Document filename: Registration Authorities Operational and Process Guidance			
Directorate / Programme	Access Control	**Project**	Access Control
Document Reference			
Project Manager	John Winter	**Status**	Final
Owner	Kuldeep Sohal	**Version**	V5.2
Author	Kuldeep Sohal	**Version issue date**	18/02/2016

Document Management

Revision History

Version	Date	Summary of Changes
0.1	11/11/05	Initial document created based on Setup and Operations but aligned for operational Registration Authority Team NPFIT-FNT-IMD-IME-0182.04
0.2	1/03/06	Updates to align with Registration Authorities: Governance Arrangements for NHS Organisations
0.3	23/03/06	Updates from reviewer
1.1	01/08/07	Updates to reflect changes in guidance and new functionality made available in March 2007
1.2	28/11/07	Update to 5.4 Independent Sector Healthcare Providers
2.0	29/08/08	Updates to include changes in guidance and functionality made available in June 2008
2.1	30/09/08	Addition of section 5.8 Registration of Students, update to 5.1 RA Forms (RA04 for Short-term Access Smartcard)
3.0	30/09/08	Approved version
3.1	19/08/10	Removal of paragraph in 5.6 relating to photographic documentation
3.2	28/02/13	Draft Changes ahead of new version. Removal of reproduction from NHS Employer and Calendra processes. Updates to include UIM processes and align with the Registration Authorities Operating Guidance 2013/14
4.0	07/03/13	Final version reflecting changes post 1st April 2013
4.1	17/04/13	Amendment on the RA manager appointment process following comments from RA Leads and reference to the new NHS Structures
4.2	09/08/13	Additional information on photograph requirements
4.3	04/06/13	Draft changes ahead of new Care Identity Service 2015
5.0	13/02/15	Approved version. Removal of references to previous systems; CMS, Calendra and UIM and updates include • Identification of the six CIS RA roles • RA Process guidance alignment to the HSCIC RA Policy • Addition of Care Identity Service application • Addition of Care Identity Service processes and workflows • Additional information on registering students in an educational establishment • Additional information of Independent Sector Healthcare Providers • Acceptable process on issuing and managing Temporary Access Cards

		• Predecessor positions • Case Studies on RA service models using the Care Identity Service. • CIS Forms
5.1	29/04/15	Update to the Temporary Access Card naming convention
5.2	18/02/2016	Updated to reflect non NHS organisations being on NHS England's Lead Provider Framework and commissioned to provide RA services

Reviewers

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

Reviewer name	Title / Responsibility	Date	Version

Approved by

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

Name	Signature	Title	Date	Version
Warner Baker	Warner Baker	manager, Access Control	18/02/2016	V5.2

Glossary of Terms

Term / Abbreviation	What it stands for
AT	Area Team (of NHS England)
CCG	Clinical Commissioning Group
CIS	Care Identity Service
CRS	(National) Care Records Service
CSU	Commissioning Support Unit
EPS	Electronic Prescription Service
ESR	Electronic Staff Record
HSCIC	Health and Social Care Information Centre
IAM	Identity Access Management
LSA	Local Smartcard Administrator
RBAC	National Role Based Access Control Database
ODS	Organisation Data Service
PKI	Public Key Infrastructure
PBAC	Position Based Access Control

RA	Registration Authority
SUS	Secondary user Service
UIM	User Identity Manager

Document Control:

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

Contents

Introduction

Purpose of Document

In Public Key Infrastructure (PKI) terms there is a single Registration Authority (HSCIC). All organisations that run a local Registration Authority do so on a delegated authority basis from HSCIC.

The RA within the local governance structure must ensure that all aspects of Registration Authority services and operations are performed in accordance with the HSCIC RA policy. Deviation from the requirements in the HSCIC RA Policy due to a local preference is not permitted.

The purpose of this document is to provide operational and process guidance to local Registration Authorities on meeting the minimum national requirements in the HSCIC Registration Authority Policy. http://nww.hscic.gov.uk/rasmartcards/docs/rapolicyv1sep14.pdf

As such, where the HSCIC RA Policy defines the 'What?' this document sets out the 'How?'

Accordingly, to be as simple as possible to use, this document considers each of the national RA policy requirements (HSCIC RA policy wording in italics) and then provides guidance for how each may be met.

This document reflects the processes in the Care Identity Service as of the publication date of this document.

Audience

This document is aimed at RA Managers, RA Agents, Sponsors, HR personnel, Executive Management team, Board and those individuals responsible for the Information Governance framework for the organisation.

Background

It is of paramount importance that patients are confident that their medical records are kept safe, secure and confidential in line with The Care Record Guarantee for England. To achieve this objective all healthcare professionals/worker requiring access to Spine enabled systems must be registered with a national digital identity, issued a NHS Smartcard and assigned an appropriate access control position according to their healthcare role.

What are NHS Smartcards?
NHS Smartcards are a plastic card containing an electronic chip (like a chip and PIN credit card) that is used to access Spine enabled systems. The chip stores the Unique User Identifier (UUID) within the Spine directory consisting of users digital identity information and access rights.

The user is requested to input their passcode after inserting the NHS Smartcard into a Smartcard reader which is authenticated against the Spine. After authentication, the Spine returns a list of all active access roles assigned to the user. This allows the user to access the NHS Smartcard enabled system(s) assigned to them from any location that has an active N3 connection.

The combination of the NHS Smartcard and the passcode together help protect the security and confidentiality of every patient's personal and healthcare information.

What is the Care Identity Service?
The Care Identity Service is the new Smartcard registration application available to all organisations to perform Registration Authority activities.. As an integrated application, it enables an automated 'workflow' approach that provides greater levels of governance, accountability, auditability and enables more efficient ways of working..

What is the ESR Interface to Care Identity Service?
The ESR Interface to CIS, also known as Integrated Identity Management (IIM) combines the separate processes, maintained within Registration Authority and Human Resource teams, for capturing and managing an employee's identity and access to the Spine. This allows for greater efficiency when controlling access to records on computer systems linked to the Spine.

What is the user registration process?
The user registration process operates locally and broadly consists of the following three stages:

1. A user is identified for a NHS Smartcard – this can be via
    - an individual (sponsor) explicitly requesting the individual be registered in CIS or
    - other means such as employment into a role or requirements of a job changing

The user provides appropriate identification as per NHS Employers Identity Check standards to ensure their identity is verified and recorded to e-GIF Level 3.

2. Access to the relevant Spine enabled application is permitted on assignment of an Access Control Position. The RA Manager or the Advanced RA Agent directly assigns the user to the Access Control Position or grants the assignment where the request has been approved by the Sponsor.
3. A NHS Smartcard is created that links the user to their record on the Spine and the required level of access. Access to the Spine enabled applications is then established.

What security and confidentiality measures are implemented?
All Spine enabled applications use a common security and confidentiality approach. This is based upon the healthcare professional's/worker's organisations, roles, areas of work, and activities that make up the required access and the position they have been employed to undertake.

Access Control Positions provide healthcare professionals/workers with the access to patient information required to perform their role within the organisation, satisfying both clinical and Information Governance needs.

Reference and Standard Documents
This document references job roles and activities in the National RBAC database which can be found in the following location:

http://nww.hscic.gov.uk/rasmartcards/docs

The Registration Authority will need to comply with the following:

- Registration Authorities: Governance Arrangements for NHS Organisations
- The Care Record Guarantee
- NHS Confidentiality Code of Practice
- HSCIC Registration Authority Policy
- NHS Offshore Policy that requires all storage of person identifiable data associated with the operation of HSCIC systems to be within the borders of England.

The HSCIC RA Policy

Section 1.2 of the HSCIC RA Policy outlines the following 5 aspects:

1.1.1 The RA Hierarchy and the principle of delegated authority to local organisations to run their RA.

1.1.2 The requirements for creating a nationally verified digital identity.

1.1.3 The roles and responsibilities within organisations that run their own Registration Authority activity

1.1.4 Requirements in relation to Smartcards

1.1.5 The requirement to develop and implement a local RA Policy.

The document considers each of these aspects in turn and provides guidance for each.

Registration Authority Hierarchy

1.2 What is the Registration Authority?

In Public Key Infrastructure (PKI) terms there is a single Registration Authority (HSCIC). All organisations that run a local Registration Authority do so on a delegated authority basis from HSCIC.

The Registration Authority consists of the Board/EMT level individual accountable for RA activity, RA Manager, RA Agents and Sponsors who have a responsibility to individuals providing healthcare services to the NHS directly or indirectly, to ensure timely access to the Spine enabled applications in accordance with their healthcare role.

1.2.1 Assignment of RA Managers and Sponsors

RA Managers & Sponsors are appointed by the Board/EMT and this appointment is confirmed in a letter of appointment which must be held by each individual appointed to these positions. Copies of these letters should also be held by the RA Manager so they are able to provide the necessary evidence to meet IG Toolkit requirements.

The local Executive Management Team should ensure that there should be a minimum of two individuals assigned the RA Manager role for business continuity reasons. RA Managers are responsible for the governance of RA within their organisation therefore assignment of RA Managers must not be titular. However, there should not be a large number of staff assigned the RA Manager role and the number of RA Managers should explicitly be agreed by the governance structures within the organisation.

Below is an example assignment letter to assign an individual to the RA Manager and Sponsor roles or assignment may be captured in the minutes of a meeting. Similarly, the local Executive Management Team must be made aware in writing where RA managers and Sponsors are no longer in these roles. All assignment letters must be stored in a secure environment in the local organisation.

1.2.2 Example Letter from local EMT to appoint RA manager and Sponsors

From (Name) Executive Management Team organisation name

Please be advised that we assign R5080/B1300 and entrust the responsibility to create and maintain the RA manager/Sponsor role to (Individuals Name). I charge (Individuals Name) with the responsibility of ensuring that the National and organisations' RA Policy and RA Procedures are adhered to in full.

Creation of a national digital identity

2.1 I.D. Management guidelines

Identity assurance is increasingly important for the NHS, both for recruitment and for access to the Spine.

Identity must be verified in a face to face meeting. It must be done by examining original documents and seeing that identity relates to the individual who presents themselves at the meeting.

The documents that can be used to verify an identity have been jointly determined by HSCIC and NHS Employers and the list is contained in the NHS Employers 'Verification of Identity Checks' standard which can currently be found at http://www.nhsemployers.org/case-studies-and-resources/2009/01/verification-of-identity-checks.NO other documents are approved for verification of identity, including those contained within other NHS Employers standards.

The NHS Employment Check Standards apply to all applicants for NHS positions (prospective employees) and staff in ongoing NHS employment. This includes permanent staff, staff on fixed-term contracts, temporary staff, volunteers, students, trainees, contractors and highly mobile staff supplied by an agency. Trusts appointing locums and agency staff will need to ensure that their providers comply with these standards.

Note*:* The only exception to the Identity checks document is that the RA does not keep photocopies of the applicant's identification documents.

Identity is required to be verified to the previous inter-governmental standard known as e-GIF Level 3. This provides assurance that the identity is valid across any organisation an individual works within.

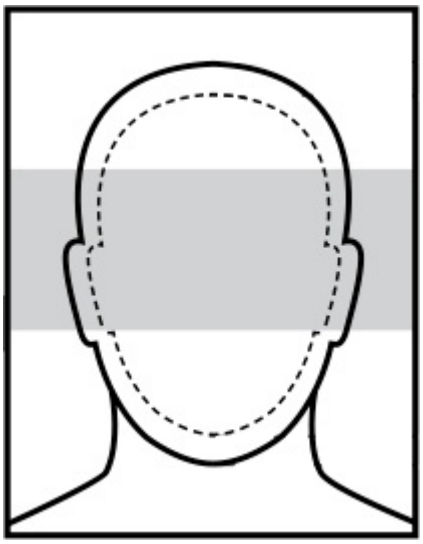
The new Care Identity Service application enforces a new user's identification to be verified to e-GIF Level 3 before a NHS Smartcard can be issued to that user. Failure to comply with the NHS Employment Check standards could potentially put the safety, and even the lives, of patients, staff and the public at risk.

RA should verify that the applicant's current UK Driving Licence photo card at the face to face meeting is a true likeness of the applicant.

2.2 Photograph

The photograph assigned to the user's profile which is printed on the Smartcard must adhere to the following standards:

- Photograph must be as per the below diagram
- Photograph must meet passport standards and be taken against a plain background with adequate lighting and be cropped to match the diagram below.
- For further information please see the Home Office Passport Photo Requirements https://www.gov.uk/photos-for-passports



The technical guidance for photographs that are captured by or imported to CIS must meet the following specification:

1. Size matches or exceeds the minimum size (420 x 525 pixels)
2. Should the captured size exceed the maximum size then the captured image should be re-sized to the maximum (i.e. 630 x 788 pixels)

On completion of the registration process of the user, the photograph of the user should be destroyed by RA staff or Sponsors. There is no requirement for RA staff or Sponsors to retain copies of the photograph once imported into Care Identity Service.

2.3 HR and RA Processes

Many organisations have integrated RA with HR as part of their approach to Integrated Identity Management to remove duplication of identification checks and achieve associated efficiency gains. Section 11: Integrated Identity Management of this document provides further details.

The table below illustrates both HR and RA responsibilities in an organisation depending on whether the HR and RA processes are aligned:

HR and RA Processes	HR staff	Photo	RA staff
Integrated as part of the recruitment/employment check/application process using the ESR Interface	HR assistant is also the RA Agent complete the identity verification process in the ESR Interface	Photo taken at the time of the identity process and saved in a secure shared folder that RA staff can access	1. Photo evidence used in the identity process reviewed by RA 2. RA upload user's photo in CIS
Integrated as part of the recruitment/employment check/application process using the ESR Interface	HR assistant is also the RA Agent complete the identity verification process in the ESR Interface	Photo not taken at the time of the identity process	RA capture and upload user's photo in CIS.
HR and RA Processes not integrated	HR assistant is not a RA Agent	RA staff capture photo in the identity process	RA staff undertake the identity process

2.4 Changes to Core identity attributes

Any changes to a person's core identity attributes (Name, Date of Birth or National Insurance Number) need to go through the same face to face check with a person holding an RA role and provide appropriate documentary evidence.

A user's Core Identity is First Name, Middle Name and Family Name, Date of Birth and National Insurance Number.

An update to a user's Core Identity using the Modify user Workflow in the Care Identity Service application can only be done after the RA has verified the user's identification according to the Identity Check Standards on NHS Employers.

The following are examples of circumstances where an update to a user's core identity will need to be made in CIS:

- Marriage
- Change of Name by deed poll
- Users name incorrect in CIS

Roles and Responsibilities

The local Registration Authority ensures that individuals providing healthcare services to the NHS directly, or indirectly, have access to the Spine enabled applications and information in accordance with their role.

A local Registration Authority consists of Board/EMT person accountable for RA activity, RA Managers, RA Agents, and Sponsors within the local Information Governance structure.

2.5 RA Manager

The following section highlights the RA Manager's responsibilities that cannot be delegated as described in the HSCIC RA Policy.

2.5.1 Responsible for running RA Governance in their organisation – cannot delegate this

For RA Managers to fulfil their governance responsibility Registration Authorities must retain RA records and implement periodical audit activities.

Should the need arise, by retaining sufficient records of RA activity enables the RA manager to be able to determine, at a later date, the supporting evidence and methods used to verify and validate identity.

This may be useful to determine for example, the Sponsor or the RA Agent that had approved or granted the user's identity using the paper forms. Additional examples include checking when a user had originally signed the Terms and Conditions of Smartcard use using the RA01 form.

The NHS England Corporate Records Retention – Disposable Schedule and Retention http://www.england.nhs.uk/wp-content/uploads/2014/02/rec-ret-disp-sch-guid.pdf provides information on retaining RA records to organisations that operate a Registration Authority.

The above document states that the following RA records need to be retained by the local organisation for a period of either 6 years after subject of file leaves service or until subject's 79th birthday whichever is the later:

- Previous Calendra forms (RA01, RA02, RA03 forms etc.)
- Assignment Letters
- Inter-organisational agreements

CIS Audit Alerts
In the Care Identity Service application, an audit alert is raised on the system during the following workflows:

- Registering a user with an out of date identity document
- Directly assigning a user to a position

Reports on the audit alerts are in development which will then need to be reviewed by the organisations RA Manager to ensure that RA staff have valid reasons to raise the alert and the workflows are aligned to the local organisations processes.

RA audit policy

As part of the RA Manager responsibility of running RA Governance, RA Managers should develop the organisation's RA audit policy and conduct annual audits on NHS Smartcard usage.

RA Managers must implement a process to run the RA reports available in CIS on a regular basis. Further information on Reporting is in section 5.19.

2.5.2 Responsible for the development of local processes that meet policy and guidance for the creation of digital identities, production of smartcards, assignment of access rights, modifications to access and people and certificate renewal and card unlocking

As part of the process to develop local RA procedures to manage RA activity, RA Managers should identify areas where the organisations business processes need integrating to minimise risk and duplication of effort. For example, HR processes for starters, leavers, suspensions, terminations, and approved leave.

Once implemented, RA Managers should ensure there are sufficient resources to operate the registration processes in a timely and efficient manner and a sufficient supply of NHS Smartcards and RA hardware.

For further information on RA Hardware orders refer to RA Hardware Ordering and Returns Process.

2.5.3 Implements RA Policy and RA Processes locally adhering to national guidance's

The local RA Policy and local RA processes should be implemented by the RA Manager and all RA staff in the organisation and child organisations should be both made aware of them and have access to them.

The organisations RA processes should reference CIS forms or Temporary Access Cards if used by the organisation or child organisations, as well as the approve and grant process and the direct assignment of positions to a user's access profile.

2.5.4 Assign, sponsor and register RA Agents and Sponsors

New roles have been created in the new Registration Authority software, Care Identity Service, which is due to replace current software in the autumn of 2014, to allow the RA Manager to delegate certain aspects of RA activity. These include Advanced RA Agents, RA Agents (ID checking only) and Local Smartcard Administrators.

RA Managers are responsible for registering users who have been identified for an RA role; RA Advanced Agent, RA Agent, RA Agent ID Checker, Sponsor and Local Smartcard Administrator in CIS. The RA Manager must ensure users assigned to RA roles are aware of their responsibilities.

2.5.5 Train RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process – If an RA Hosting organisation with a child hosting organisation – need to train RA Manager at next level down

The training of RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process. A RA Hosting organisation parenting another RA Hosting organisation is responsible in providing training to the RA Manager in the next level down

To support the RA Managers responsibility to deliver training on Care Identity Service to staff involved in carrying out Registration Authority activities, the HSCIC has developed an interactive e-learning package. The e-learning focuses on the application of national RA policy, governance and includes training modules on the use of the new Care Identity Service (CIS) application.

An e-learning account can be activated by accessing the e-learning home page: https://hscic.premierittask.com

The HSCIC RA Policy also states that: *The person verifying the identity must be trained to do so. In Registration Authority terms this means that individuals holding the roles of RA Managers and RA Agents must perform these checks at face to face meetings since part of their responsibilities and requirements are that they are trained to carry out this activity. The RA Manager is responsible for training all other RA staff who will conduct ID checking to ensure that appropriate standards exist and they can evidence good ID checking as part of the IG Toolkit requirements.*

Only the following CIS RA Roles have a responsibility to verify a user's identification as part of the registration process

- RA Manager
- Advanced RA Agent
- RA Agent
- RA Agent ID Checker

All personal data processed by the RA relating to the registration process must be processed in accordance with the Data Protection Act 1998. RA Staff should maintain the confidentiality of personal information provided to them as part of the authentication process.

RA Managers should also ensure all RA roles are aware of the CIS workflows available to them and users are aware of the self-service functionality available to them, including how to reset Passcodes and renew Smartcard certificates – this should include any localised requirements.

RA Managers should assist Sponsors in understanding the Role Based Access Control (RBAC) model and Position Based Access Control (PBAC) in finding information about applications they sponsor users for.

2.5.6 Facilitate the process for agreeing the organisations access control positions

Once the organisations Access Control Positions have been agreed by the organisations key stakeholders, RA Managers must ensure that the organisation formally approves the positions in writing before creating the positions in Care Identity Service.

RA Managers must identify in the organisations local processes the process for the Executive Management Team to approve new and modifications to existing positions in the organisations.

Further information on the organisation approval is in section 5.2.7 of this document.

On approval by the organisation's Executive Management Team, the RA Manager has the required agreement to create and modify Access Control Positions in CIS.

2.5.7 Responsible for ensuring users are compliant with the terms and conditions of Smartcard usage

Ensuring users accept terms & conditions of Smartcard use when registering them

Following the creation of a user's digital identity on the CIS application and/or assignment to a position in the organisation by the local RA, the organisations local processes should reference that the user access the CIS application to electronically accept the Terms and Conditions of Smartcard use when they first log in with their Smartcard.

It is mandatory that users sign the Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.

However, organisations must ensure that all RA01 forms are retained in a secure location as per NHS England's guidelines. http://www.england.nhs.uk/wp-content/uploads/2014/02/rec-ret-disp-sch-guid.pdf

This will ensure that there is an accurate record of when the user accepted the Terms and Conditions of Smartcard use.

2.5.8 Verifies user's ID to e-GIF level 3 when they register users

The RA Manager must ensure that all RA roles responsible in the creation of a digital identity are effectively trained to do so and adhere to the identification documentation guidelines at NHS Employers:
http://www.nhsemployers.org/Aboutus/Publications/Documents/Verification%20of%20identity%20checks.pdf

2.5.9 Ensuring leavers from an organisation have their access rights removed in a timely way

When Smartcard users leave an organisation they should have their access assignment end dated in that organisation. However unless it can be reasonably foreseen that they will not require access in another organisation in the future, leavers should retain their Smartcard.

In organisations where HR duties are separated from RA, then the local organisations RA processes must reference the local joiners and leavers policy. HR should advise the local RA in a timely way in the event a user leaves or will not work for the organisation so that RA can revoke access accordingly by setting an end date to the position assignment.

Where HR and RA processes are integrated, it is expected that HR will be setting an end date to the position assignment.

The Smartcard should be retained by the user at all times except in the event when the user will work in the NHS or Healthcare sector in the future.

