficiency gains, each NHS organisation has to commit to a strategy that will best match the use of integrated business processes and new systems to your own operational needs. There is not a 'one size fits all' solution. The strategy must take account of current systems deployment, existing procedures for identity management and access control, and the future plans for your organisation. This toolkit offers a guide to the issues you will need to address.

It is important to note that regardless of any new technical solution that may support the management of the personal identifiable data, many of the benefits can be achieved through the integration of existing paper-based processes, and therefore can be achieved now.

#### 3.1 Why do it?

##### The benefits of integrating identity management processes

###### Improved governance

Trusts involved in the early development work found that typically 20 days elapsed between an individual leaving an organisation and their access rights being revoked. Subsequently they have adopted a standard where the access rights are removed on the same day.

###### Productivity gains

Trusts participating in the development work found that integrating business processes saved £24.00 in productive time for each NHS CRS Smartcard issued.

#### 3.2 Designing your Integrated Identity Management strategy

This section takes you through the stages involved in implementing your strategy. Step 1 "*Where we are now*" and Step 2 "*Where do we want to be*" are essential before deciding which route you adopt. Step 3 sets out scenarios for the three typical organisation models.



## 4.0 Step 1: “Where we are now”

The existing deployment of systems and management of staff identity and access control varies widely across different organisations. Before going any further you should, as a board, acquire a report from the directors responsible for RA, HR and IT which provide answers to, amongst others, the following questions about identity management:

- How do we currently do identity management?
- Who is responsible for doing it?
- Does it involve single or multiple processes?
- How effectively is ESR being operated as the HR/payroll system for all staff employed by your organisation, including temporary and bank staff?
- How many NHS CRS Smartcards are in use in your organisation to access NHS CRS systems: who is using them and what has been the experience so far?
- What major deployments of NHS CRS systems are planned in the future and what is the impact on the issuance of NHS CRS Smartcards?
- What staff responses have been reported to the implementation of ESR and issuance of NHS CRS Smartcards?

The reports should also provide detail about:

- Who carries out the NHS Employment Checks and how robust the checks are in respect of employees and other staff providing NHS care on behalf of your organisation.
- How access controls are currently applied and removed, including RA responsibility for staff employed by other organisations.
- How data is collected and held on ESR and the purpose for which it is used.



## 5.0 Step 2: “Where do we want to be?”

The key strategic questions are:

- What will my organisation look like in the future? Is it the foundation trust route, is it the World Class Commissioning PCT route, or is it an autonomous provider organisation route?
- What individuals will I have identity management responsibility for?
- Which individuals will I be responsible for granting NHS CRS Smartcards to?
- Do I see my organisation providing these services?
- Do I see others providing it?
- Do I see my organisation providing it to others?

Once your organisation is clear about the answer to these questions you will be able to determine the Integrated Identity Management strategy you are going to adopt, and the process integration and technological solution required to support it.



## 6.0 Step 3: “How are we going to get there and what strategy are we going to adopt?”

There is no ‘one size fits all’ solution for any NHS organisation, however the following scenarios are offered as examples:

### **a) Integrating HR and RA processes and utilising ESR to manage access to NHS CRS applications**

This approach is likely to be the preferred option for NHS organisations where:

- the majority of staff who deliver care on its behalf are directly employed
- these organisations have a range of temporary staff (e.g. students, locums) and might conclude that they can be managed through their Integrated Identity Management approach.

With the introduction of the enhanced NHS Employment Check Standards in 2008, identity capture for new staff joining these organisations already meets RA requirements. This information will be entered in ESR. Because any changes in employment such as new starter, job change, leaver, etc are reflected immediately in ESR, this provides the most responsive and efficient method of enabling, modifying or withdrawing access to care records.

The required elements are:

- ESR is operating effectively within the organisation and is using NHS CRS Smartcards for access
- integration of RA identity capture processes with HR processes
- PBAC (Position Based Access Control) has been introduced in UIM, assigning access rights to the job that someone does
- the new UIM has been introduced to manage NHS CRS access control positions and issue NHS CRS Smartcards
- the mapping of positions in ESR to access control positions in UIM
- the implementation of the ESR Interface.