2.5.10 Responsible for the security of (old) paper based RA records

RA records need to held in a secure location and be retained in accordance with NHS England Corporate Records Retention – Disposable Schedule and Retention http://www.england.nhs.uk/wp-content/uploads/2014/02/rec-ret-disp-sch-guid.pdf. RA documentation must be retained 6 years after subject of file leaves service or until subject's 79th birthday whichever is the later.

Furthermore, as per the above document, any CIS forms used for data input in the Care Identity Service application need to be retained for a period of 2 years.

RA Managers should identify a secure locked area for the storage of all previous paper based registration documentation, CIS forms and associated information in accordance with the Data Protection Act 1998. This includes RA Manager and Sponsor assignment documents, RA forms, RA reports and inter-organisational agreements. All RA forms must be clearly marked with the user's UUID number and filed in a designated area that the RA have access to typically in HR/Personnel.

When an organisation is merging or closing, RA Manager must identify where the RA records and RA hardware will reside and gain approval from those individuals responsible for Information Governance.

Successor organisations have the responsibility to safely manage RA documentation.

- If an organisation is being merged into a new organisation, RA documentation should be transferred to the new organisation.
- If an entire organisation is being closed, RA documentation should be transferred to a senior RA organisation.
- If an organisation is being merged into a new organisation, the records and hardware should be transferred and retained by the new organisation.
- If an organisation is being merged with more than one organisation, the records and hardware should be distributed and retained between the organisations.
- If an entire organisation is being closed, the records and hardware should be transferred and retained by a senior RA organisation.

Furthermore, the NHS Offshore Policy requires all storage of person identifiable data associated with the operation of HSCIC systems to be within the borders of England. http://systems.hscic.gov.uk/infogov/igsoc/links/offshoring.pdf

2.5.11 Ensure all service issues are raised appropriately locally and nationally

The RA Manager should report all RA related security incidents and breaches to the organisation's Risk Management Team, Caldicott Guardian, and Executive Management Team or as indicated by the local Information Governance policy.

In addition, the RA Manager should advise RA staff to ensure service issues are presented through normal service, supplier or programme channels before escalating to the next level in the RA cascade.

2.6 The functions of the RA Roles in the Care Identity Service

New roles have been created in the new Registration Authority software, Care Identity Service, which is due to replace current software in the autumn of 2014, to allow the RA Manager to delegate certain aspects of RA activity. These include Advanced RA Agents, RA Agents (ID checking only) and Local Smartcard Administrators

Depending on the RA role, the RA role will be limited to request, approve or grant a request or perform a different RA function.

Separation of RA staff roles and Sponsor's responsibility must be adhered to in Care Identity Service to allow for the governance of approve and grant processes. Therefore, RA roles that have the ability to grant requests in CIS must not in addition be assigned the Sponsor business function B1300 – to approve activity.

The CIS application supports:

- Requests to be approved and granted by separate individuals or,
- As a single step process if the approval has been provided as employment into a role or requested by email or on completion of a CIS form,
- RA staff in ensuring access is assigned and revoked by the appropriate CIS role

Further information on the activities included in the baseline of the RBAC role and activity for each of the CIS RA roles is shown from sections 2.6.1 to 2.6.6.

The table provides an overview below of the Care Identity Service RA roles and business functions:

CIS RA Role Name	Job Role / Activity Code	Description
RA Manager	R5080	Overall responsibility for local RA processes and governance
Advanced RA Agent	R5090 + B0274	Has the ability to action nearly all of the RA processes available to the RA Manager except assign register users to the RA roles in their own organisation and assign RA Managers in child organisations that are RA hosting
RA Agent	R5090	Main function is to grant requests
RA Agent ID Checker	B0267	Only has the ability to perform the identity checks to register users in CIS
Sponsor	B1300	Main function is to approve requests
Local Smartcard Administrator	B0263	Only has the ability to unlock Smartcards and assist in the renewal of certificates

Further information on the operations available to the CIS RA roles is outlined sections 2.6.1 to 2.6.6.

2.6.1 RA Manager Functions in CIS

The following functions are available to the RA Manager in the CIS application:

- Register RA Manager in child hosting organisation
- Register Advanced RA Agent, RA Agent, RA Agent ID Checker, Sponsors and Local Smartcard Administrators in own organisation and child organisations
- Register Smartcard users
- Search and view closed users
- Reopen closed users
- Create positions and workgroups
- Modify positions
- Assign individuals to positions
- Review positions definitions including assigned users
- Assign individuals to workgroups
- Manage request lists
- Access reporting and run reports
- Assign users to positions
- Use batch functionality
- Create Temporary Access Cards
- Cancel Smartcards
- Close user
- Unlock Smartcards & renew certificates
- View all requests

2.6.2 Advanced RA Agent Functions in CIS

The following operations are available to users assigned to the Advanced RA Agent role in CIS:

- Register Smartcard users
- Search and view closed users
- Reopen closed users
- Create positions and workgroups
- Modify positions
- Assign individuals to positions
- Review positions definitions including assigned users
- Assign individuals to workgroups
- Manage request lists
- Access reporting and run reports
- Assign users to positions
- Use batch functionality
- Create Temporary Access Cards
- Cancel Smartcards
- Close user
- Unlock Smartcards & renew certificates
- View all requests

2.6.3 RA Agent Functions in CIS

The following operations are available to RA Agents in CIS:

1. Register Smartcard users

2. Search and view closed users
3. Reopen closed users
4. Assign individuals to positions (only grant the assignment)
5. Review positions definitions including assigned users
6. Assign individuals to workgroups
7. Access reporting and run reports
8. Create Temporary Access Cards
9. Cancel Smartcard
10. Close user
11. Unlock Smartcards & renew certificates
12. View all requests

2.6.4 RA Agent ID Checker

Users assigned to the RA Agent ID Checker role in CIS only have the ability to check user's identification and grant the digital identity. RA Agent ID Checkers do not have the ability to print Smartcards and grant access assignment requests in CIS.

2.6.5 Sponsor Functions in CIS

The following operations are available to Sponsors in CIS:

- Raise and approve request to assign a user to a position
- Directly assign user to any assignable position
- Raise request to register a new user (completed by RA)
- Review positions definitions including assigned users
- View my requests and requests pending approval
- Unlock Smartcards & Renew Certificates
- Can assign users to Workgroups

2.6.6 Local Smartcard Administrator Functions in CIS

Users assigned to the Local Smartcard Administrator role in CIS only have the ability to renew certificates and unlock Smartcards for users that have not been assigned to a CIS RA Role.

2.7 Registration of Healthcare Professionals/Workers

The Registration Authority should use the following to determine their responsibilities for registering and managing the access of healthcare professionals/workers.

- **Healthcare professionals/workers in an NHS organisation** will normally be registered and granted access to the organisation's Spine compliant applications by the organisations own RA. In some cases the NHS organisation may agree to have their RA services provided by a Shared Service. Generally these individuals will only have an access profile for the organisation they work for.
- **Healthcare professionals/workers in GP practices** will normally be registered and granted access by the RA Service Provider that is commissioned to provide the RA service by the Area Team. Generally, GP's and practice staff will only have an access profile for the practices they work in.
- **Healthcare professionals/workers in the Independent Sector** will have their RA service provided by a NHS organisation. This is usually one for whom they provide clinical services for or by a RA Service Provider commissioned by the Area Team. In the RA hierarchy, the Independent Sector organisation will be RA parented to their RA Hosting organisation on the Spine. The Independent Sector Healthcare

professionals/workers will normally only have access profiles for their Independent Sector Healthcare provider units' organisation.

- **Local Authority and Social Services' workers** are generally registered and granted access by the RA Service Provider commissioned by the Area Team. In the RA hierarchy, the Independent Sector organisation will be RA parented to their RA Hosting organisation on the Spine. These individuals will only have access to their Local Authority organisation.
- **A Shared Service organisation** that supports multiple organisations will have RA staff including RA Managers in each NHS organisation that it provides a RA service to. RA Managers from the Shared Service organisation will be identified by the Executive Management team in the individual organisation for which the Shared Service organisation is providing the RA service. The Shared Service organisation is not the RA parent in the RA hierarchy to the organisations that it supports.
- **Prison workers** are generally registered and granted access by the RA Service Provider commissioned by the Area Team. In the RA hierarchy, Prisons will be RA parented to their RA Hosting organisation on the Spine. Prison workers will only have access to the prisons they work for.

Healthcare professionals/workers or Local Authority and Social Services' workers who work in more than one care setting may have their RA services provided via more than one of the above categories. For example, a GP who performs some sessions in an Acute Trust will generally be registered by the RA in the CSU but have their Acute access profile managed by the Acute Trust's RA.

Further information on the RA Hierarchy on the Spine is in section 6.2 of this document.

2.8 Inter-Organisational Agreement

Where an organisation needs to perform registration activities on behalf of another organisation, it is the responsibility of the RA Hosting organisation to ensure a contractual arrangement or inter-organisational agreement exists between all parties and that appropriate positions have been granted. This should detail what each party does, and explicitly state the liability of each for their actions or omissions, the disciplinary process, and audit arrangements. The inter-organisational agreement identifies which organisation's RA Manager will register the RA agents and the groups of healthcare professionals/workers needing access to the Spine enabled applications.

Requirements in relation to Smartcards

3.1 NHS Smartcards

All users including RA staff must have only one NHS Smartcard issued to them showing their UUID and photograph.

The primary purpose of NHS Smartcards is to provide identification and system authentication to Spine enabled applications. Some organisations have extended use of NHS Smartcards for a range of innovative uses including single sign-on to access non spine applications and door access.

However any use should be in line with the organisations security policy and there should be no permanent changes to the NHS Smartcard; and therefore organisation names should not be printed on the NHS Smartcard. For further information on the extended use of NHS Smartcards refer to http://systems.hscic.gov.uk/rasmartcards/strategy/extended.

NHS Smartcards must be kept at all times with the user. Under no circumstances can NHS Smartcards be:

1. Issued with the organisation name
2. Issued without the user's UUID and a true likeness of the user's photograph displayed
3. Shared including the passcode
4. Shared by any other user other than the user on the Smartcard
5. Remain in the Smartcard reader when the workstation is unattended by the user
6. Removed from the user when they leave an NHS organisation if they intend or there is a possibility that they will work for organisations that use Smartcard enabled systems at some point in the future

This document only endorses the use of NHS Smartcards and Temporary Access Cards.

3.2 NHS Terms and Conditions

It is mandatory that users sign the Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.

In the CIS application, users need to be assigned to an organisation code and position to enable them to log in with their NHS Smartcard. Once a user has been assigned a position, the RA should ensure that the user accesses the CIS application to electronically accept the Terms and Conditions of Smartcard use if they have not already done so.

RA Service Providers must ensure that NHS Smartcard users comply with the terms and conditions of Smartcard use. Breach of the terms and conditions and/or organisational procedures relating to NHS Smartcard usage should be linked to the organisations disciplinary measures.

3.3 NHS Smartcard Passcode

Only the end user for whom the Smartcard is intended should know their passcode for their Smartcard, no-one else should, including RA staff. If anyone else knows the end users passcode it breaches the Smartcard terms and conditions of use and the Computer Misuse Act 1990.

The Terms and Conditions of Smartcard use *reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.*

Passcodes are automatically checked every time a NHS Smartcard user authenticates to the Spine to prevent unauthorised access.

The NHS Smartcard Passcode is

- Set only by the user during the registration meeting.
- Entered by the user in conjunction with their NHS Smartcard to log on to the Spine.

Only the user must set and know their NHS Smartcard Passcode. The Passcode cannot be shared or disclosed to anyone else and must be a strong passcode consisting of between four to eight alpha, numeric and/or special characters.

3.3.1 Can a user be assigned a Temporary Passcode?

No. As part of the Public Key Infrastructure process, the user to whom the NHS Smartcard is issued must be the individual that uses the NHS Smartcard for the first time to authenticate to the Spine when they login and enter their Passcode. Therefore, RA Staff, Sponsors and LSAs are not permitted to assign a new user a temporary Passcode and/or login with the user's NHS Smartcard for any reason, including checking the viability of the NHS Smartcard.

Where it is not possible for the user to set their Smartcard Passcode at the registration meeting, RA staff must ensure that the NHS Smartcard is issued in a locked format. Users can then set a Passcode during the face to face meeting with the RA Staff, Sponsor or the LSA using the Assisted Unlock Smartcard Process workflow in CIS.

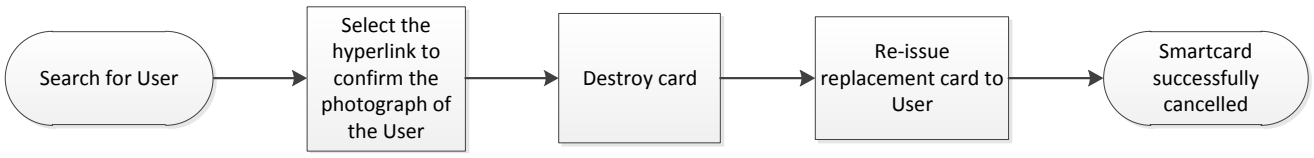
If the user suspects their Passcode has been compromised, the user should seek assistance from RA Staff, Sponsor or LSA to reset their Passcode as soon as possible

Note: Currently in CIS to reset a user's Passcode, the NHS Smartcard must be locked in advance.

3.4 Lost, Stolen and Damaged Smartcards

In the event a user has lost, stolen or damaged their NHS Smartcard, the user should report this immediately to the organisations Registration Authority.

Lost / Stolen / Damaged Process



The RA should implement the following process once the user has reported that they have lost, stolen or damaged their Smartcard:

1. Meet the user face-to-face and confirms their identity by the user's photograph in CIS. If the identity cannot be verified the user will be required to produce documentary evidence of their identity, refer to section 2.1: I.D. Management Guidelines of this document.
2. Cancel the lost, stolen or damaged NHS Smartcard using the Destroy Card workflow in CIS.
3. Issue a replacement NHS Smartcard.

Note: Under NO circumstances should organisations abuse the process for handling lost and returned NHS Smartcards by sending NHS Smartcards that are no longer required to the postcode on the back of the card for cancelling and disposal. The RA within the organisation must cancel the NHS Smartcard and follow the recommended process for disposing NHS Smartcards that are no longer required.

3.5 Temporary Access Cards

Smartcards can only be issued to individuals who have a national verified digital identity. This is also the case for processes that are used to issue temporary access to an individual – they need to have a verified identity first.

Temporary access cards (TAC) mitigate the risk of Smartcard users not being able to access clinical systems in particular circumstances. National RA policy makes clear that if a user already has a verified national digital identity it is allowable to issue them a Temporary Access Card, a card with pre-assigned access issued for a set short period, in particular circumstances (these cards have been known as short term access cards in the past). These circumstances include:

- The individual has forgotten their Smartcard passcode and a CIS role is not available to unlock the individual's Smartcard
- The individual has locked their Smartcard and a CIS role is not available to unlock the individual's Smartcard
- The individual has forgotten their Smartcard
- The individual is required to use different access to what they normally use and RA is not available to assign this
- The individual needs different or continued access and RA functionality is not available to do this (e.g. at go live date, an absence or RA etc.)

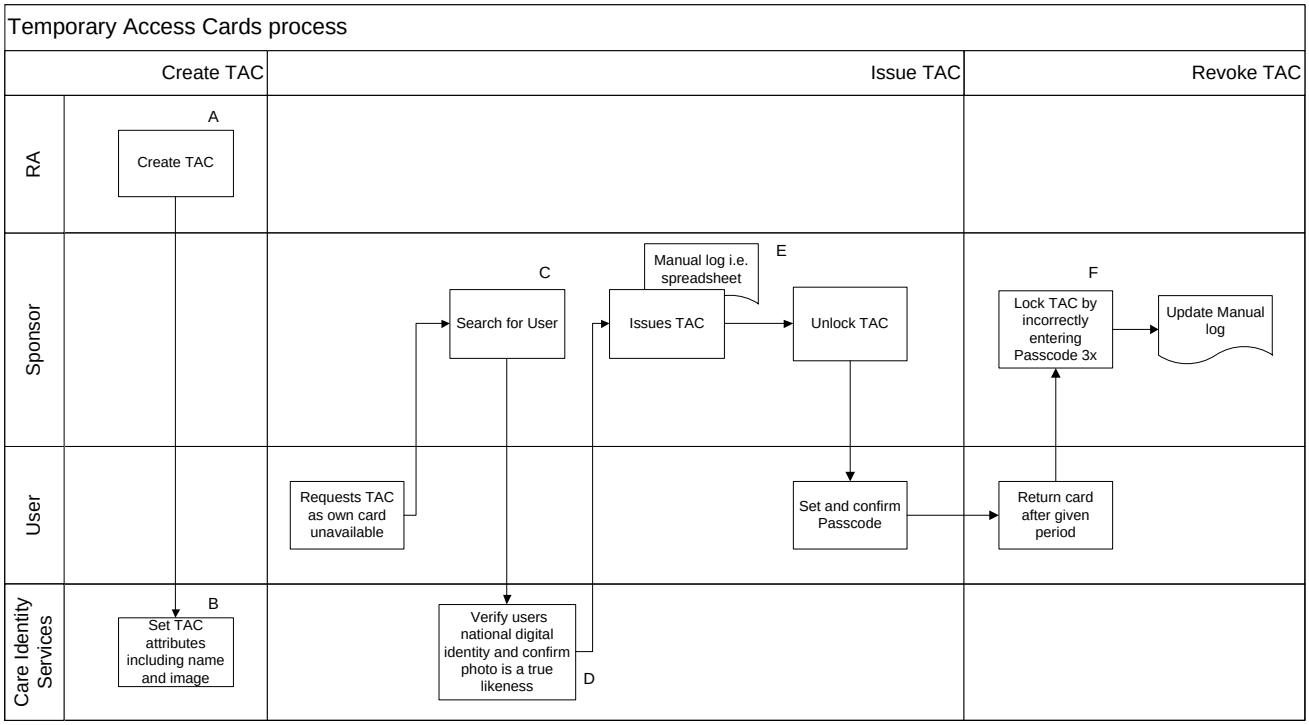
Please note that if a user does not have a verified national digital identity it is not permissible to use a Temporary Access Card to give them access to Spine systems – this breaches National RA Policy which can be found at http://nww.hscic.gov.uk/rasmartcards/docs.

RA must only use the following image to issue Temporary Access Cards:

Some cards for temporary access, known as Short Term Access Smartcards will have been created prior to the implementation of Care Identity Service. These will continue to be valid to use in CIS.

3.5.1 Temporary Access Cards Process

Temporary Access Card process



Notes	Description
A	Temporary Access Cards can only be created by RA staff (with R5080 or R5090 in their access control position).
B	The naming convention for the card is **'TAC [reference to the organisation i.e. organisation code] [position name]'** Given Name: **Temporary Access** Surname: **Card** Preferred Name: **TAC [organisation code] [position name]**
	TAC Image is in the following location: http://nww.hscic.gov.uk/rasmartcards/cis/training/tac.jpg

	When created the following information will need to entered into the Care Identity Service application, it will use a combination of 1 photo, and 2 non-photo ID documents: ○ NI number to be entered is **AB123456C** ○ The photo evidence to be entered is **ABW Aruba Passport**, number '**TAC**' ○ The non-photo ID to be entered is '**TAC1**' and '**TAC2**' from the document drop down list, document issuer 'TAC' date of issue as today's date
	Notes field in CIS to be completed to indicate it is a temporary access card
	Cards should be created 'locked' and the user liaises with RA or Sponsor will unlock the Smartcard using the Assisted Unlock Workflow in CIS.
C	Temporary Access Cards can only be issued by a Sponsor assigned the business function B1300 or RA staff assigned R5080 or R5090 within their access control position.
	When a user presents for a TAC the sponsor must log in Care Identity Service and search for the user.
D	Sponsor verifies they have a national digital identity, to capture their UUID and that the photograph on their record is a true likeness.
E	A manual log needs to be maintained for each TAC – it must be completed with a minimum of: • Smartcard user UUID • Smartcard user Name • Reason for issue • Log out time and date • RA/Sponsor name and UUID issuing TAC • Log back in time and date
	Sponsors should review these logs daily and take action if cards are not returned within a reasonable time period (72 hours normally) to return them or contact their RA to cancel the card if it is not returned.
	RAs should monitor the use and record keeping for these cards on a regular basis.
F	Cards returned should be 'locked' via entering an incorrect passcode 3 times.

Note: A future Care Identity Service enhancement will require an electronic log to be completed and cards will be de-activated after 72 hours from the time and date it is electronically 'signed out' to a user.

Local RA Policy

4.1 Local RA Policy

It is a mandatory requirement that organisations that run local RA activity have a local policy outlining their approach. The following are mandatory requirements within the local organisation's policy.

1. *The name of the Board/EMT accountable person and the RA Manager within the organisation must be named within the policy. The policy needs to outline the governance requirements placed upon these individuals. The local organisation's policy must be updated to reflect any changes to the named individuals.*

2. *The policy must describe how access rights will be granted and revoked in a timely way, ensuring that requirements for staff to be able to access electronic records in a timely way can be met and that individuals do not retain access within an organisation once they have left that organisation.*

3. *The policy must not contradict the mandatory requirements contained within this national RA policy document. At a minimum the policy must cover:*

    i. *Governance arrangements*
    ii. *A demonstration of the adherence to this policy document requirements in relation to the verification of identity*
    iii. *Roles & responsibilities*
    iv. *Smartcard Use*

4. *The policy must be formally signed off by the organisation at an appropriately senior level, e.g. the EMT, the IG Committee on a delegated authority basis, etc.*

5 Care Identity Service

Care Identity Service (CIS) is the electronic registration application that is available to all organisations to perform Registration Authority activities. This system improves automation, supporting an enhanced registration process.

This section sets out each of the key CIS workflows and provides business process guidance for them.

5.1 Position Based Access Control

5.1.1 What is Position Based Access Control?

Position Based Access Control (PBAC) is a key pre-requisite to implementing the Care Identity Service. PBAC builds on the existing Role Based Access Control (RBAC) security model, which provides access to the Spine systems appropriate to the job that the staff have been employed to do.

5.1.2 Why positions are used in CIS?

PBAC links the job to the access rights it requires, thereby reducing the need for access rights to be assessed on an individual basis. PBAC provides a simple and effective mechanism for providing users with 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.

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.