Access rights for any other staff not identified in ESR who require access to patient records can be managed through UIM alone. For these staff, it is important that systems are in place to track changes in employment status and implement those changes without delay.

### **b) Integrating HR and RA business processes or RA and other business processes, and utilising ESR to manage access for employed staff, and UIM to manage access for staff employed by others**

This approach will suit organisations who:

- provide RA services to GPs, community pharmacists and local independent healthcare providers
- have a sizeable number of directly employed staff e.g. provider organisation of community services staff.



The advantages of utilising events in ESR to manage access to NHS CRS make a compelling case for its use wherever possible. Where responsibility for managing access extends to users who are not directly employed by the organisation, the option of using UIM alone has to be added. UIM replaces the old paper-based RA procedures with electronic methods of identity capture and signature, but will not provide the automatic triggers to change in employment status supplied by ESR.

The required elements are:

- ESR is operating effectively within the organisation
- availability of UIM as part of RA services to GPs, community pharmacists and other providers
- integration of RA identity capture processes with HR processes for directly employed staff
- integration of RA processes with other business processes for the identity capture in relation to those staff not directly employed by the organisation
- implementation of PBAC (Position Based Access Control) to approve access rights.

In this scenario it is essential that measures are in place to monitor control of access rights among staff not directly employed by the organisation, and therefore not present in ESR.

### **c) Integrating RA and other business processes and utilising UIM to manage access to NHS CRS applications**

This approach will suit organisations who:

- provide RA services to GPs, community pharmacists and local independent healthcare providers
- have a small number of directly employed staff.

For staff working in non-NHS organisations contracted by trusts or PCTs, UIM becomes the only practicable method for the exercise of robust and effective control of access. The RA processes for sponsoring and approving access rights become part of the contractual arrangements with service providers. RA sponsors and agents may be located within any provider, as long as oversight of their activities is exercised by an NHS organisation.

The required elements are:

- adoption of UIM as part of RA services to GPs, community pharmacists and other providers
- implementation of PBAC (Position Based Access Control) to approve access rights within provider organisations
- effective monitoring of access control as part of service level agreements with providers.



## 7.0 Tips

**These are the critical success factors identified by the 100 trusts and PCTs who took part in the development work.**

- **Identify a 'champion'**

Someone on the Board should be nominated as Integrated Identity Management 'champion', charged with overseeing the whole project and providing high level support for the RA/HR business process integration and PBAC teams.

- **Set up HR/RA business process integration and PBAC project teams**

The relevant toolkits provide advice on the make-up and operation of these two teams. Agree the project manager and the individual project leads.

- **Communication with NHS CRS users and other stakeholders**

The context for the Integrated Identity Management project will be either a steady expansion of NHS CRS systems and increase in the numbers of staff who are able to use them, or preparation for expansion. It's important that existing and potential users are made aware of what's happening. The key message is that identity management is critical to enhance efficiency and effectiveness of access control, and that existing or future access rights for staff are not directly affected by the project.

- **Set target date for process and technical implementation**

Running concurrently, HR/RA business process integration and PBAC implementation could take up to six months to complete. Agree schedules with the two teams and set a target date when both projects will be complete, and when implementation of the Integrated Identity Management project will be signed off at board level.

Agree and set target dates for the technical implementation to include UIM and the ESR Interface recognising these are not sequential with the process integration.

- **Receive progress reports**

Receive monthly reports at board meetings through the 'champion' on progress and any obstacles or problems encountered.

- **Confirm Information Governance compliance and sign off on HR/RA business process integration and PBAC processes**

It is essential that the new or revised processes involved in HR/RA business process integration and PBAC are checked for compliance with information governance policies in your organisation. When confirmed, the Board can sign off their implementation.

- **Develop key performance indicators, these might include:**

- single identity checking of staff to satisfy both HR and RA standards
- employment checks carried out to national standards
- greater compliance with the Healthcare Commission annual health check
- electronic storage and management of employee identity data, including access rights, securely protected
- PBAC (Position Based Access Control) to grant most NHS CRS access rights for most users



- day 1 availability of NHS CRS Smartcards for new staff; same day withdrawal for leavers
- improved compliance with information governance standards.

As further supporting information is produced it will be made available on:-

**Electronic Staff Record**

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

**Registration Authority**

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