PBAC ensures greater consistency within NHS organisations about how access to care records is controlled and managed. PBAC also facilitates the management of access via the ESR interface to CIS. Please refer to section 6: Integrated Identity Management for further details.

5.1.3 Who needs to be involved?

In addition to the organisations Registration Authority, the Information Governance Manager and/or Information Technology Manager may need to be involved in setting up PBAC within the organisation.

5.1.4 How to design PBAC within your organisation

To set up Position Based Access Control within an organisation, an analysis of the organisation is undertaken of posts within an organisation requiring access, establishing the access profiles and Workgroup requirements of each post in the organisation that access the Spine applications.

Organisations should identify access requirements to a system and group them into Access Control Positions based on the job that users are assigned to. This is likely to be particularly important when deploying a new system, such as SystmOne, Lorenzo or Rio; to review who needs access to that system, and for what purpose.

5.1.5 Approach

There are a number of methods an organisation can adopt using this approach:

- Discuss with clinical staff and managers to verify and agree access requirements.
- Review the 23 rationalised job roles contained in the National RBAC Database. These roles have been widely consulted upon and represent a set of baseline access rights appropriate to the jobs people do.
- Map the patient journey through episodes of care, and establish any additional access rights that staff may require through this process. Mapping sessions assist in process improvement and service redesign work.

Once the access has been identified, then the organisation will need to define a position name and optionally a description to inform RA staff and Sponsors on the use of the position.

5.1.6 Set up PBAC

As a minimum an Access Control Position in CIS must consist of the following:

- Position name
- Job Role Code
- Organisation approval

Additional information may be added to the position in CIS including position description, business activity codes, workgroups and setup as an assignable position.

In the Care Identity Service, an image of a red flag is denoted with an Access Control Position when any of the following are included in the position:

- Sensitive business functions assigned to the Access Control Position
- Predecessor position link added to the Access Control Position
- RA job roles or RA activity codes

5.1.7 Organisation Approval

Organisations must undertake local approval of the Access Control Positions to strengthen the governance and organisational ownership which is then registered in CIS. Once the Access Control Positions have been defined, they will need to be clearly documented and approved in writing 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.

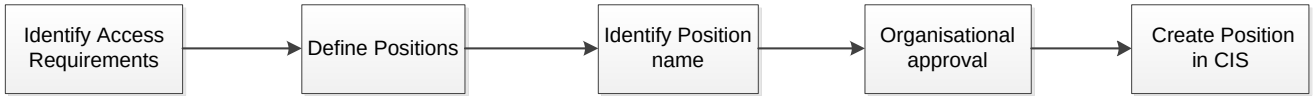
The approved Access Control Positions will form the basis for inputting positions into the Care Identity Service. Information on the organisations approval; how and when the organisation has ‘signed off’ their positions in CIS must be included in the **Notes** field for audit purposes.

The written approval enables the Registration Authority to create Access Control Positions as a single person without any additional sponsorship approvals.

In CIS, the following information must be entered as a minimum:

1. Name of the approval authority
2. Date of the approval authority
3. Purpose of the Access Control Position including why it has been created.

PBAC process



5.2 Registration Process

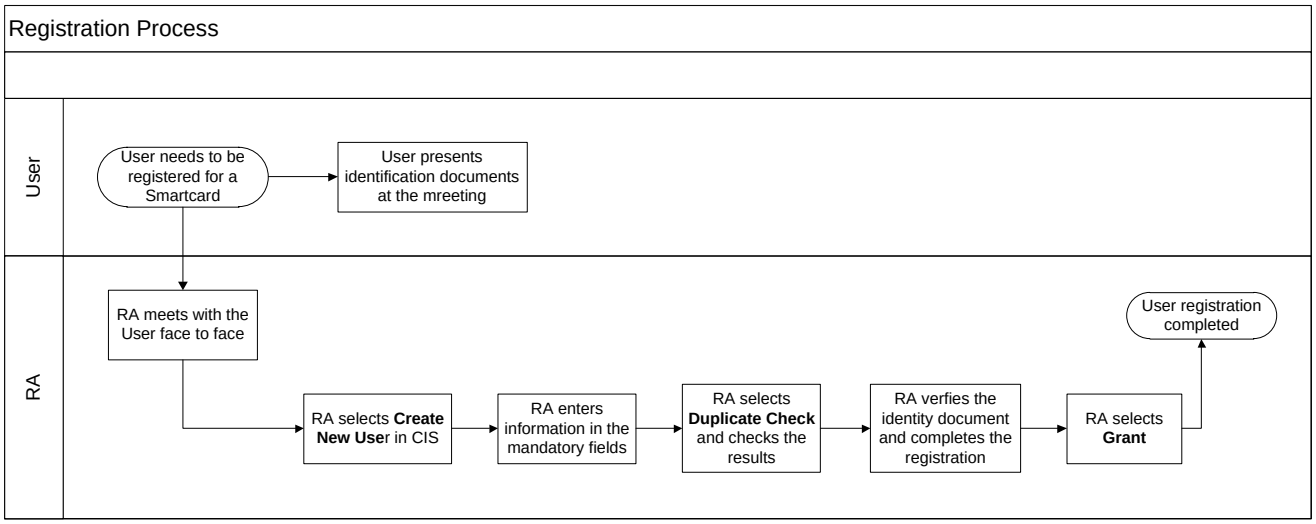
The following RA roles have the function to verify and create the identification of the user in Care Identity Service:

- RA Manager
- Advanced RA Agent
- RA Agent
- RA Agent ID Checker

Care Identity Service enables RA staff to register users as a single person process without the requirement for a Sponsor to approve the request.

Note: Using a document that is out of date will generate an audit alert that must be investigated by the RA Manager and the organisations governance structure.

An overview of the Registration Process in Care Identity Service:



5.3 Issue Card Workflow

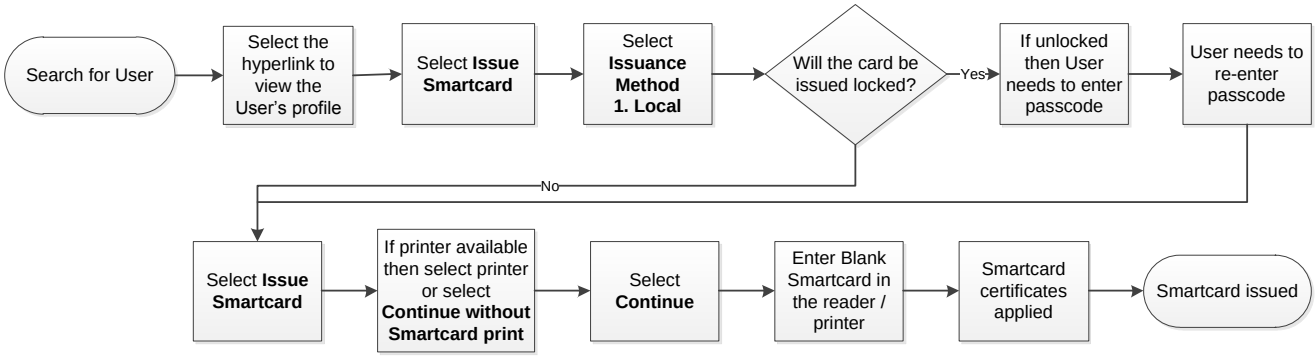
On registration of the user's details, RA staff must access the users access profile and select the **Issue Card** button to print the NHS Smartcard.

RA staff responsible in issuing Smartcards should be aware of the following:

- If the user is present, then the user must set and confirm their Passcode in person.
- If the user is not present, then the Smartcard must be issued locked which means no Passcode is applied to the Smartcard.
- If the Smartcard has been issued locked then upon receipt of the Smartcard, the user must liaise with a Sponsor or a Local Smartcard Administrator to choose and set their Passcode in person using the *Assisted Unlock Smartcard Process*.

The Issue Card Process enables RA staff to either print the Smartcard at the time of issuance or defer to a later date. It is expected that RA staff will only defer printing Smartcards at the time of issuance due to Printer issues or where local processes require Smartcards to be printed in batch.

Issue Card Process



5.4 Assigning Access Control Positions

The CIS application enables RA staff to assign users Access Control Positions using any of the three options below:

- Approve and grant functions once a request has been created
- Directly assign Positions
- Assignable Positions

A declaration must be completed by the RA should they wish to directly assign positions to users without Sponsor approval. This process results in an audit alert that should be followed up and reviewed by the RA Manager and the organisations governance structure. Further information on the workflows of the three options is illustrated in this section.

The following table outlines the activities included in the baseline of the RA staff and Sponsors roles using the options to assign positions in CIS:

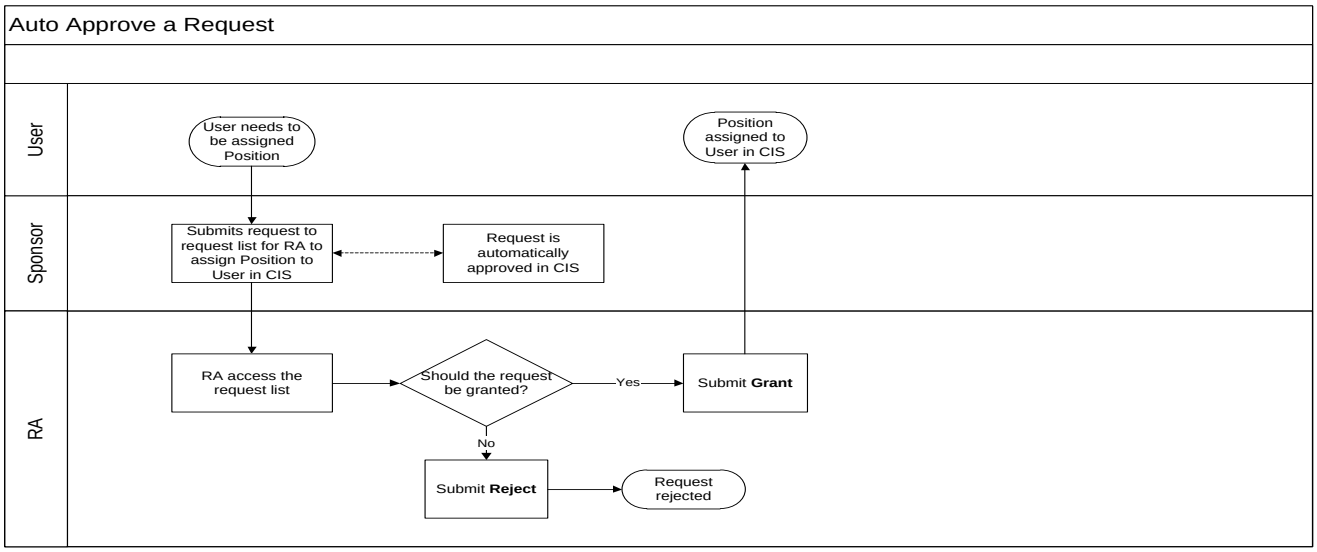
	RA Manager	Advanced RA Agent	Sponsor	RA Agent
Two person process- Approve and grant	Grant	Grant	Approve	Grant
Directly assign positions	✓	✓	×	×
Assignable positions	×	×	✓	×

5.4.1 Approve and Grant Process

Care Identity Service provides RA staff and Sponsors the option to use the mechanisms of two individuals to approve and then grant a request when assigning a position to a user.

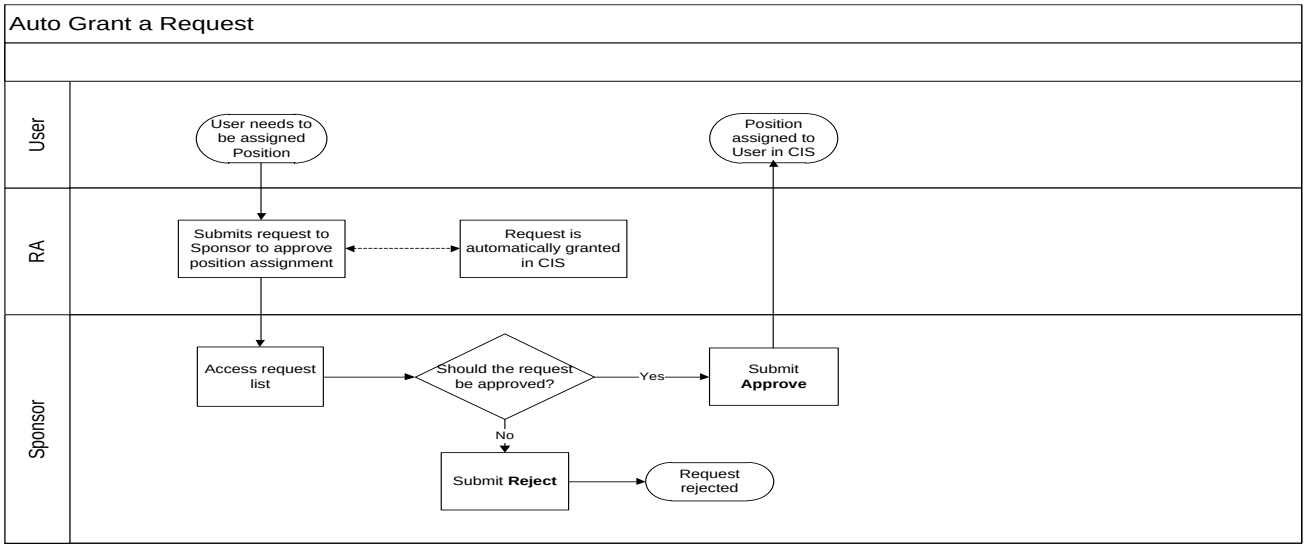
5.4.1.1 Auto Approved Request

A request submitted by a Sponsor in CIS is automatically approved. Thereby the RA Manager, Advanced RA Agent or RA Agent has the option to grant the request or reject it.



5.4.1.2 Auto granted request

In addition, a request submitted by the RA Manager, Advanced RA Agent or RA Agent in CIS is automatically granted. Thereby the only remaining action is for the Sponsor to approve the request.



5.4.2 Directly Assign Position

Access Control Positions can be directly assigned to users by RA Managers and Advanced RA Agent without Sponsor approval. A declaration must be completed by RA Managers and Advanced RA Agent where a request is not completed using the two person process of approve and grant.

The declaration consists of the RA Manager or the Advanced RA Agent selecting the checkbox **Proceed without Sponsor approval** within CIS which provides them the ability to directly assign the position to the user. If the checkbox is not selected, then the request will be submitted to the request list waiting for Sponsor approval.

Once the **Proceed without Sponsor approval** is selected, then a note is generated informing the RA Manager, that an audit event has been created.

Assigning this access without Sponsor approval will raise an audit event for possible follow up action by a governance authority.

5.4.3 Assignable Positions

Assignable positions are the term used for a group of positions assigned to a Sponsor to assign to users. Occasionally organisations will require Sponsors to have the ability to manage assignment to, and from, a limited set of positions. CIS allows organisations to use the Sponsorship activity function B1300 to approve requests to do this. Sponsors can be set up with the capability to assign individuals to a fixed set of positions.

5.4.3.1 Setting up Assignable Positions in CIS

In CIS when the RA create the position and select B1300, the tab ‘Assignable Positions’ is then displayed for that organisation. RA can select from the list which positions they will make as directly assignable positions.

The Sponsor’s position which includes B1300 is now defined with a list of ‘Assignable Positions’.

The user identified as the organisation’s Sponsor by the Executive Management Team needs to be assigned an Access Control Position that includes the B1300 activity and the assignable positions.

5.4.3.2 Assigning users to an Assignable Position

The Sponsor has the option to be able to assign users to any of these Assignable Positions in a single step using the Grant function.

5.4.3.3 Revoking users assignment

To remove the assignment, access can be revoked immediately using a one stage process by RA managers and Sponsors. Alternatively the assignment end date may be changed to today's date (if removal required immediately) or an appropriate date can be selected.

5.4.3.4 Example setting using Assignable Positions

At a GP practice, a practice manager's Access Control Position may contain the activity B1300 and the following Assignable Positions:

1. Practice Receptionist
2. Practice Nurse
3. Practice Medical Secretary
4. Practice GP
5. Practice Locum GP

This allows the practice manager to manage an existing NHS Smartcard user by single-handedly assigning the user to any of the above Access Control Positions. This could be for example, a temporary secretary or locum GP. There is no additional requirement to 'Approve' as this has already been done.

The practice manager has the option to set a start date of the position assignment in CIS in advance of the user joining the organisation so that the user has immediate access when they commence employment. In addition, the practice manager has the option to either set the end date of the assignment in advance or can directly revoke a user's position assignment when they leave the organisation.

5.5 Copy Position Process

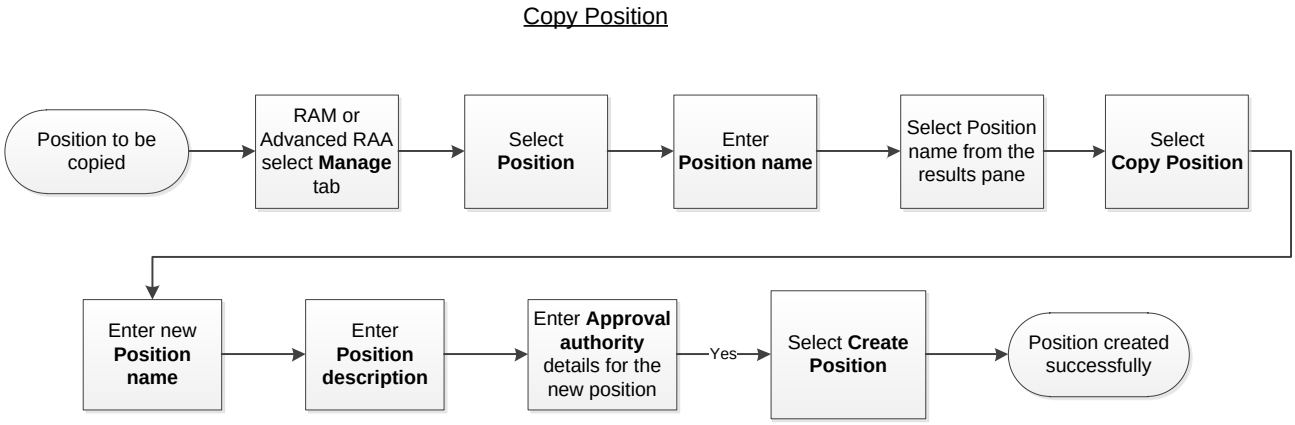
Further to the creation of an Access Control Position in CIS, RA Managers and Advanced RA Agents have the option to copy an existing Access Control Position in Care Identity Service using the Copy Position workflow.

This may be useful when an existing position has already been created either by the organisation or by another organisation which needs to be replicated in additional organisations.

However the following information is required in advance of creating the position in CIS as it the fields are mandatory in CIS:

- New Position Name
- Approval from the local governance structure

An overview below of the Copy Position process in CIS:



5.6 System Generated Positions

Access profiles assigned to users using the Spine User Directory/Calendra will migrate as a System Generated Position as a result of the Care Identity Service application only operating on positions.

At go live of the Care Identity Service, each of the access profiles assigned to a user in an organisation will migrate as a separate position. The format of the position name will be **00SYSPOS_[organisation NACS code]_Individual UUID**

There are certain limitations to Systems Generated Positions where RAs cannot:

- Assign other users to a System Generated Position
- Use as a predecessor position

However RAs can copy the System Generated Position which may be useful in the creation of a new Access Control Position. However there must be organisational approval in writing to create the position in CIS.

User's assigned more than one access profile in an organisation will migrate in a single System Generated Position**.** However where users are assigned an access profile in more than one organisation, the access profile in each organisation's will migrate as a separate System Generated Position.

5.6.1 Move to PBAC

Organisations must ensure they have moved fully to Position Based Access Control or have a plan to do so by December 2015 which includes moving people from System Generated Positions to Access Control Positions.

RA Managers and Advanced RA Agents have the option to use the batch function in CIS to assign users to an Access Control Position.

5.7 Request Lists

Request lists are the mechanism for managing requests that are created in CIS (or received from the ESR interface). An organisation can have as many request lists as required to support the needs of the business. However each organisation assigned an ODS Code, must have at least one request list. This includes any child organisations that are associated to the RA parent organisation including GP Practices and Pharmacies

Request lists can be used as a method of identifying the requests of specific departments and teams within an organisation.

All RA staff and Sponsors have the ability to view all the request lists within an organisation. However requests can only be viewed by RA staff or the Sponsor if they are able to action it.

In addition, only the RA Manager, Advanced RA Agent, RA Agent and Sponsor can submit a request in Care Identity Service.

Requests are submitted but not limited to the following processes:

- Assigning access to a user
- Un-assign and remove access from a user

5.8 System Generated Request Lists

Organisations that used the previous registration system UIM will have had to create a Worklist. Worklists in UIM will be migrated to the new Care Identity Service application.

However if an organisation has not created a Worklist in UIM, then at go-live of the Care Identity Service a default Request List will be assigned to the organisation which cannot be renamed or deleted in CIS.

The format of the default Request list name is as follows: “SYS_DEFAULTREQUESTLIST”.

5.9 Assisted Unlock Smartcard Process

The Assisted Unlock Smartcard Process enables the following RA roles to assist users to unlock their Smartcards and set a new Passcode:

- RA Manager
- Advanced RA Agent
- RA Agent
- Sponsor
- Local Smartcard Administrator

The functionality to unlock is included in the baseline of the RA Manager and RA Agent roles and is also included in the Sponsor or Local Smartcard Administrator business functions.

In addition to being able to unlock users NHS Smartcards RA roles; RA Managers, Advanced RA Agents, RA Agents can unlock each other’s NHS Smartcards. These RA roles should ensure that they are aware of how to reset NHS Smartcard passcodes using the Assisted Unlock Smartcard process in CIS and have access to a second card reader.

Sponsors and Local Smartcard Administrators can only unlock NHS Smartcard users and one another's NHS Smartcards and reset passcodes. Sponsors and Local Smartcard Administrators are unable to reset the passcode for any other RA role.

The table below determines who can unlock NHS Smartcards using the Care Identity Service application:

Role	Can unlock
RA Manager (R5080)	All other RA staff (including other RA Managers) and all other users
Advanced RA Agent (R5090 + B0274)	All other RA staff (including RA Managers) and all other users
RA Agent (R5090)	All other RA staff (including RA Managers) and all other users
RA Agent ID Checker (B0267)	None – needs B0263 to perform this function
Sponsor (B1300)	Can unlock all non RA users (including a Sponsor or LSA)
Local Smartcard Administrator (B0263)	Can unlock all non RA users (including a Sponsor or LSA)

Note: The Smartcard must be locked prior to resetting their Passcode in the CIS application.

5.9.1 To reset/unlock a user's Smartcard:

RA arranges a face-to-face meeting where the RA or Sponsor verifies the identity of the user and resets the Passcode. The user's identity should be confirmed by:

- The photograph on their NHS Smartcard
- If the identity cannot be verified, the user is required to produce documentary evidence to the RA. Refer to section 2.1: I.D. Management Guidelines.
- If the identity still cannot be verified, the incident is reported to the RA manager. It may be necessary to cancel or revoke the locked NHS Smartcard. Refer to section 5.20.7 Cancel Card Process.

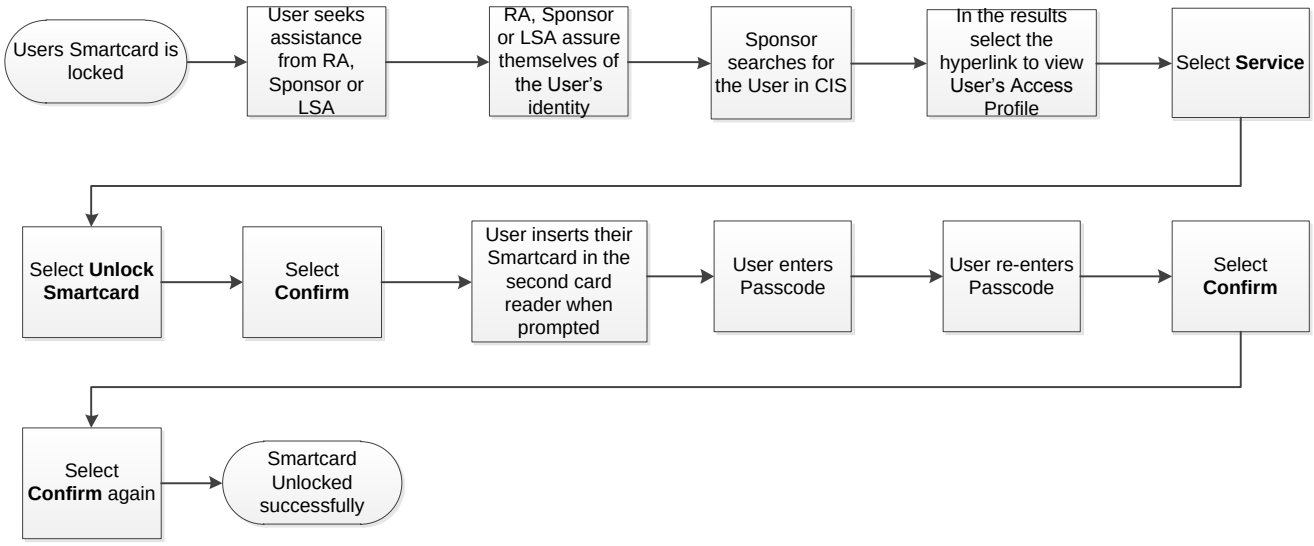
5.9.2 Assisted Unlock Process in CIS

The process below provides an overview of the workflow in CIS when a RA, Sponsor or LSA assists the user to unlock their Smartcard and reset the Passcode in the event the user forgets their Passcode or has incorrectly entered their Passcode three times.

The process below highlights the option where RA staff, Sponsor or LSA search for the user before selecting the option to unlock the user's Smartcard from their profile page in CIS.

However the tab **Manage Smartcard** is available to RA staff, Sponsors and LSAs to negate the need to search for the user first. Further information on the Manage Smartcard workflow is in section 5.18 of this document.

Assisted Unlock Process



5.10 Renewal of Certificates before expiry

Certificates assigned to NHS Smartcards need to be renewed every two years as per the Public Key Infrastructure policy. Users have the option to self-renew their Smartcard certificates on two separate occasions every two years before the certificates expire. However on the third renewal, users must visit their RA Manager, Advanced RA Agent or RA Agent to renew their certificates. RA staff renewing the certificates must verify that the individual is the user to whom the NHS Smartcard has been issued to. RA staff must check the photograph on the NHS Smartcard and assure themselves that the likeness is satisfactory before renewing their certificates.

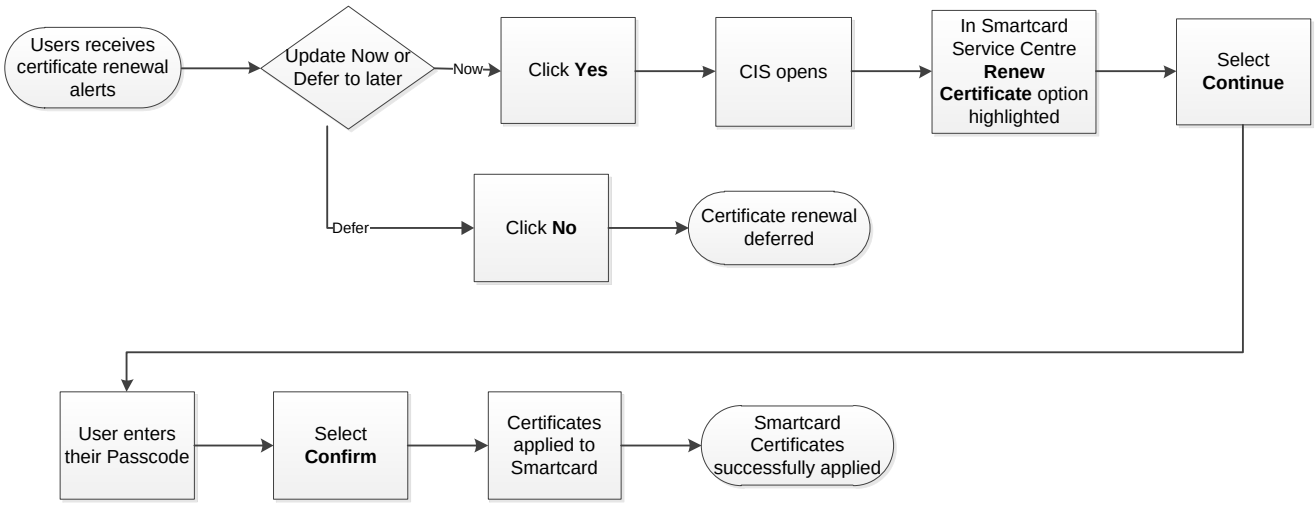
BT Identity Agent v11, v13 and the HSCIC Identity Agent v1.0 automatically prompt a NHS Smartcard user to renew their certificates within 30 days of expiry. In the 30 days prior to certificate expiry, users receive an alert once per day. Upon receiving this message users can choose to renew their certificates at that time or decline and renew later. In the seven days prior to certificate expiry, the renewal message is updated to reflect the urgency and the user receives the stronger message every day. Whilst it is not compulsory for the user to renew their certificates in the seven days prior to expiry, failure to do so will make their Smartcard inoperable once expired.

Users that are prompted to renew their certificates have the option to self-renew their certificates twice every two years using the Self–Renew Smartcard Certificates process in Care Identity Service.

5.10.1 Self-Renewal of Certificates Process

In the event a user receives an alert to renew their Smartcard certificates when they login with their Smartcard before they expire, the user has the option to continue to renew the Smartcard certificates or to defer until convenient.

Self-Renewal of Certificates Process



5.10.2 Assisted Renewal of Certificates Process

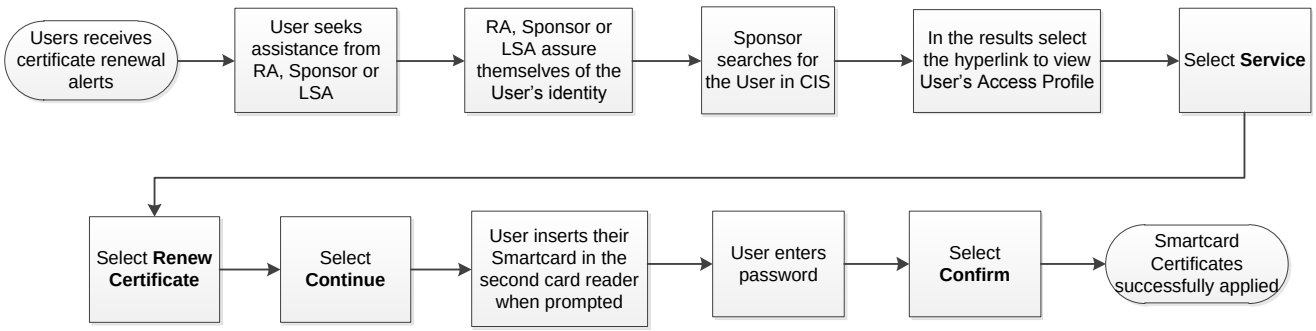
In addition there may be instances where users are unable to self-renew their certificates when prompted. Users can liaise with Sponsors or Local Smartcard Administrators who will assist to renew their certificates before they expire. RA staff, Sponsors or LSAs would need to utilise the Assisted Renewal of Certificates process in CIS to renew their Smartcard certificates.

The process below provides an overview of the process when a RA, Sponsor or LSA assists the user to renew their Smartcard certificates.

This option requires RA staff, Sponsor or LSA to search for the user first and then select the option to unlock the user's Smartcard from their profile page in CIS. However the tab Manage Smartcard is available to RA staff, Sponsors and LSAs to negate the need to search for the user first. Further information on the Manage Smartcard workflow is in section 5.21 of this document.

The option to renew certificates is only available when the certificates are due to expire within 30 days. However users will be prompted 30 days before the certificates expire on a daily basis.

Assisted Renewal of Certificates Process



5.11 Expired Certificates

Where the certificates have expired, this now becomes a Public Key Infrastructure aspect of the identity process and the NHS Smartcard may only be reissued by the following RA staff:

1 RA Manager
2 Advanced RA Agent
3 RA Agent
4 RA Agent ID Checker

Sponsors or Local Smartcard Administrators will not have access to the relevant workflows in CIS to reissue NHS Smartcards once the certificates expire.

The RA Manager, Advanced RA Agent and the RA Agent can re-issue certificates by reissuing the certificates using the Issue Card process in CIS. There is no requirement for the Smartcard to be cancelled before it is re-issued.

In addition the RA Agent ID Checker is only able to re-issue certificates using the Repair Card process.

5.11.1 Repair Card Process

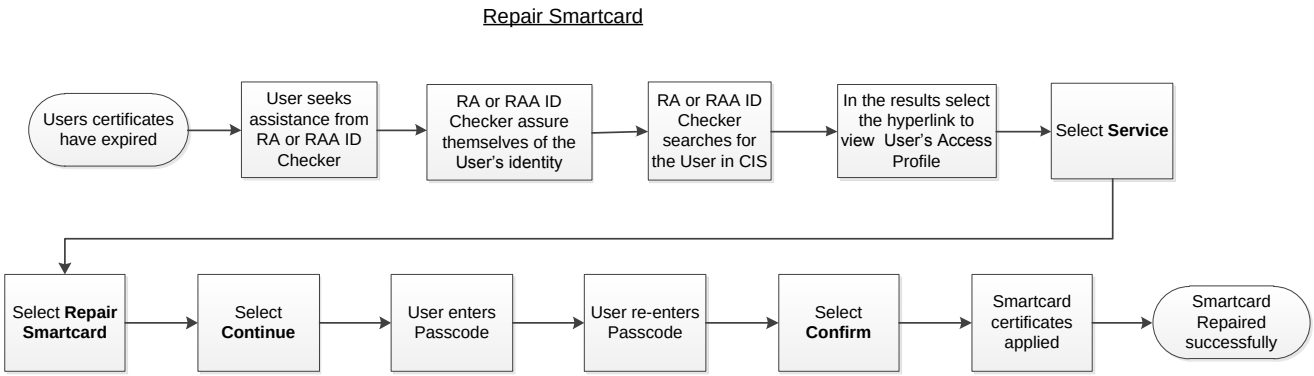
The Repair Card process needs to be undertaken when there is no physical change to the NHS Smartcard but the user's NHS Smartcard is faulty and is not permitting the user to log in with their NHS Smartcard to Spine. This could be as a result of the certificates being corrupted or the Issue Card process has not worked.

In addition the Repair Card process does not remove any other tokens assigned to the Smartcard where the Smartcard may be used for Extended Use purposes and the process is available to all RA staff including RA Agent ID Checkers to enable them to re-issue users NHS Smartcard certificates.

The Repair Card workflow initially removes all existing Smartcard certificates assigned to the NHS Smartcard and Passcodes before re-issuing the certificates and prompts the user to set a new Passcode. Users are advised to set a new Passcode that they have not already used.

During the issuance process when new certificates are applied to the NHS Smartcard, if the process fails, then this indicates that the Public Key Infrastructure has been unsuccessful. RA staff are advised to repair the Smartcard later when the Public Key Infrastructure is available.

An overview of the Repair Card workflow in CIS is outlined below:



5.12 Summary of the Processes available to Renew Certificates

The table below provides a summary of the processes available in CIS depending on the role assigned to the user.

Assisted Renewal of Certificates	Repair Smartcard	Cancel Smartcard and Issue Smartcard
Smartcard certificates are due to expire.	Smartcard certificates are due to expire or have expired.	Smartcard certificates have expired.
Assisted Renewal of Certificates Process is only available during the 30 day time period up to the certificate expiry date.	Repair Smartcard process to be used once the certificates have expired. All existing certificates are removed. Certificates are reissued as part of the PKI process.	Cancel Smartcard and Issue Smartcard process to be used once the certificates have expired. This now becomes a PKI process of creating new aspects of a digital identity.
Select **Renew** from Service.	Select **Repair Smartcard** from Service.	Select **Cancel Smartcard** from Service and select **Issue Smartcard** from user's profile page.
User prompted to enter their existing Passcode.	User prompted to set a new Passcode and confirm it.	Card can be issued locked or unlocked.
Can be actioned by RA staff, Sponsors or LSAs.	Can be actioned by RA staff including RA Agent ID Checkers but not Sponsors or LSAs.	Can only be actioned by RA Staff not RA Agent ID Checkers, Sponsors or LSAs.
Existing Smartcard to be used.	Existing Smartcard to be used.	User may require a new Smartcard to be issued if old one is lost/stolen.

5.13 Other User Processes

The NHS Smartcard user is able to perform the following processes themselves using the Care Identity Service application without additional assistance from the RA, Sponsor or LSA.

5.13.1 Change Passcode

A user will be able to change their Passcode at any time using the Change Passcode process in CIS. RA should recommend users do so at regular intervals.

5.14 Predecessor Positions

5.14.1 What are Predecessor Position links?

Care Identity Service has the functionality to link a Position in one organisation to one or more Positions in other organisations, known as Predecessors.

There is no electronic workflow in CIS to inform the RA of an organisation if another organisation has linked to their Position as a predecessor. Specific approval authority from the source organisation must be in place as this approval is recorded in CIS and is auditable. Therefore on creating the position and setting up the link, approval from the source organisation must be entered in the mandatory field in CIS. This is an additional authority to the approval authority required to create or modify the Position per se.

5.14.2 Why are Predecessor Position links needed?

There is an issue when Position assignment updates are sent from ESR to CIS to transfer access rights between organisations the process closes off the assignments in the user's old (source) organisation immediately.

From a legal/payroll perspective this behaviour is correct, but this action potentially results in users being denied access to IT systems in the source organisation before reconfiguration activity has taken place to enable access to IT systems in the user's new (target) organisation.

To resolve this issue, the functionality to add predecessor links to Positions was introduced.

The predecessor link continues to provide access even when the Position assignment in the source organisation has been end dated.

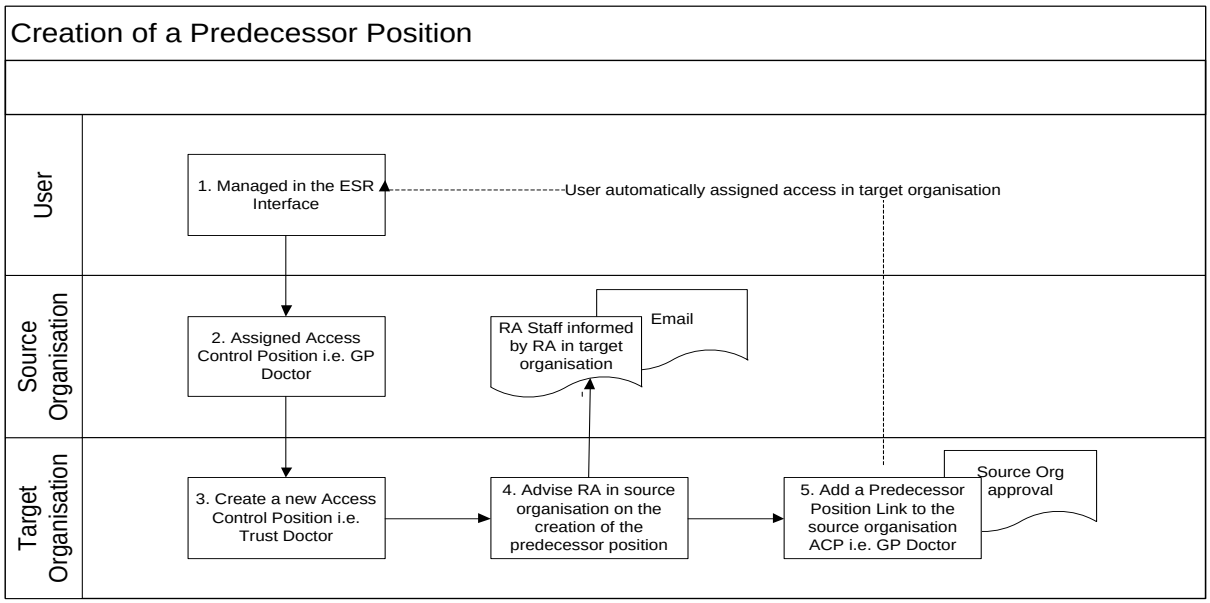
It is important to note that the predecessor position link must be removed by RA once the transition has been completed.

5.14.3 How is the Predecessor Position link created?

Predecessor Position links are added to the Position in the target organisation by RA staff at that organisation. The RA category does not have to be the same to allow predecessors between Positions in the target and the source organisation to be approved and granted in CIS.

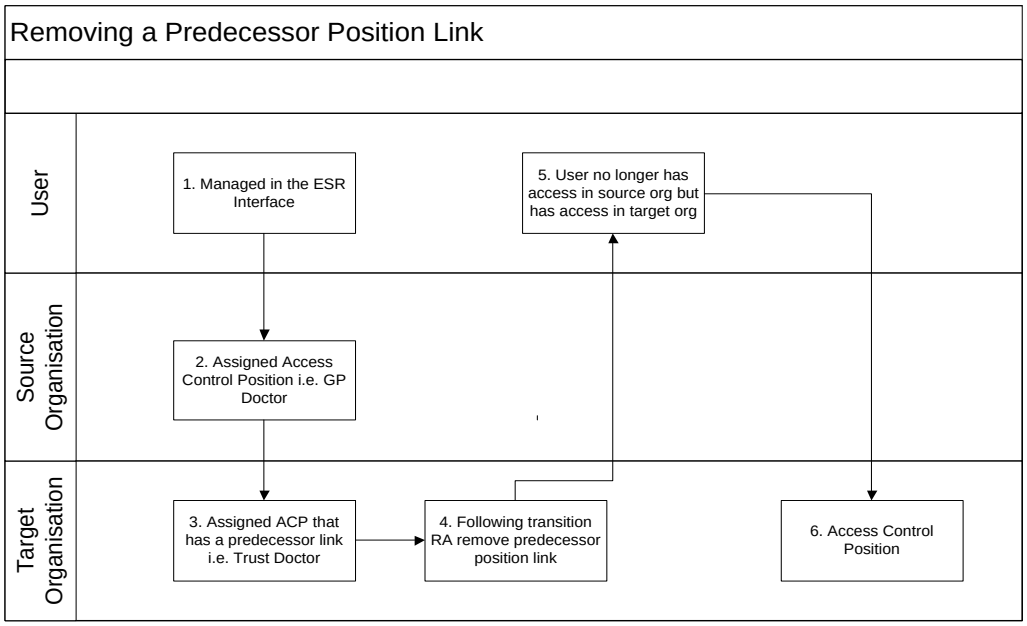
On creating a new position RA in the target organisation have the option to search for Positions in other organisations using CIS. Although the link can be added without the need for the RA at the source organisation being involved, it is expected that all RA staff will be aware of transition activities and the source organisation's approval is in place.

5.14.4 Creating the Predecessor link



5.14.5 Removing the Predecessor link

Once the predecessor link has been established and the user's access is managed by the RA at the target organisation, it is expected that the link is removed from the target organisation's position. Predecessor position links should be removed 12 months from the time they are set up.



5.15 Workgroups

Some applications use Workgroups to manage the access individuals have into the software. This additional level of access control is used in conjunction with the access assigned to a user's record on the Spine. The purpose of a Workgroup is to ensure that the individuals only have access to the patients within the remit of their departments or teams. Workgroups define and maintain Legitimate Relationship (LR) between patients and healthcare workers.

There are a number of applications that use the Workgroup functionality. These include TPP SystmOne and Lorenzo. These applications use Workgroups in two entirely different ways, Lorenzo is hierarchical and TPP SystmOne is granular and the options available for managing them through CIS are very different.

5.15.1 Workgroup roles

There are two Workgroup roles that are included in the baseline of certain RA roles and can also be assigned to an alternative user. The Workgroup roles consist of

- Workgroup Administrator (B0100 Manage Workgroups)
- Workgroup Membership Administrator (B0090 Manage Workgroup Membership)

5.15.1.1 Workgroup Administrator (WGA)

RA Manager and the Advanced RA Agent have the functionality in CIS to manage any Workgroup within their organisation as the business function B0100 is included in the baseline of the RA Manager and Advanced RA Agent roles.

In addition, the organisation has the option to assign the business function B0100 – Manage Workgroups to an alternative user to enable them to administer and oversee workgroups. The workgroup management actions consist of the following:

- Creating Workgroups
- Establishing and modifying the Workgroup hierarchy
- Changing the state and properties of an owned Workgroup
- View Workgroup membership and Workgroup membership administrators for Workgroups in their own organisation
- Manage Workgroup membership both for individuals and groups

5.15.1.2 Workgroup Membership Administrator (WGMA)

RA Managers, Advanced RA Agents and Sponsors have the functionality in CIS to manage workgroup membership for any workgroup that they have been assigned to manage. The business function B0090 – Manage Workgroup Membership is included in the baseline of the RA Manager, Advanced RA Agent and Sponsor roles. The Workgroup must be in the user's organisation or in the case of cross organisational Workgroups, linked to a Workgroup in the user's organisation.

In addition the organisation has the option to assign the business function B0090 - Manage Workgroup Membership to an alternative user to enable them with the following Workgroup membership responsibilities:

1. View members of their Workgroup
2. Adding users to Workgroups on an individual basis
3. Modify Workgroup membership from profile page

5.15.2 Workgroup Structure Setup

The first Workgroup created in an organisation is known as the **Root Workgroup**. Once created the Root Workgroup is fixed and cannot be removed or replaced. As further

Workgroups are created they must be linked to an existing Workgroup, known as its parent Workgroup. The newly created Workgroup is then referred to as a child Workgroup of its parent. However any number of Workgroups can be created.

If a user is a member of a Workgroup that has one or more child Workgroups below it, then they will also be able to access patient records through LRs not only of their Workgroup, but also of any child Workgroups.

It is important to ensure that the child Workgroup is created beneath the correct parent Workgroup by checking the parent Workgroup code and name.

5.15.3 Workgroup Approval

A mandatory requirement in Care Identity Service is to record the approval authority of the organisation's governance structure in the creation of a new Workgroup. This information must include as a minimum:

- Name of the approval authority
- Date of the approval authority
- Purpose of the Workgroup including why it has been created

5.15.4 Care Identity Service Options

CIS provides organisations the following three options when assigning Workgroups to users. These consist of:

- Access Control Position includes relevant Workgroup(s) OR
- Access Control Position consisting of access rights and an additional Access Control Position includes Workgroup(s) OR
- Workgroup assignment via Workgroup workflow separate to Access Control Position assignment

Note: In CIS a user is not limited to one Access Control Position assignment

5.15.5 ESR Interface Options

As a result of enhancements to the ESR Interface and the development of the Care Identity Service, organisations using the ESR Interface have an additional two options to assign users to workgroups.

The first option is an enhancement to a limitation in the ESR Interface which prevented users assigned to an ESR position to be linked to more than one Access Control Position. However since 25th September 2014, users assigned to one ESR Position can be linked to more than one Access Control Position.

The second option allows organisations to manage users assigned an ESR Position using the ESR Interface and assign Workgroups to the user as a separate workflow in Care Identity Service.

5.15.6 Workgroup Options

Option	ACP	Job Role Code	Business Codes	Workgroup	Assign	RA Impact	IG Level	ESR Compatible
1	One ACP	One Job Role Code	All relevant B codes	All relevant Workgroups	One ACP accessing all Workgroups	Low	Low – additional audit controls required	Yes
2 Part One	ACP Access	One Job Role Code	All relevant B codes	None	Assign Access Rights in one ACP – no access to Workgroups with just this ACP	Medium	Medium	Yes
2 Part Two	Workgroup ACP	Same Job Role Code as the Access	None	A single Workgroup	Assign the correct ACP Access ACP *(as per 2 Part One)* and assign each ACP for the required Workgroup for the user	Low	Medium	Yes
3 Part One	ACP Access	One Job Role Code	All relevant B codes	None	Assign Access Rights in one ACP – no access to Workgroups with just this ACP	Low	Medium	Yes - ACP linked to ERS Position
3 Part Two	Workgroup assignment outside of ACP	No Job Role	None	One or more Workgroups	Assign Workgroup access as a separate workflow	Low	Medium	Yes user access rights managed in ESR *(3 Part One)* and Workgroup assignment managed using CIS

5.15.7 Lorenzo Workgroups

There is a hierarchical solution for Workgroup management within Lorenzo; this allows any organisation that implements this solution, to produce a ‘family tree’ of the organisation. This allows a manageable solution to the organisation as the RA staff can assign individuals to a specific Workgroup and those individuals will automatically receive access to all of the Workgroups further down the tree.

It is recommended that CIS is implemented in advance of deploying Lorenzo.

Note: Staff will not be able to access Workgroups higher up the tree to the one(s) they have been assigned to.

5.15.8 TPP SystmOne Workgroups

There is a granular solution for Workgroup management within TPP SystmOne; this option requires staff to be assigned to every single Workgroup that they require access into. Depending on the approach adopted by an organisation, this solution can be very resource intensive and require a high level of management to maintain, especially if you have lots of Workgroups or users are constantly working in different teams on a regular basis for short periods of time.

5.16 Batch

The Batch functionality is only available to RA Managers and Advanced RA Agents.

Batch functionality enables the organisation's Registration Authority to group users and assign or un-assign positions in bulk. The following batch functions are currently available in CIS although further batch functions will be developed in a future release.

- Create Batch
- Assign users from one batch to another
- Bulk assignment to positions
- Bulk end date to positions

5.16.1 Create Batch

The Create Batch functionality is used to group a specific set of users within the organisation for various purposes.

5.16.2 Assign users from one Batch to another

Users can be assigned from an existing batch to an alternative subset of the batch.

5.16.3 Bulk assign users to Positions

Users identified in the batch can be assigned to a position in bulk. This negates the need for the RA to assign users to the position on an individual basis.

5.16.4 Bulk end date Position assignment

Existing users in a batch that have already been assigned to a position in bulk, may also have the position end dated in bulk by the RA.

5.17 Manage Smartcard workflow

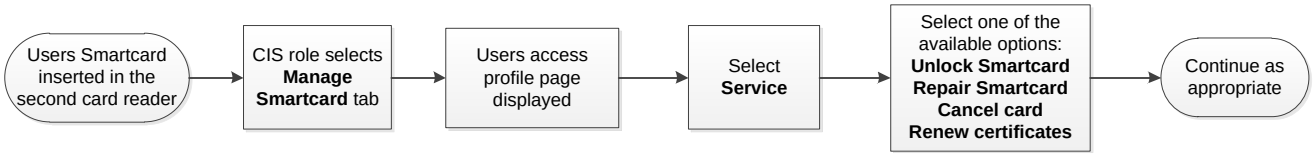
The Manage Smartcard tab enables RA staff to be automatically directed to the user's Access Profile page in CIS when the user's NHS Smartcard is inserted in the second card reader. This alleviates the need for RA staff to search for the user in CIS.

On selection of the Manage Smartcard tab in CIS, RA staff are prompted to insert the user's NHS Smartcard in the second card reader if a second NHS Smartcard is not automatically detected.

Depending on the RA role accessing CIS, the following options are available from the **Service** button in the user's Access Profile:

- Unlock Smartcard
- Change Passcode
- Print Smartcard
- Renew Certificates (only active if certificate is due for renewal)
- Repair Smartcard (renews certificates without formatting the card)
- Cancel Smartcard (allows Smartcard to be reissued)
- Destroy Smartcard (renders Smartcard unusable)

Manage Smartcard tab



5.18 Modify User

There may be instances including information entered incorrectly where the RA needs to modify the users Core identification (Name, Date of Birth and NI number).

Supporting information including Marriage or civil partnership certificate, Marriage or civil dissolution or Deed poll certificate must be provided to the RA to update the user's name.

The following workflow identifies the process in CIS where the RA modifies the user's core identification.

Modify User Process

5.19 Reporting

The following initial reports are available in the Care Identity Service application; additional reports will be made available to RA Managers in subsequent releases.

- Active user Report
- Positions in Organisations Report
- Smartcard Report

Active user Report

Column Headers of the Active user Report consist of the following:

- UUID
- Name (family, given, preferred)
- DOB

- Telephone number
- Email address
- Created on date
- Last modified date
- Created by
- Last modified by
- Whether managed by ESR
- E-GIF Status
- NI Number
- Number of assigned Smartcards
- Number of certificates due to expire
- Serial numbers
- Certificate expiry date
- Active user (Y/N)
- Last authenticated on
- IP address of last login
- T&Cs last version accepted
- T&Cs last version accepted on
- Organisation name
- Organisation code
- Legal parent name
- Legal parent code
- RA parent organisation name

Positions in Organisations Report

- Position name
- Position ID
- Access profile ID
- Organisation in which position is created
- Position status
- Is a system generated position
- Role code
- Organisation code for which access profile is created
- Is restricted?
- Is sensitive?
- Predecessor position ID
- Predecessor position name
- Access profile created date
- Access profile created by UUID
- Access profile last modified date
- Access profile last modified by UUID
- Number of users assigned to the position

Smartcard Report

- Smartcard Serial Number
- Smartcard type
- Smartcard Status
- UUID of user assign to Smartcard
- Name of the user Smartcard is assigned to

- Organisation Code
- Name of Organisation
- Number of certificates on Smartcard
- Will certificates expire in the next 90 days
- UUID of the Smartcard issuer
- Name of the Smartcard issuer
- Organisation that issued the Smartcard
- Date the Smartcard was issued

5.20 Leavers

All leavers must retain their NHS Smartcard if there is any possibility in the future that the user will access Spine enabled applications.

The only process that RAs should utilise to revoke access assigned to a user when the user is leaving the organisations is to set the position(s) assignment date to the leaving date or an appropriate date.

Users that are leaving the NHS or Healthcare should have their access revoked using one of the following options:

- Cancel Smartcard
- Destroy Smartcard
- Close user

Further information on the Cancel Smartcard, Destroy Smartcard and Close user Processes is provided below in this section.

It is essential that when closing a user, the correct user is identified. The RA should use the users UUID, or the user's name in the CIS search function.

When the RA is advised of the need to perform a revocation for a leaver it is recommended that they:

- Verify the user's identity by asking them their name, UUID, and confirm the user's identity or their photograph in CIS.
- If the leaver is a Sponsor, RA manager, or RA agent, establish role succession arrangements. If necessary, request they are removed from the temporary distribution list.
- If the user advises the RA directly that they are leaving, the RA should advise HR of the leaver's name, UUID, and the date the user is leaving. The RA updates the end assignment of all Access Control Positions associated to the user in that organisation to the leaving date.

RA Managers must ensure that they action the following in the event a NHS Smartcard has been returned to the organisation.

- NHS Smartcards that have been returned to the organisations should be destroyed using the Destroy Card workflow in CIS.
- Records must be kept of all NHS Smartcards that have been returned and destroyed.
- If returned NHS Smartcards are not destroyed immediately, they must be kept in a secure environment until they are destroyed.

To physically destroy a NHS Smartcard, either fold the NHS Smartcard so the crease goes through the chip, cut the NHS Smartcard through the chip, or hole punch the NHS Smartcard through the chip and use a permanent marker to mark that the card is no longer valid before placing in secure waste.

5.20.1 HR and RA departments

In organisations where HR duties are separated from RA, then the local organisations RA Policy must reference the local joiners and leavers policy. HR must advise the local RA in a timely way in the event a user leaves or will not work for the organisation so that RA can revoke access accordingly.

Where HR and RA processes are integrated, it is expected that HR will be involved in cancelling NHS Smartcards with the process described in their local policies for starters, leavers, and as part of their disciplinary or risk management process.

Where HR and RA duties are integrated using the ESR Interface then the five processes below from 5.20.2 to 5.20.6 are managed entirely using the ESR Interface. Refer to section 11: Integrated Identity Management for further details regarding the benefits of utilising the ESR Interface to CIS.

5.20.2 Leavers not returning to the NHS

Leavers with no intention to return to the NHS or unlikely to work in a healthcare organisation that may access Spine enabled applications or leavers having a change of career or leavers retiring should have all their access revoked. Once the date of leaving has been confirmed, the end assignment date for all the leaver's Access Control Positions within that organisation must be updated accordingly.

There are some healthcare workers that may work temporarily after retirement. Therefore leavers that are retiring should only have their access revoked by setting an end date to the position assignment and retain their NHS Smartcard.

If there is no likelihood that the leaver will ever work in the NHS or Healthcare and is not assigned additional position in other organisations then the leaver should be closed in CIS to revoke the access. Refer to section 5.20.9: Close User Process.

However, if the leaver has additional open organisations on their profile, the RA should confirm with the leaver that they no longer work for another organisation for which they require the NHS Smartcard before closing the leavers' profile.

In the event that the user's access profile is closed in CIS, it is the responsibility of the RA to request that all such NHS Smartcards are returned and destroyed within a reasonable timescale.

5.20.3 Leavers transferring to another NHS organisation

If the user is transferring to another health organisation, for example a GP practice, Acute Trust then the user must retain their NHS Smartcard but their current position assignment must be set an end date. This process is automated where the ESR Interface to CIS is deployed.

5.20.4 Short Term Leave (up to six months)

Where leave is expected to be up to six months and the user intends to return after this period, it is recommended that user's organisational access are removed the day they leave but the user must retain their NHS Smartcard. CIS should be used to identify the positions

assigned and must be end dated as appropriate. users can be reinstated their access when they return by assigning the user to the position again.

If prior to the end of the leave, RA has been advised by HR that the user has ceased to provide their services, then the user's end assignment date to positions in CIS for that organisation needs to be amended.

5.20.5 Extended Leave (more than six months)

Users who are planning to take sabbaticals should only have their position assignment end dated in CIS and retain their NHS Smartcard.

5.20.6 Maternity Leave

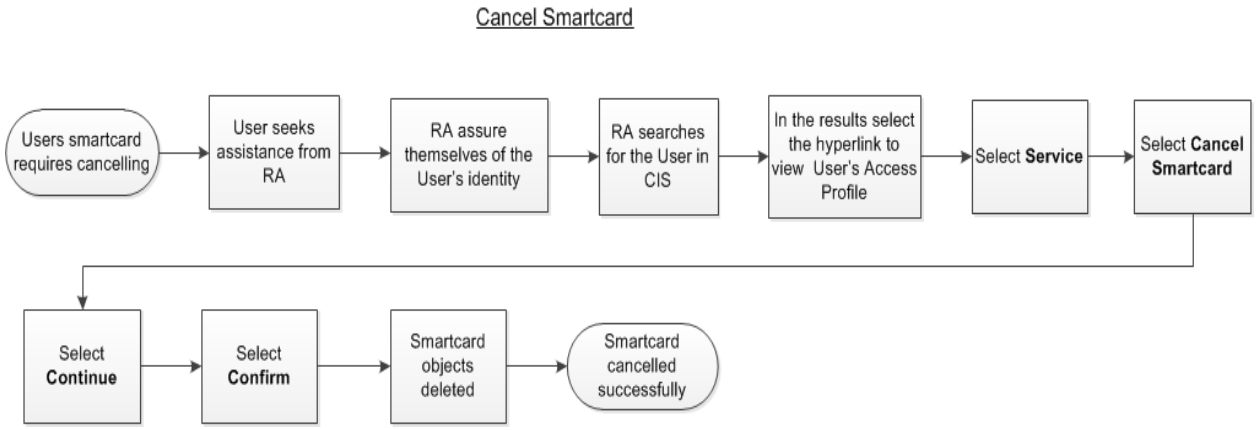
In the case of maternity leave it is still acceptable for the user to retain their NHS Smartcard whilst they remain in the employment of the organisation (even if it is unpaid maternity leave). The RA manager needs to gain assurance from the user through the application of the organisation's maternity leave policy as to the return date to work.

5.20.7 Cancel Card Process

The Cancel Card Process removes the users access profile including any position assignments, certificates and any additional tokens assigned to the Smartcard used for Extended Use purposes.

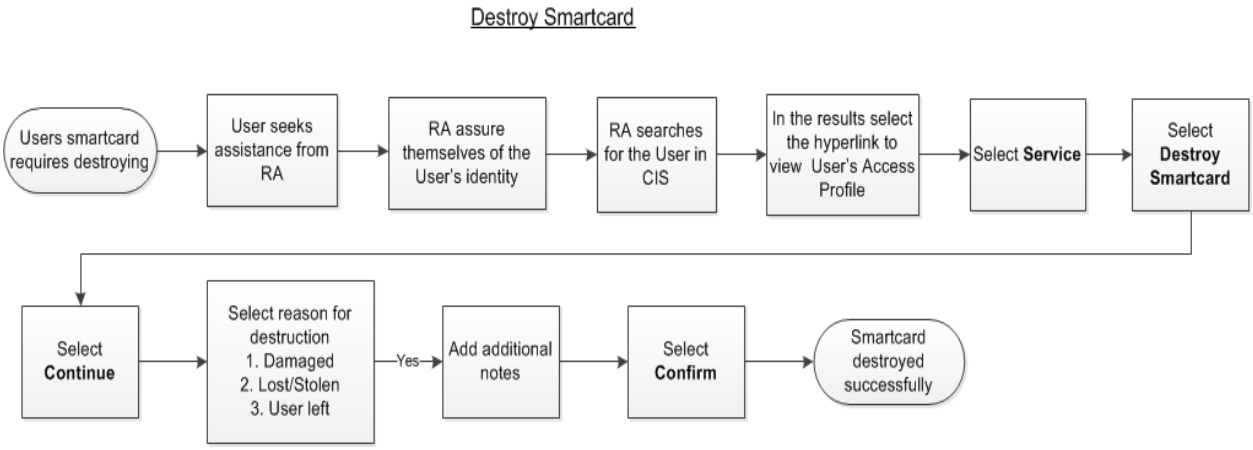
RAs are advised to action the Repair Smartcard process in CIS initially to resolve issues experienced with the NHS Smartcard.

Once the NHS Smartcard has been cancelled, it can be used to reissue certificates and assign access to the user.



5.20.8 Destroy Card Process

The Destroy Card Process renders the NHS Smartcard unusable and should only be used in the event the NHS Smartcard has been lost, stolen or damaged.



5.20.9 Close User Process

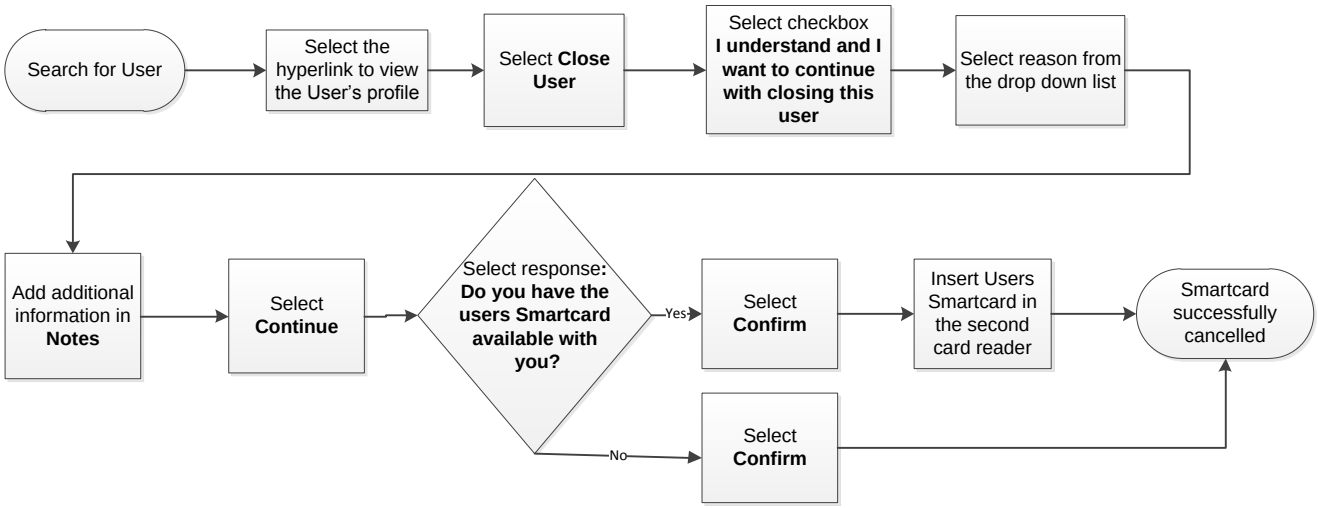
If a user is leaving an organisation, then the assignment end date for positions should be populated to ensure that all access is revoked in that organisation. The Close user workflow should only be used in exceptional circumstances where the user does not have any additional access profiles and will not be returning to work in the NHS or Healthcare.

Closing users using the Close user workflow will close all open requests, remove all access profiles, remove all Access Control Positions and cancel all Smartcards associated with the user. Available reasons in CIS include:

1. Card damaged
2. Lost or stolen
3. Leaving healthcare

Note: RAs that have to close a user's profile should exercise great care with the wording of any statement to be included in the CIS **Notes** field since this entry will form a permanent part of the Spine Audit Trail. If the closure results from sensitive or potentially contentious reasons, the RA is recommended to consult their HR colleagues department in advance to agree appropriate wording.

Close User Process



5.20.10 Reopen user Process

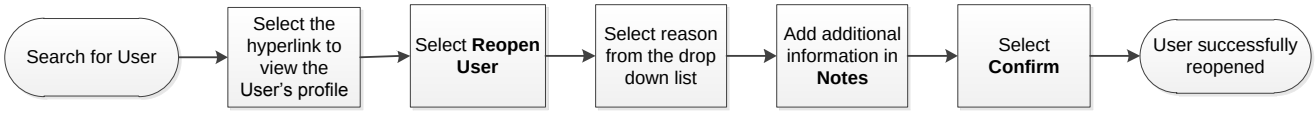
Users that have been closed using the Close user workflow can be reopened subsequently in CIS. This may be required where users have been closed by mistake, or returned to work in the organisation.

In CIS, the reasons when reopening a user consist of

1. Returned from long leave
2. Closed by mistake
3. Joined back
4. Other

RA staff must reconfirm identification where reasons1, 3 or 4 from the above list are selected.

Reopen User Process



5.20.11 Scenarios and Processes

The table below provides an overview of the different types of scenarios and what action RA should take in CIS.

	Cancel Card Process	Destroy Smartcard Process	Close user Process	End date Position Assignment
Lost or Stolen	×	✓	×	×
Leaving the organisation	×	×	×	✓
Leaving Healthcare	×	×	✓	×
Deceased	×	×	✓	×
Suspended	×	×	×	✓

5.21 CIS Forms

The Care Identity Service is an electronic system to register, issue Smartcards and assign access to Users. There may be circumstances where RA staff do not use CIS but the minimum mandatory data needs to be captured in a paper format to be entered into the electronic system CIS at a later time.

The CIS Forms are a contingency process for RA staff in the event CIS is not being used. RA staff will subsequently need to enter the information from the forms in CIS.

The CIS Forms are available in the following location:
http://systems.hscic.gov.uk/rasmartcards/cis/forms/cisforms

RA staff that have not completed the forms but are entering the information from the forms in CIS must record the RA staff or Sponsor declaration details from the forms in the **Notes** field in CIS.

As the CIS forms capture the minimum CIS mandatory data and are used to enter data into an electronic system, the CIS forms will need to be retained for 2 years in a secure location as per NHS England guidance at http://www.england.nhs.uk/wp-content/uploads/2014/02/rec-ret-disp-sch-guid.pdf. (Page 22)

The CIS Forms consist of the following:

- CIS - Create New User (RA use only)
- CIS - Request Creation of New User (Sponsor use only)
- CIS - Modify User Personal Details
- CIS - Position Assignment Modification
- CIS - Cancel Smartcard

5.21.1 CIS Create New User form

The information in the CIS Create New User form must be entered in CIS in the event CIS is not being used to register a new Smartcard user. This form is to be used by the following RA roles to register a new Smartcard user in CIS.

- RA Manager
- Advanced RA Agent
- RA Agent
- RA ID Checker

The above RA roles must ensure that the applicant's identification is verified to e-GIF Level 3. Identification documentation presented by the applicant as per the Identity Checks at NHS Employer Standards at the face to face meeting must be recorded in the form and a photograph of the individual must be captured at the meeting that is suitably labelled to be uploaded to CIS.

New Smartcard Users will still be required to access the Care Identity Service to electronically accept the Terms and Conditions of Smartcard use once they have been issued their NHS Smartcard.

5.21.2 CIS Request Creation of New User form

The CIS – Request Creation of New User form is to be used by Sponsors to request the creation of a new user in the Care Identity Service which must then be sent to their local Registration Authority who will arrange a meeting with the applicant to verify identification.

5.21.3 CIS Modify User Personal Details form

The CIS - Modify User Personal Details form is to be used by RA staff responsible for verifying identification in the event a change needs to be made to a user's personal identity. Identification must be verified to e-GIF Level 3 and Smartcard Users must present proof of identity as per the Identity Checks at NHS Employer Standards to request a change to a user's personal details as result of the following circumstances:

- Marriage
- Change of Name by deed poll
- User name incorrect in CIS

5.21.4 CIS Position Assignment Modification form

The CIS - Position Assignment Modification form is to be used by RA staff or Sponsors to request the assignment or un-assignment of a position to an existing user's access profile.

5.21.5 CIS Cancel Smartcard form

The CIS – Cancel Smartcard form is to be used by RA staff or Sponsors to request the cancellation of a Smartcard.

RA staff entering the information in CIS should select the appropriate CIS workflow to cancel the Smartcard. Further information on the different scenarios and guidance of the workflows is found in section 5.20.11 of this document.

6 Registration Authority Restrictions

RA restrictions impact the workflows available to Registration Authorities in Care Identity Service to grant access to identified users access profiles. There are two areas which affect and restrict the access that can be assigned to users. These consist of:

- Root RA function
- RA Hierarchy

6.1 Root RA Function

There are restricted Job Roles and Activities which can only be granted by the Root RA function at the HSCIC.

The National RBAC Attribute Administrator can specify that certain elements of an access profile (Restricted Job Roles and Activities) are only granted by the Root RA function.

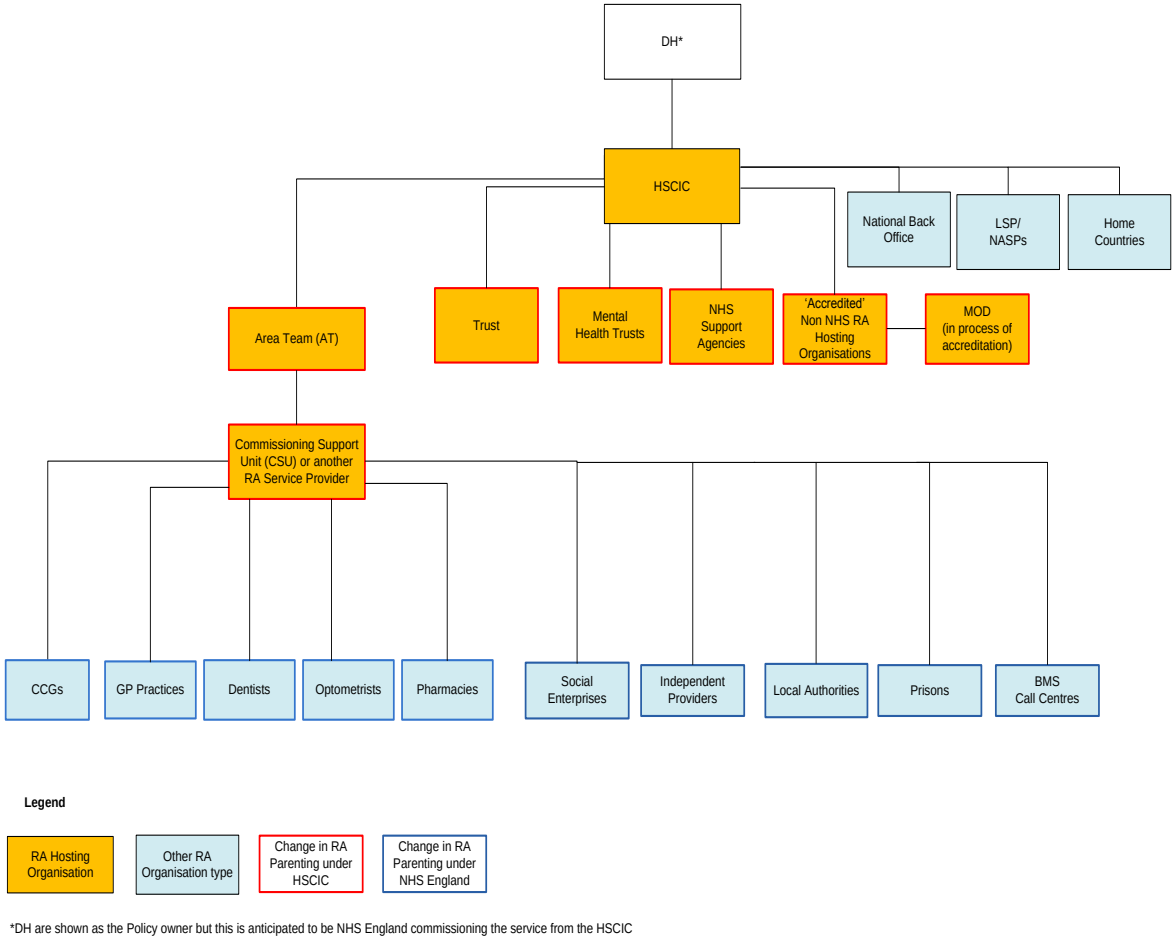
These access profile elements generally relate to those used by system suppliers and the HSCIC to provide access to functionality not intended for users accessing the Spine. These activities are visible in the National RBAC Database but are marked **NOTE: THIS ROLE IS NOT YET AVAILABLE FOR GRANTING** and have a **Yes** in the restricted column.

6.2 RA Hierarchy on the Spine

The RA Operating Guidance 2013/14 stated that Area Teams should commission the RA service from a RA Service Provider via a contract. Although the RA hierarchy potentially identifies RA Service Providers that have GP practices and pharmacies explicitly associated with them; the RA hierarchy may not reflect the detail of the contract process.

However, the commissioning contract process recognises that a RA Service Provider can include a CSU, CCG, Trust (where providing a service to the primary care) or any other organisation that will provision the issuing and updating of NHS Smartcards.

The diagram below sets out the RA Hierarchy on the Spine as per the Registration Authorities: Operating Guidance 2013/14 and is still relevant:



*DH are shown as the Policy owner but this is anticipated to be NHS England commissioning the service from the HSCIC

A cascade model is used to issue NHS Smartcards to RA Managers within NHS legal organisations. The updated RA Hierarchy models broadly consist of but are not limited to:

1. HSCIC to Trust
2. HSCIC to Area Team to RA Service Provider
3. HSCIC to Local Service Providers, National Application Service Providers
4. HSCIC to 'Accredited' Non NHS RA Hosting organisations (subject to successful completion of pilot implementations)

The RA hierarchy ensures that

- RA Managers can manage the Job Roles and Activities in their organisation and RA hierarchy.
- Registration Authorities cannot assign or un-assign an Access Control Position from users access profiles who are not in their organisation or in an organisation for which they are not a provider of RA services for.
- RA Managers and RA Agents can grant Access Control Positions to their own organisation and to any organisation that they have explicitly requested to associate to in the RA hierarchy.

6.2.1 RA Hierarchy Principles

The RA hierarchy is updated and maintained using the HSCIC RA08 form. The HSCIC RA08 form enables the RA admin link to be created or modified; an explicit association between an organisation and the RA Parent organisation. The RA Manager of an organisation is the designated signatory of a request to the HSCIC ODS team.

The principles below refine the setup of an organisations RA Hierarchy model and are used by the HSCIC ODS Team when the RA Manager in an organisation submits a HSCIC RA08 form to create or modify a RA admin link with another organisation.

- The RA Hierarchy does not necessarily follow the contract.
- Where sub contract arrangements exist, re-parenting will be to the prime contractor
- Only ISHP organisations and the virtual locum organisation will have a RA category type ‘RA non Hosting’ parented by the relevant RA Service Providers.
- PCT organisations must be RA Parented to the NHS organisation that employs the users accessing PCT codes.
- PCT organisations to be set a RA category type of ‘RA Parented’.
- Only legal entities can RA Parent child organisations and be set as RA Hosting organisations.
- CSU will be RA Parented to the Area Team where the CSU is the RA Service Provider and has a RA category type ‘RA Hosting’.
- Where CCG organisations are the RA Service Provider, they will be parented to the Area Team and have a RA category type as ‘RA Hosting’.
- All other CCG organisations will be at the same level as GP Practices, Pharmacists, the Independent Sector, Dentists, and Prisons etc.
- HSCIC is the RA Parent of Trusts.
- Where Trusts are the RA Service Provider, although they will be RA Parented to the HSCIC, they will still be accountable to the Area Team. Trusts will need to demonstrate contract compliance, provide the necessary reports and KPIs to the Area Team.
- NHS Health Informatics Services (HIS) are not legal entities and cannot operate a Registration Authority. The hosting organisation i.e. Trust of the HIS must be the RA Parent in the RA Hierarchy.
- Non NHS organisations that are not included in the non NHS RA pilot, or not commissioned by NHS England to provide RA services under the Lead Provider Framework, cannot operate as their own Registration Authority. Staff in the non NHS organisation will need to be assigned the appropriate RA function in the NHS organisation.
- The RA Service Provider must be the RA Parent of the child organisation except where the RA Service Provider is a non NHS organisation and when the RA service is provided by more than one RA Service Provider.
- Where the RA Parent is not the RA Service Provider, there must be an agreement in place with the Area Team confirming this arrangement.
- The RA Hierarchy must be aligned to the governance elements of the Public Key Infrastructure (PKI) requirements.
- Accountability must be clearly defined in the RA Hierarchy or through contractual arrangements.
- Where a RA Service Provider has a contract with more than one Area Team then a Lead Area Team must be identified to parent the RA Service Provider.

- Where a CCG has identified more than one RA Service Provider to provide the RA service, then the RA category type of the CCG will need to be 'RA Hosting'. The RA Service Providers will need to be assigned the RA roles in the CCG.
- Where a CSU is providing the RA service to the Area Team, then the CSU will need to be assigned the appropriate RA roles in the Area Team.
- Other than the Area Team or the HSCIC in the RA hierarchy, a 'RA Hosting' organisation cannot RA parent another 'RA Hosting' organisation.

6.3 RA category types

As part of the process of assigning a new organisation an Organisation code on the Spine, the HSCIC ODS team also assign one of the following RA admin category types from the table below. The table below also provides information on the aspects and restrictions of each of the RA category types.

RA admin category	Details
Non-RA Hosting	• can have multiple parents • RA agents in the parent(s) cannot manipulate users in the organisation • can only establish RA agents within the organisation
RA Hosting	• can only have single parent • RA agents in the parent cannot manipulate users in the organisation (with one caveat, the RA manager can 'seed' the RA manager) • can have RA manager(s) and RA agents
RA Parented	• can only have single parent • RA agents in the parent CAN manipulate users in the organisation • can only establish RA agents within the organisation

Prior to 2008, Independent Sector Healthcare Providers were created with an RA admin category of RA Parented. Since the introduction of the 2008-a Spine upgrades, ISHPs are sometimes created with an RA admin category of Non RA hosting.

The only exceptions and CIS processes that override the organisation restrictions include

- **Close User Process** - A RA Manager or a RA Agent can close a person entry in an organisation outside of their administrative control despite any open access profiles associated with that entry. If there are access profiles open, then attempting to close the person entry will close all entries belonging to the RA's organisations and close the entries associated belonging to organisations outside of the RA's control.
- **Unlock Smartcard** – A Sponsor or a LSA can assist a user to unlock and reset a user's Smartcard even if the user does not belong to their organisation.
- **Renew Certificates** – Similarly a Sponsor or LSA can assist a user to renew their certificates before they expire even if the user does not belong to their organisation.

7 Independent Sector Healthcare Providers

Independent Sector Healthcare Providers are defined as provider units that can be private, voluntary, not for profit, or independent healthcare establishments under the regulatory remit of the Care Quality Commission. An ISHP is any establishment (or service, agency, practice, or business) registered with the Commission under the Care Standards Act 2000, as amended by the Health and Social Care Act 2012, and to also comply with Private and Voluntary Health Care (England) Regulations 2001.

7.1 ISHP in the RA Hierarchy

Users in ISHP organisations requiring NHS Smartcards and an access profile associated with their ISHP organisation must be technically associated with a NHS organisation on the Spine. The ISHP organisation must be a child organisation of an NHS organisation in the RA hierarchy.

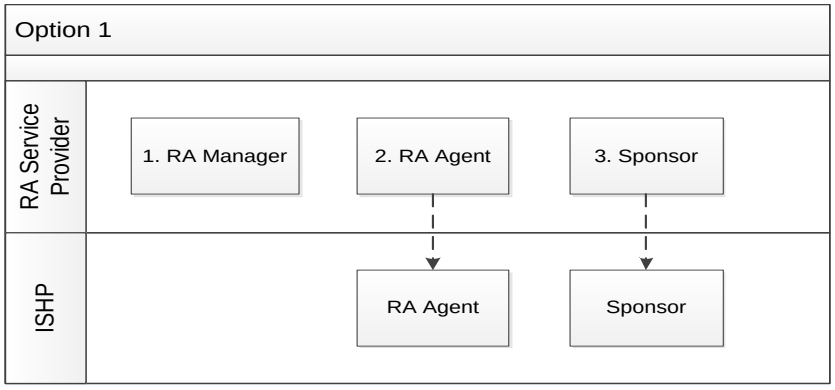
As a result of the RA hierarchy principles in section 6.2.1; if the RA Service Provider is an NHS organisation then the NHS organisation is the RA Parent of the ISHP organisation. However if the RA Service Provider is not a NHS organisation, save for the Non NHS pilots or non NHS organisations commissioned to provide RA services under NHS England's Lead Provider Framework, then RA staff in the RA Service Provider must be assigned an access profile in the NHS organisation to discharge their RA duties.

RA Service Providers that provide a RA service to an ISHP have a range of options that they can implement to issue NHS Smartcards to users, assign and update users' access profiles.

The options available to RA Service Providers are as follows:

7.1.1 Option 1

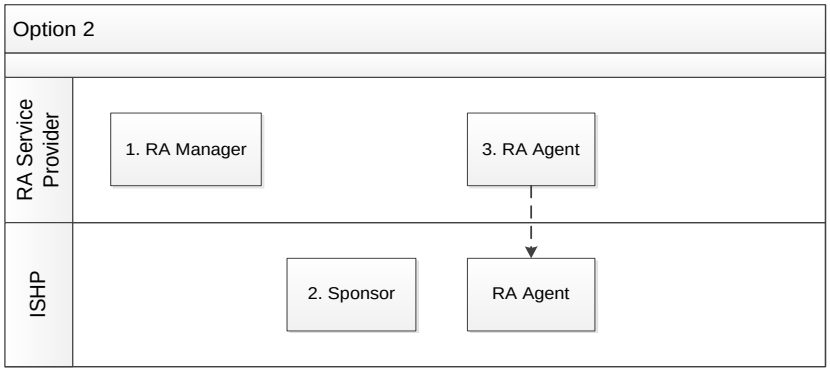
Identify and provide RA staff from the RA Service Provider to the ISHP.



Notes	Description
1	RA Manager at the RA Service Provider identifies a RA Agent and Sponsor from the RA Service Provider to provide a RA service to the ISHP. Sponsor is appointed in writing by the Executive Management Team at the RA Service Provider or the Executive Management Team at the ISHP.
2	RA Agent from the RA Service Provider assists in providing a RA service to the ISHP.
3	Sponsor from the RA Service Provider assists in providing a RA service to the ISHP.

7.1.2 Option 2

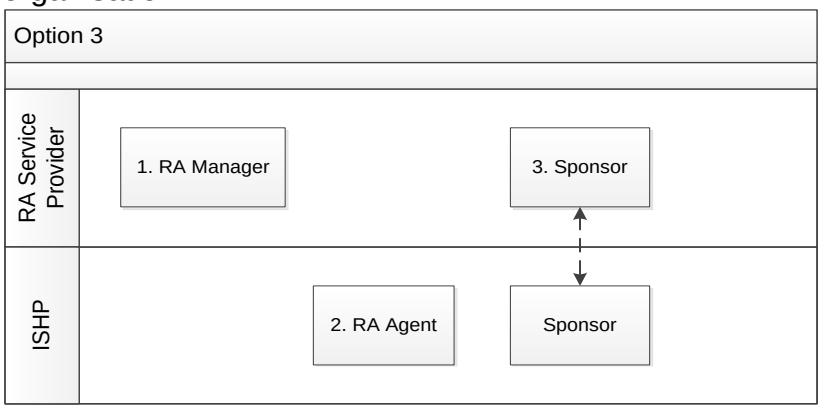
Identify Sponsors belonging to the ISHP to perform the Sponsor role using the same RA processes as the NHS organisation, whilst retaining the RA agent role within the NHS organisation.



Notes	Description
1	RA Manager at the RA Service Provider identifies a RA Agent to provide a RA service to the ISHP. Sponsor is identified by the ISHP and is appointed in writing by the Executive Management Team at the RA Service Provider or the Executive Management Team at the ISHP.
2	RA Agent from the RA Service Provider assists in providing a RA service to the ISHP.
3	Sponsor from the ISHP assists in providing a RA service to the ISHP

7.1.3 Option 3

Identify RA Agents belonging to the ISHP to perform the RA Agent role using the same RA processes as the NHS organisation, whilst retaining the Sponsor role within the NHS organisation.

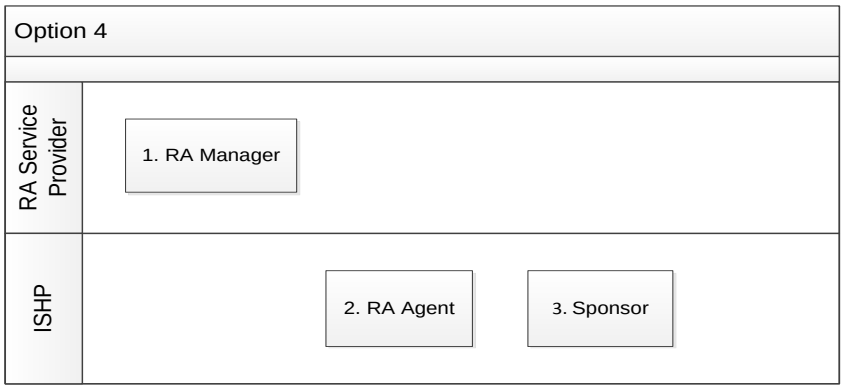


Notes	Description
1	RA Manager at the RA Service Provider identifies a Sponsor to provide a RA service to the ISHP. Sponsor is appointed in writing by the Executive Management Team at the RA Service Provider or the Executive Management Team at the ISHP.
2	RA Agent from the ISHP assists in providing a RA service to the ISHP.

3	Sponsor from the RA Service Provider assists in providing a RA service to the ISHP.

7.1.4 Option 4

Use a combination of RA Agents and Sponsors belonging to the ISHP.



Notes	Description
1	RA Manager at the RA Service Provider identifies a RA Agent and Sponsor from the ISHP. Sponsor is appointed in writing by the Executive Management Team at the RA Service Provider or the Executive Management Team at the ISHP.
2	RA Agent from the ISHP assists in providing a RA service to the ISHP.
3	Sponsor from the ISHP assists in providing a RA service to the ISHP

7.1.5 Consumables

ISHPs are required to procure their own Smartcard readers and where necessary Smartcard printers. The NHS organisation providing RA services to the ISHP will provide sufficient NHS Smartcards for ISHP healthcare professional/workers' to access Spine compliant applications.

7.2 ISHP Headquarters

ISHP Headquarters are required for Choose and Book or the new eRS Directory of Service (DoS) purposes. All private providers requiring Choose and Book/eRS must ensure users are registered to e-GIF level 3 in CIS. The Care Identity Service only supports users being registered to e-GIF Level 3.

7.2.1 Background

Services provided by an ISHP are registered for the purposes of the Directory of Services to the ISHP Headquarter (ISHP HQ) regardless of the location of the provider of the service or the organisation managing the service. As the Directory of Services for the ISHP HQs may be managed by an ISHP site or any other organisation, users need to be assigned to the ISHP HQ.

7.2.2 RA Parents of ISHP HQs

Organisations must complete and submit the HSCIC RA08 form to be set as the RA Parent of an ISHP HQ on the Spine.

ISHP HQs may be supported by a single legal organisation in which case they must support

- Staff at other organisations who require access to set up the Choose and Book / or the new eRS DoS
- Staff at ISHP Sites who are either setting up the ISHP Choose and Book / or the new eRS DoS, or require access to Choose and Book to manage referrals.

Alternatively, multiple legal NHS organisations can support the providers who require access to the ISHP HQ NACS code. A single RA Parent may support the geographical ISHP HQ, other sites or commissioning organisations may utilise a different organisation to provide the support ISHP sites.

ISHP Headquarters have the RA admin category type as non RA Hosting organisation to enable multiple RA Parents support ISHP sites. The RA agent will need to be assigned to the organisational code of the ISHP HQ.

The Care Identity Service enables the RA Service Provider to devolve RA activities to the ISHP HQ by identifying and assigning users in the ISHP HQ to the Advanced RA Agent, RA Agent, RA Agent ID Checker, Sponsor and Local Smartcard Administrators roles. However, the RA Manager in the RA Service Provider is responsible for training users assigned to the RA roles and regular audits of the roles and activities associated with the ISHP HQ as they are responsible for governance within the ISHP HQ.

7.2.3 Approval of Sponsors in ISHP HQ

Users assigned to the Sponsor position in the ISHP HQ must be identified and approved by either the Executive Management Team at the RA Parent organisation or the Executive Management Team at the ISHP HQ.

7.3 Non - NHS Pilots

In 2014, the HSCIC commenced a pilot with a small number of non NHS organisations running their own Registration Authority. Following evaluation of the pilots, the HSCIC will review options for a wider roll-out in the future. However in the interim, the role of RA managers must not be created in any non-NHS organisation, except where non NHS organisations have been commissioned to provide RA services under NHS England’s Lead Provider Framework, until further guidance is made available from HSCIC.

8 FFFFF

FFFFF is the virtual National Locum Pharmacy organisation on the Spine parented by all RA Service Providers in the RA hierarchy.

8.1 Background

As locum pharmacists that use the Electronic Prescription Service application require an access profile in each organisation that they work, the National Locum Pharmacy organisation FFFFF was created on the Spine to enable locums to operate within the country without the need to be assigned to a specific organisation in which they are working.

The former National Information Governance Board (NIGB) originally agreed that Locum Pharmacists when logged onto the EPS application do not need to be associated with the specific organisation in which they are working.

As a result the virtual National Locum Pharmacy organisation (FFFFF) RA parented by all RA Service Providers was created specifically for this purpose, and no other. The RA admin category type of FFFFF is set to non RA Hosting organisation.

Subsequently the NIGB extended the use of the FFFFF code to include pharmacy technicians.

8.2 RA Roles in FFFFF

The RA Service Provider must be the RA Parent to FFFFF to assign RA Agents from their organisation to the FFFFF organisational code. RA Service Providers must complete and submit the HSCIC RA08 form to the Exeter Helpdesk to enable the RA parent and child association on the Spine.

To manage users within FFFFF a RA Agent will need to be assigned with the organisational code of FFFFF.

The Local Smartcard Administrator role is not required in FFFFF as users should be assigned this role within the pharmacy because unlocking works irrespective of the organisation. Therefore RA staff in the RA Parent organisations must assign users to the Local Smartcard Administrators position in the organisational code of the local pharmacy. On assignment of the local pharmacy organisation code, Local Smartcard Administrators have the functionality to unlock users Smartcards in FFFFF.

8.2.1 Assignments

The FFFFF code is used by qualified locum pharmacy staff and pharmacy technicians to operate EPS Release 2 functionality. This enables a Pharmacist or a Pharmacy Technician to have one position to provide locum support at different dispensing sites where it is not practical to assign them to individual Pharmacy ODS location codes and commence in a single period when RA services are unavailable, thereby mitigating patient safety risks.

However, Sponsors must not approve assignment of the Pharmacist or Pharmacy Technician positions to staff not qualified as pharmacists or pharmacy technicians.

On assignment of the FFFFF code, pharmacy staff and pharmacy technicians can operate within the entire country.

8.2.2 Process

The FFFFF code must only be allocated to those locums who do not work at a regular location or are expected to work in five or more different locations at very short notice. If the FFFFF code is not allocated, the locum who is expected to work at different locations at short notice runs the risk of not being able to access necessary systems at their place of work and in turn this may compromise patient care.

8.2.3 Access Control Positions

The following Access Control Positions within the National Locum Pharmacy organisation FFFFF have been made available in CIS for use by the RA parenting organisations; organisations must not create any further Access Control Positions in the virtual National Locum Pharmacy organisation FFFFF.

Org Code: National Locum Pharmacy (FFFFF): FOR PHARMACY STAFF ONLY

Position	Job Role / Activities	Notes
Community Locum 'Short Term' Pharmacist	R8003 Health Professional Access Role B0572 Manage Pharmacy Activities B0068 Verify Prescription	Position to be assigned to Pharmacy who require access to all relevant EPS dispensing functionality.
EPS Enabled Pharmacy Technician	R8008 Admin/Clinical Support Access Role B0572 Manage Pharmacy Activities B0401 View Patient Medication	Position to be assigned to Pharmacy Technicians who require access to all relevant EPS dispensing functionality
Community Locum Pharmacy Sponsor	R8008 Admin/Clinical Support Access Role B1300 Approve RA Requests	Position to be assigned to Sponsors to approve users to the Locum Pharmacists and Pharmacy Technicians position. In addition, this position has been *allocated* the "Community Locum (short notice) Pharmacist" position so that anyone in this Sponsor position is able to assign appropriate users into the locum position.
Community Locum Pharmacy Advanced RA Agent	R5090 – Registration Authority Agent B0274 - Perform RA Activities (Advanced)	Position to be assigned to Advanced RA Agents to directly assign users to Locum Pharmacist and Pharmacy Technician positions.

8.2.4 Sponsor Approval

It is the responsibility of the RA Service Providers to decide if locums are sponsored by a Sponsor in the RA Service Provider, Pharmacy or a Pharmacy Area Manager.

Further information on EPS2 is available in the following location:
http://systems.hscic.gov.uk/eps

9 Registration of Students

Undergraduate students undertake a number and range of clinical placements. As a result students require a NHS Smartcard to access Spine enabled applications during these placements.

To be issued a NHS Smartcard, students must verify their identity to the Identity Check Standards at NHS Employers and to the previous inter-governmental standard e-GIF Level 3 in CIS. NHS Smartcards only need to be issued to students who do not already have a NHS Smartcard.

The need to verify students' identities and issue Smartcards could be integrated into a single business process, coordinated between educational establishments and the RA Service Provider. It is advised that the educational establishment and the RA Service Provider together develop a proposal detailing how students can register for a NHS Smartcard and submit the proposal to those responsible for information governance and the Executive Management Team for approval.

There are two possible approaches RA Service Providers may consider adopting to register students which are detailed below:

- **Educational Establishment Delivered Services** - The Executive Management Team at the RA Service Provider identify and appoint a RA Agent, and a Sponsor(s), from the staff within the educational establishment to register students or
- **RA Service Provider provides RA Services to Educational Establishment** - The RA Service Provider provides RA registration services to students via a bureau service or as part of the induction process

9.1 Educational Establishment Delivered Services

In this scenario, the Executive Management Team of the RA Service Provider would agree to appoint and enable access to the HSCIC e-learning to train staff of the educational establishment to the following roles; RA Agent, RA Agent ID Checker role and additionally Sponsors or Local Smartcard Administrators.

The RA Agent ID Checker in the educational establishment will perform the following actions:

- Register the user
- Capture a photograph that is a true likeness of the user
- Upload the photograph and
- Verify the students identity to e-GIF Level 3

Once the registration of a user has been completed in CIS, the following three options are available to the RA Service Provider to issue the NHS Smartcard:

- The RA Service Provider would issue the NHS Smartcard to the Sponsor or the Local Smartcard Administrator within the educational establishment. The Sponsor would store the NHS Smartcards in a secure location. In the presence of the registered user, the Sponsor or the LSA would unlock the Smartcard using the Assisted Unlock Workflow and the user would enter a new Passcode.

- Or the educational establishment has a N3 connection and a Smartcard printer and the Executive Management Team formally approves an RA Agent in the educational establishment to issue Smartcards and assists the user in assigning a Passcode.
- Or the educational establishment does not have an N3 connection and a Smartcard printer and the appointed RA Agent in the educational establishment) issues the Smartcards using the RA Service Providers facilities.

Given that student registration is a high volume, but infrequent activity, the RA Service Provider needs to assure itself that RA staff, Sponsors and LSAs in the educational establishment are proficient in conducting the registration process. RA staff, Sponsors and LSA should review the HSCIC e-learning training materials on a regular basis.

9.2 RA Service Provider provides RA Services to Educational Establishment

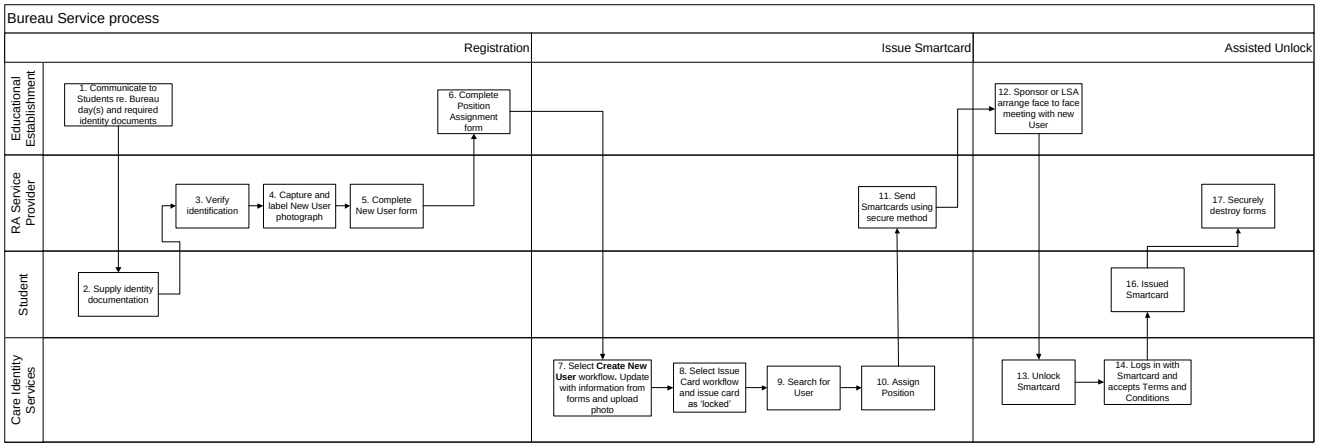
RA Service Providers providing a RA service to the Educational Establishment have at least two further sub options when registering students undertaking placements:

9.2.1 Bureau Service

In this scenario, the first organisation the student undertakes their placement where they need access to Spine enabled system would be responsible for the registration of the student in CIS.

The RA Service Provider would agree to provide to the educational establishment, scheduled bureau day(s) with the relevant educational establishments.

RA Service Provider provides RA Services to Educational Establishment



Notes	Description
1	The educational establishment would be responsible in communicating and ensuring students attend the scheduled bureau day(s) with the appropriate identification documentation as per the Identity Check standards at NHS Employer.
2	Students attend the Bureau day along with their identity documentation.
3	RA staff verify the students and ensure that it is aligned to the Identity Check standards at NHS Employers.
4	RA staff capture a photograph of the student and label it correctly.
5	RA staff complete the CIS – Create New User form with all the appropriate information
6	Sponsor at the educational establishment completes the CIS - Position Assignment

	Modification form with the position assigned to students in educational establishments.
7	RA would then electronically complete the registration and issuance of Smartcards in CIS back at the RA Service Provider organisation. Information from the CIS – Create New User form is uploaded to the **Create New user** workflow in CIS and the photo is uploaded.
8	Once the registration has been granted, RA staff select the **Issue Card** workflow in CIS and print the card 'locked'.
9	RA staff search for the user in CIS.
10	RA staff select the **Assign Position** workflow and ensure that information from the CIS – Position Assignment Modification form is uploaded appropriately including the Sponsors details in the Notes field.
11	RA staff then send the NHS Smartcards using a secure method of transfer to the designated Sponsor or LSA at the educational establishment.
12	Sponsor or LSA arranges a meeting with the Smartcard user.
13	At the meeting, Sponsor or LSA assists the user in unlocking their Smartcard and enables them to set a Passcode.
14	User logs in with their NHS Smartcard and accesses the CIS application, reviews and accepts the Terms and Conditions of Smartcard use.
15	User is issued their Smartcard.
16	RA staff securely store the forms as the information as the information has been entered into the CIS application.

9.2.2 Registration as part of the induction process

In this scenario, the first organisation students could be registered for their NHS Smartcard which may accompany arriving for the placement as part of the induction process. Students would have been notified by their educational institution or individual responsible for placements of the process to issue a NHS Smartcards and documentation they need to produce referring to the Identity Checks standard at NHS Employer Check Standards. At the induction the RA Agent would register the user; ensuring identity is checked to e-GIF Level 3 and issue the NHS Smartcard to the student.

10 Issuing Smartcards via a Bureau Style Model

A bureau style model enables an organisation to manage elements of the Registration process in bulk resulting in organisational efficiencies and potentially reducing costs whilst still adhering to national RA policy.

Registration Authorities must ensure that they adhere to all RA policy aspects when running a bureau service. The main elements of the Registration Process that could be managed in bulk consist of the following but it is imperative that Registration Authorities adhere to the relevant RA policy aspects.

- Creation of identity
  - *Identity must be verified in a face to face meeting. It must be done by examining original documents and seeing that identity relates to the individual who presents themselves at the meeting.*
  - *The person verifying the identity must be trained to do so. In Registration Authority terms this means that individuals holding the roles of RA Managers and RA Agents must perform these checks at face to face meetings*
  - *The documents that can be used to verify an identity have been jointly determined by HSCIC and NHS Employers and the list is contained in the NHS Employers 'Verification of Identity Checks' standard which can currently be found at http://www.nhsemployers.org/case-studies-and-resources/2009/01/verification-of-identity-checks.NO other documents are approved for verification of identity, including those contained within other NHS Employers standards.*
  - *Verification of user's ID to e-GIF level 3 when they register users*

- Printing NHS Smartcards
  - *Smartcards can only be issued to individuals who have a national verified digital identity. This is also the case for processes that are used to issue temporary access to an individual – they need to have a verified identity first.*
  - *Only the end user for whom the Smartcard is intended should know their passcode for their Smartcard, no-one else should, including RA staff. If anyone else knows the end users passcode it breaches the Smartcard terms and conditions of use and the Computer Misuse Act 1990.*
  - *It is mandatory that users sign the Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.*

This permits RAs to register a 'batch' of users face to face and print their NHS Smartcards centrally.

Pre-requisites for using the Bureau Style Model

Pre-requisites are:

- The organisation's RA complies with DH Information Governance standards
- All RA staff of the Bureau team are approved by the Executive Management Team, registered and assigned the appropriate position in CIS and complete the HSCIC e-learning modules on RA policy and CIS.
- A RA Manager or Advanced RA Agent is available to support the model.
- Sponsors are in place to support the model

Operating a Bureau Style Model

To operate a bureau style service, the RA may approach this in various ways. Providing that the identity checking processes are maintained at e-GIF Level 3 standards then the process below in CIS can be adapted appropriately to the local organisation.

- The organisation has delivered the governance framework information and an explanation of the RA process, including support, escalation arrangements, local Sponsor and LSA contacts, helpdesk procedures.
- Sponsors submit a request to register a new user in CIS using the CIS – Request Creation of New User form and complete the CIS –Position Assignment Modification form with the position that should be assigned to the user.
- RA staff arrange a face-to-face meeting with the user and verify the user's identity.
- RA staff complete the CIS – Create New User form with the appropriate information.
- RA Manager or Advanced RA Agent takes a photograph of each applicant, ensuring that each photograph is correctly labelled and associated with the correct request.
- RA staff complete the registration for a new user in CIS including the identification information from the CIS – Create New User form and uploads the user's photo.
- RA Manager or RA Agent creates and prints a NHS Smartcard in a 'Locked' state i.e. no Smartcard Passcode is entered at the time of printing.
- RA Manager or Advanced RA Agent searches for the user in CIS and assigns the user a position as specified by the Sponsor in the CIS – Position Assignment Modification form.
- RA staff send NHS Smartcards using a secure method of transport to the applicant's site.
- At the applicant's site, the RA Manager, RA Agent or Sponsor unlocks the NHS Smartcard to the user, having ensured that the user is the individual whose photograph is on the card.
- The applicant logs into the CIS application.
- The applicant must accept the Terms and Conditions of Smartcard use.

Any unclaimed NHS Smartcards, for example when a user becomes ill and cannot collect their NHS Smartcard, should be stored in a secure lockable environment. If it becomes clear that the NHS Smartcard cannot be issued to the user, the NHS Smartcard should be destroyed using the Destroy Card Process in CIS, and the NHS Smartcard physically destroyed.

11 Integrated Identity Management

Integrated Identity Management (IIM) combines the currently separate processes within Registration Authority and Human Resources for capturing and managing employee identity. If you are using this option you should contact the ESR team for further information on implementing and utilising the interface.

Combining these two parallel activities into a single Integrated Identity Management (IIM) has been proven to deliver the following benefits:

- Improvements in information governance
- Elimination of unnecessary duplication of activities between and within HR and RA functions
- More robust control of accessibility rights
- Organisations using IIM can move organisational boundaries more easily, making restructuring both faster and simpler.

To further support this, there is an interface between ESR and CIS..

The ESR interface to CIS can be used to automatically update an individual's access rights to Spine compliant systems, reflecting the requirements of their new position. It enables the management of access control via a single point of data – the change to the employee's position in ESR, thereby generating further savings for the NHS.

For further information please refer to the ESR website:
http://www.electronicstaffrecord.nhs.uk

11.1 The benefits of the ESR Interface to CIS

The ESR interface to CIS allows organisations to activate a new employee's access to a NHS Smartcard immediately, and to suspend it immediately when they leave. Any changes in employment, such as new starter, job change, and leaver are reflected immediately in ESR, thereby providing the most responsive and efficient method of enabling, modifying or withdrawing access to computer systems linked to the NHS Spine.

The ESR interface to CIS supports better information governance by linking their NHS Smartcard to the NHS employee's staff record in one step.

Using the ESR interface to CIS, organisations can check employee identity and arrange NHS Smartcard access at the same time – using a single IIM approach that avoids dual processing across HR and RA departments.

Coordinating recruitment, HR and RA procedures via the interface will facilitate NHS Smartcard issue during the initial induction period for new staff, enabling them to participate effectively from the start of their employment.

Closer integration of HR and RA activity can lead to savings in the time spent overall in capturing and processing staff information. Once the technical interface is in place, data entry can be reduced to a single event on both ESR and CIS systems.

11.2 Implementing the ESR Interface to CIS

Please e-mail esr.smartcard@nhs.net to request further information regarding the implementation of the ESR interface to CIS and the benefits of it..

Additional resources regarding the ESR interface to CIS is available via the ESR IIM website which can be accessed via the link below:

http://www.electronicstaffrecord.nhs.uk/esr-projects/integrated-identity-management/

12 Appendix A – Centralised Organisation Case Study

Overview

Synopsis
Trust provides a RA Service to its organisation. The local Executive Management Team has approved two users to the RA Manager position. RA Manager will set up the Registration Authority, identify and update local RA processes and users to the six CIS RA roles.

Setting
Trust currently provides a RA service to its own organisation over two sites.

Business Situation
Trust will need to find an effective RA model to not only issue NHS Smartcards but to provide ongoing support to existing users.

Solution
Trust will implement Care Identity Service (CIS) application benefitting from the flexibility of using an electronic system to manage the issuing of NHS Smartcards and updating Access Profiles. To establish a highly efficient model at the Trust, the RA Manager will provide training to support certain responsibilities devolved to the Advanced RA Agent, RA Agent ID Checker, Sponsor and Local Smartcard Administrators.

Benefits
Trust is seeking to benefit from the flexibility in using CIS ensuring business continuity, minimising impact to patient care whilst still maintaining a high level of governance.

Trust is seeking to ensure users a quick turnaround to receive their NHS Smartcards minimising delays to patient care.

Background
The Trust is a centralised organisation operating on two sites. The local Executive Management Team has identified two users to the RA Manager position at the Trust. The responsibilities of the RA Manager will include setting up a Registration Authority that is efficient, effective, responsive and flexible, whilst adhering to National RA Policy, Public Key Infrastructure (PKI) requirements, local resource constraints and local budget constraints.

The Trust has been made aware of the benefits of the electronic system Care Identity Service (CIS) application including the six RA roles to issue NHS Smartcards and update users' access profiles.

The Business Need
The implementation of CIS at the Trust is intended to make an efficient front line service delivery and ensure governance and National RA policy requirements are still met.

CIS will be required to issue NHS Smartcards, update user's access profiles, provide RA management tools and rationalise RA roles while providing better, faster and simpler workflows. Further requirements will include:

- Assess access requirements to be used for Position Based Access Control (PBAC)
- Assess Workgroup structure setup
- Ensure new employees at the Trust have fast turnarounds to receive a new NHS Smartcard from RA so that they can start working as quickly as possible
- Assign employees with existing NHS Smartcards the appropriate Access Control Position without delay to ensure a high level of patient care
- Remove Access Control Position's from users profiles as soon as staff leave employment at the Trust
- Comply with National RA Policy and PKI requirements
- Ensure users identity is verified by the appropriate RA staff, aligned with Identity Checks at NHS Employment Check Standards, and the previous inter-governmental standard e-GIF Level 3 standards (authentication) requirements
- Assign staff in the Trust with the appropriate permissions to support assisted unlock NHS Smartcards and assisted renewal of certificates
- Reporting on both RA roles and NHS Smartcard users
- Create digital identities as a single process
- Train the six CIS RA roles

The Solution	
The Trust will set priorities and create a roadmap of tasks and activities in preparation for the new CIS application including approval from EMT on the organisations Access Control positions, identifying users to the RA roles and establishing local processes. On implementation of the CIS application, the following steps will be undertaken to set up the central Registration Authority team and to delegate other RA related roles and responsibilities throughout the organisation.	
Registration Authority Setup - 1	
RA Manager at the Trust will setup the RA service and create Access Control Positions in a single process including the RA positions.	
Registration Authority Setup - 2	
	The RA Manager will identify a further two users to the Advanced RA Agent position in CIS. This will enable the RA Manager to devolve the following responsibilities; Create digital identities (either from requests raised in CIS or local processes), Batch functions, Direct position assignment, Workgroup setup, Workgroup membership assignment and Reporting.
Registration Authority Setup - 3	
In addition to the Advanced RA Agents, the RA Manager will assign a further two users to the RA Agent position to assist in the centralised function of printing and issuing of NHS Smartcards. Furthermore as the Trust use the ESR Interface, HR staff will be assigned the RA Agent ID Checker position to enable them to complete the registration of new users in the CIS application including uploading the user's photo at the same time as they perform the identification checks prior to employment. Using the ESR Interface enables the Trust to ensure a high level of governance and highly efficient adherence to the local leavers and joiners' policy. In addition users will only be assigned the access they need for the period of time that they are employed.	

Registration Authority Setup – Local RA related roles & responsibilities	
	RA Manager will also identify additional users to the Sponsor position to raise requests (2 per division) and support the assisted unlock and assisted renewal of certificates processes in CIS. Also a number of LSAs will be identified to support the assisted unlock and assisted renewal of certificates.
Summary of the RA Service at the Trust	
The above steps will contribute to an efficient RA service that will meet the demands of its users within short time frames. The central team will consist of the RA Managers, Advanced RA Agent, RA Agent and the RA Agent ID Checkers. Locally there are will be a number of Sponsors and LSAs.	

The Trust will meet the demands of a RA service within short time frames by having local RA related roles where Sponsors will raise a request for an existing user to be assigned an Access Control Position in CIS and LSAs will perform the assisted unlock and the assisted renewal of certificates. Upon receiving a request from the Sponsors to assign a position to a user, RA Agents in the central team will be able to grant the request thereby updating the user's access profile. The benefits of this model are expected to be huge and will ensure any loss of service is minimised in the Trust and will reduce time wasted for the user having to liaise with local RA related staff to have their Smartcards unlocked or the certificates renewed.

However a great deal of training will be implemented to ensure that not only are mistakes minimised but that the RA Manager will also fulfil their responsibility to provide suitable training to RA agents and Sponsors as per National RA Policy. RA Managers at the Trust will ensure that users assigned to the RA roles complete the HSCIC e-learning material on RA Policy and RA Processes and will be regularly reviewed.

Challenges

Adopting this approach should minimise the challenges of transition. The only major challenges foreseen will be allocating time to all users assigned RA roles to complete the HSCIC RA e-learning and advising existing NHS Smartcard users on the updated local RA Processes. The impact of the Trust not implementing the RA model above is likely to include recruiting additional centralised RA staff and compromising on the delivery of the RA service to manage existing and new NHS Smartcard users.

Conclusion

The Trust is hoping to achieve the RA service model above to reduce the day to day burden on the central RA team. NHS Smartcard users at the Trust will have the option to liaise with Sponsors and Local Smartcard Administrators or with the central team as appropriate.

13 Appendix B – De-centralised Organisation Case Study

Overview

Synopsis
CSU commissioned by the Area Team to provide a RA Service to its child organisations that include GP Practices, Community, Pharmacies and the Independent Sector. The local Executive Management Team has approved two users to the RA Manager position. RA Managers will set up the Registration Authority, update local RA processes and users to the six CIS RA roles.

Setting
CSU is located on three sites and is the RA Service Provider to over 40 GP Practices, 20 Pharmacies and a small number of Community Providers and organisations in the independent sector within a 50 mile radius.

Business Situation
CSU needs to find an effective RA model to not only issue NHS Smartcards but to provide ongoing support to existing users.

Solution
CSU will implement the Care Identity Service (CIS) application to benefit from the flexibility of using an electronic system to manage the issuance of NHS Smartcards and updates to Access Profiles. To establish a highly efficient model at the CSU, the RA Manager will devolve certain responsibilities to the Advanced RA Agents at the CSU. In addition users will be identified in the child organisations of the RA hierarchy to be assigned the RA Agent ID Checker, Sponsor and Local Smartcard Administrator roles to support the RA service.

Benefits
CSU expects to benefit from the flexibility in using CIS to ensure business continuity, minimise impact to patient care whilst still maintaining a high level of

Background
The CSU is a de-centralised organisation operating across three sites. The CSU has also been commissioned by the Area Team to provide RA services to GP Practices, Pharmacies, Community Providers and the Independent Sector over a 50 mile radius. The organisation's Executive Management Team has identified two users to the RA Manager position at the CSU. The responsibilities of the RA Manager include setting up a Registration Authority that is efficient, effective, responsive and flexible, whilst adhering to National RA Policy, Public Key Infrastructure (PKI) requirements, local resource constraints and local budget constraints.

The CSU has been made aware of the benefits of the electronic system Care Identity Service (CIS) application including the six RA roles to issue NHS Smartcards and update users' access profiles.

The Business Need
The implementation of CIS at the CSU is intended to make an efficient front line service delivery and ensure governance and National RA policy requirements are still met.

CIS will be required to issue NHS Smartcards, update user's access profiles, provide RA management tools and rationalise RA roles while providing better, faster and simpler workflows. Further requirements will include:

- Assessing access requirements to be used for Position Based Access Control (PBAC)
- Assessing Workgroup structure setup
- Ensuring new employees at the CSU and the child organisations have fast turnarounds to receive a new NHS Smartcard from the central RA team so that they can start working as quickly as possible
- Assigning employees with existing NHS Smartcards the appropriate Access Control Position without delay to ensure a high level of patient care
- Removing Access Control Position's from users profiles as soon as staff leave employment at the CSU and at the child organisations
- Complying with National RA Policy, Identity Checks at NHS Employment Check Standards, PKI requirements and the previous inter-governmental standard e-GIF Level 3 (authentication) requirements to assure the identity of the individual applying for registration and

governance. CSU will ensure new users a quick turnaround to receive their NHS Smartcards minimising delays to patient care. At the same time, new users will be registered in CIS locally and existing NHS Smartcard users will be able to liaise with local RA related roles in the event Smartcards need unlocking or the certificates need renewing.	access. • Assigning staff at the CSU and the child organisations with the appropriate permissions to action assisted unlock NHS Smartcards and assisted renew certificates • Reporting on both RA roles and NHS Smartcard users • Create digital identities as a single process • Train the six CIS RA roles
The Solution The CSU will set priorities and create a roadmap of tasks and activities in preparation for the new CIS application including EMT approval at the Trust and Information Governance approval from each of the child organisations on the organisations Access Control positions, identifying users to the RA roles and establishing local RA processes. On implementation of the CIS application, the following steps will be undertaken to set up the central Registration Authority team and to delegate local RA related roles and responsibilities throughout the RA hierarchy.	
Registration Authority Setup - 1	
RA Manager at the CSU will setup the RA service and create Access Control Positions in a single process including the RA positions.	
Registration Authority Setup - 2	
	The RA Manager will identify a further six users to the Advanced RA Agent position in CIS at each of the CSU sites to maintain business continuity in the event of absence, leave or sickness. Having Advanced RA Agents will enable the RA Manager to devolve the following responsibilities; Create digital identities (either from requests raised in CIS or local processes), Batch functions, Direct position assignment, Workgroup setup, Workgroup membership assignment and Reporting. In addition the Advanced RA Agents will be responsible to print and dispatch NHS Smartcards to users at the site and to child organisations.

Registration Authority Setup – Local RA related roles & responsibilities	
RA Manager will identify local users to the Sponsor position to raise requests (2 per organisation) and support the assisted unlock card and the assisted renewal of certificates processes. In addition Sponsors will also be able to manage users using the Assignable positions process. RA Agent ID Checker roles will be identified within the child organisations to check identification and renew expired certificates and repair certificates. Also a number of Local Smartcard Administrators will support assisted unlock card and assisted renew al of certificates.	
Summary of the RA Service at the CSU	
	This RA model is expected to contribute to an efficient RA service that is expected to meet the demands of its users within short time frames. The central team will consist of the RA Managers and Advanced RA Agent. Locally there will be a number of RA Agents ID Checkers to verify users' identification, Sponsors will be able to assign users using the Assignable positions process and LSAs will assist in the unlocking of Smartcards and renewal of certificates.

The combination of the CIS application and the highly flexible approach (establishing hubs at the child organisations for ID checking and assigning Access Control Positions) is an attractive RA service model to the CSU. The RA Service model will contribute to an efficient RA service that will be able to meet the demands of its users within short time frames.

CSU will implement the following processes in the child organisations prior to rolling out CIS:

- Develop a standardised template of Access Control Positions for PBAC suitable for staff depending on the child organisation type
- Modify Access Control Positions as per local requirements in each of the child organisation types where the Information Governance Lead (usually senior managers) will confirm that they were appropriate
- Advanced RA Agents in the CSU will create the Access Control Positions in CIS as a single step process
- Create the RA Agent ID Checker Access Control Position for each child organisation allocating both the business function code B0267 and the sponsorship business function B1300 to that position
- Set up the local Access Control Positions in the child organisation as 'Assignable Positions'. By implementing 'Assignable Positions' the Sponsor will directly assign or remove a position from a user's Access Profile
- Assign a minimum two people to the RA Agent ID Checker Access Control Position in

each child organisation generally two organisational Managers to cover leave and absence
- Create the Local Smartcard Administrator Access Control Position for each child organisation to support the assisted unlock card and assisted renewal of certificates

The CSU will meet the demands of a RA service within short time frames by implementing the Assignable Positions process. This is where users who will be assigned the sponsorship role will also be able to directly assign users to a pre-approved position in CIS. At the same time when users leave employment within child organisations, Sponsors will be able to un-assign user's Access Control Positions immediately, ensuring a high level of governance and highly efficient adherence to the local leavers and joiners' policy. The benefits of this model are expected to be huge and will ensure minimal loss of service in the child organisation and reduction in time wasted for the user travelling between large geographical distances to be assigned the relevant Access Control Positions.

In addition, as the local HR staff in the child organisations already perform the identification checks for users prior to employment; it makes sense that they continue this process in registering new users on CIS. By appointing staff who are already responsible in appointing new staff, they will be authorised to perform the verification of identity checks as per *NHS Employment Check Standards*. HR staff who are already involved in the recruitment of staff in child organisations will be best placed to know what access their staff require.

CSU will implement the following process to register new users thereby will eliminate the need for new users having to travel large geographical distances and will ensure that there is a fast turnaround in issuing NHS Smartcards. They will aim to send out the printed NHS Smartcard within 24 hours from the time of receiving the request in the Request List in the CIS, as per the process below:

- RA Agent ID Checkers in the child organisations will perform the identification checks as per Identity Checks at NHS Employment Check Standards and will input the identification information in CIS as a single process. The printing function will be centralised at the CSU sites which will only be accessible to the central Registration Authority team.
- Once a user has been registered, the Sponsor will be able to assign a user to an Assignable Position and set the start date accordingly.
- The request to print the NHS Smartcard will then be sent to the child organisation request list which will picked up by the central Registration Authority team who will have access to those request lists. Printers will not physically be located in child organisations and they will not therefore produce 'live' Smartcards.
- The central RA team will implement an assurance check process before printing the NHS Smartcard. This will include a standard check to make sure that information has been entered correctly into CIS and confirm that the identification has been verified by the RA Agent ID Checker in the child organisation.
- The NHS Smartcard will be printed and will be 'locked' (requiring the new user to input their new passcode when they receive it).
- The NHS Smartcard will then be sent out on the same day to identified Sponsors at the child organisation using a secure method of delivery, with instructions on how to unlock. The Sponsor will only release the NHS Smartcard to the new user during the face to face meeting.
- At the face to face meeting with the new user, the Sponsor will action the assisted unlock card process in CIS which will require the new user to input a new passcode.
- The new user will log in with their NHS Smartcard to access the Spine to review and

accept the Terms and Conditions of Smartcard use.

The above process will minimise the need for RA staff based in the CSU to make site visits to child organisations reducing the time to issue NHS Smartcards and overall organisational costs. NHS Smartcards will be printed at the CSU as a centralised function by a small number of experienced Advanced RA Agents benefitting from increased efficiency and economies of scale.

RA Managers at the CSU will ensure that users assigned the RA roles complete the HSCIC e-learning material on RA Policy and RA Processes.

Challenges
Challenges are expected to be minimal. The only challenges foreseen include ensuring all users assigned RA roles complete the HSCIC RA e-learning, implementing local RA processes and advising existing NHS Smartcard users on the local RA Processes.

It is expected that if the CSU does not implement the RA model above, the impact will consist of recruiting additional centralised RA staff and compromising on the delivery of the RA service to manage existing and new NHS Smartcard users.

Conclusion
The CSU expects to achieve the RA service model and reduce the day to day burden on the central RA team. The following RA processes are expected to greatly reduce the day to day burden on the central RA team and minimise overall organisational costs:

- Implement ‘Assignable Positions’
- Localise the identification check function by appointing RA Agent ID Checkers in child organisations
- Centralise the bureau printing function of NHS Smartcards at the CSU

The strength of CIS is expected to enable RA Service Providers to offer powerful services to organisations despite large geographical areas as Area teams continue to commission RA services to RA Service Providers.

14 Appendix C – Centralised and De-centralised Organisation Case Study

Overview

Synopsis
Trust provides a RA Service to its organisation and child organisations that include GP Practices, Community Providers, Pharmacies and Independent Sector organisations. The local Executive Management Team has approved two users to the RA Manager position. RA Managers will set up the Registration Authority, identify local RA processes and users to the six CIS RA roles.

Setting
Trust provides a RA service to its own organisation. In addition the Trust is the RA Service Provider to over 30 GP Practices, 10 Pharmacies and a small number of Community Providers and organisations in the independent sector within a 30 mile radius.

Business Situation
Trust needs to find an effective RA model to not only issue NHS Smartcards but to provide ongoing support to existing users.

Solution
Trust will implement Care Identity Service (CIS) application benefitting from the flexibility of using an electronic system to manage the issuing of NHS Smartcards and updating Access Profiles. To establish a highly efficient model at the Trust, the RA Manager will devolve certain responsibilities to the Advanced RA Agents, RA Agents, RA Agent ID Checkers, Sponsors and Local Smartcard Administrators (LSA). Additional users will be identified in the child organisations of the RA hierarchy to be assigned the RA Agent ID Checker, Sponsor and Local Smartcard Administrator roles to support the RA service locally.

Benefits
Trust will benefit from the flexibility in using CIS ensuring business continuity, minimising impact to patient care whilst still maintaining a high level of governance.

Background

The Trust provides a RA service to its own organisation and child organisations consisting of GP Practices, Pharmacies, Community Providers and the Independent Sector over a 30 mile radius. The organisation's Executive Management Team (EMT) has identified two users to the RA Manager position at the Trust. The responsibilities of the RA Manager include setting up a Registration Authority that is efficient, effective, responsive and flexible, whilst adhering to National RA Policy, Public Key Infrastructure (PKI) requirements, local resource constraints and local budget constraints.

The Trust has been made aware of the benefits of the electronic system Care Identity Service (CIS) application including the six RA roles to issue NHS Smartcards and update users' access profiles.

The Business Need

The implementation of CIS at the Trust will be intended to make an efficient front line service delivery and ensure governance and National RA policy requirements are still met.

CIS will be required to issue NHS Smartcards, update user's access profiles, provide RA management tools and rationalise RA roles while providing better, faster and simpler workflows. Further requirements include:

- Assessing access requirements to be used for Position Based Access Control (PBAC)
- Assessing Workgroup structure setup
- Ensuring new employees at the Trust and the child organisations have fast turnarounds to receive a new NHS Smartcard from the central RA team so that they can start working as quickly as possible
- Assigning employees with existing NHS Smartcards the appropriate Access Control Position without delay to ensure a high level of patient care
- Removing Access Control Position's from users profiles as soon as staff leave employment at the Trust and at the child organisations
- Complying with National RA Policy, *Identity Checks* at *NHS Employment Check Standards*, PKI requirements and the previous inter-governmental standard e-GIF Level 3 (authentication) requirements to assure the

Trust will ensure new users a fast turnaround to receive their NHS Smartcards minimising delays to patient care. At the same time, new users will be registered in CIS locally and existing NHS Smartcard users will be able to liaise with local RA related roles in the event Smartcards need unlocking or the certificates need renewing.	identity of the individual applying for registration and access • Assigning staff at the Trust and the child organisations with the appropriate permissions to action assisted unlock NHS Smartcards and assisted renew certificates • Reporting on both the RA roles and NHS Smartcard users • Create digital identities as a single process • Train the six CIS RA roles

The Solution

The Trust will set priorities and will create a roadmap of tasks and activities in preparation for the new CIS application including EMT approval from the Trust and Information Governance approval from each of the child organisations on the Access Control Positions, identifying users to the RA roles and establishing local RA processes.

On implementation of the CIS application, the following steps will be undertaken to set up the central Registration Authority team and to delegate local RA related roles and responsibilities throughout the RA hierarchy.

Registration Authority Setup – 1	
RA Manager at the Trust will setup the RA service and create Access Control Positions in a single process including the RA positions.	

Registration Authority Setup – 2

	The RA Manager will identify a further two users to the Advanced RA Agent position in CIS at each of the Trust sites to maintain business continuity in the event of absence, leave or sickness. Having Advanced RA Agents will enable the RA Manager to devolve the following responsibilities; Create digital identities (either from requests raised in CIS or local processes), Batch functions, Direct position assignment, Workgroup setup, Workgroup membership assignment and Reporting. RA Agents will be responsible in printing and dispatching NHS Smartcards to users at the site and to child organisations. As the Trust uses the ESR Interface, HR staff will be assigned the RA Agent ID Checker position to enable them to complete the registration of new users in the CIS application including uploading the user's photo at the same time as they perform the identification checks prior to employment. Using the ESR Interface will enable the Trust to ensure a high level of governance and highly efficient adherence to the local leavers and joiners' policy. In addition users will only have the access they need for the period of time that they are employed.
Registration Authority Setup – Local RA related roles & responsibilities	
RA Manager will identify local users to the Sponsor position to raise requests (2 per organisation), assist in unlocking users NHS Smartcards cards and assist in renewing certificates. In addition Sponsors will also be able to manage users using the Assignable Positions process. RA Agent ID Checker roles will also be identified within the child organisations to check identification and renew expired certificates and repair certificates. Also a number of Local Smartcard Administrators will be identified to support the assisted unlock card and assisted renewal of certificates	

processes.	
Summary of the RA Service at the Trust	
	This RA Service model will contribute to an efficient RA service that will be able to consistently meet the demands of its users within a short time frame. The RA central team will consist of RA Managers, Advanced RA Agents, RA Agents and RA Agent ID Checkers. Locally there will be a number of RA Agent ID Checkers to verify users' identification and Sponsors will be set up to assign users to Assignable positons and LSAs.

The combination of the CIS application and the highly flexible approach (establishing hubs at the child organisations for ID checking and assigning Access Control Positions) is attractive to the Trust. The RA Service model will contribute to an efficient RA service that will be able to consistently meet the demands of its users within short time frames.

Trust will implement the following processes in the child organisations prior to rolling out CIS:

- Develop a standardised template of Access Control Positions for PBAC suitable for staff depending on the child organisation type
- Modify them as per local requirements in each of the child organisation types where the Information Governance Lead (usually senior managers) will confirm that they are appropriate
- Advanced RA Agents in the Trust create the Access Control Positions in CIS as a single step process for the child organisations
- Create the RA Agent ID Checker Access Control Position for each child organisation allocating both the business function code B0267 and the sponsorship business function B1300 to that position
- Set up the local Access Control Positions in the child organisation as 'Assignable Positions'. By implementing 'Assignable Positions' the Sponsor directly assigns or removes a position from a user's Access Profile
- Assign a minimum two people to the RA Agent ID Checker Access Control Position in each child organisation generally two Managers to cover leave and absence
- Create the Local Smartcard Administrator Access Control Position for each child organisation to support the assisted unlock card and assisted renewal of certificates

Trust will be expected to meet the demands of an RA service within short time frames by adopting the model 'Assignable Positions'. This is where users who will be assigned the sponsorship role are able to directly assign existing NHS Smartcard users to a pre-approved directly assignable Access Control Position in CIS as soon as required. At the same time when users leave employment within child organisations, Sponsors will be able to remove user's Access Control Positions immediately, ensuring a high level of governance and highly efficient adherence to the local leavers and joiners' policy. The benefits of this model are expected to be huge and will ensure any loss of service is minimised in the child organisation and reduction in time wasted for the user travelling between large geographical distances to

be assigned the relevant Access Control Positions.

In addition, as there are already staff in the child organisations that already perform the identification checks for users prior to employment; it makes sense that they continue this process in registering new users on CIS. By appointing staff who are already responsible in appointing new staff, they are authorised to verify users identification. HR staff who are already involved in the recruitment of staff in child organisations are also best placed to know what access their staff require.

Trust will implement the following process to register new users thereby eliminating the need for new users having to travel large geographical distances and ensuring that there is a fast turnaround in issuing NHS Smartcards. They will aim to send out the printed NHS Smartcard within 24 hours from the time of receiving the request in the Request List in the CIS, as per the process below:

- RA Agent ID Checkers in the child organisations will perform the identification checks and will input the identification information in CIS as a single process. The printing function is centralised at the Trust sites which will only be accessible to the central Registration Authority team.
- Once a user has been registered, the Sponsor will be able to assign a user to an Assignable Position and set the start date accordingly.
- The request to print the NHS Smartcard will then be sent to the child organisation Request List which will be picked up by the central Registration Authority team who have access to those request lists. Printers will not be physically located in the GP Practices and they cannot therefore produce 'live' Smartcards.
- The central RA team will implement an assurance check process before printing the NHS Smartcard. This includes a standard check to make sure that information has been entered correctly into CIS and confirm that the identification has been verified by the RA Agent ID Checker in the child organisation.
- The NHS Smartcard will be printed and 'locked' (requiring the new user to input their new passcode when they receive it).
- The NHS Smartcard will then be sent out on the same day to identified Sponsors at the child organisation using a secure method of delivery, with instructions on how to unlock. The Sponsor only releases the NHS Smartcard to the new user during the face to face meeting.
- At the face to face meeting with the new user, the Sponsor will action the assisted unlock card process in CIS requiring the new user to input a new passcode.
- The new user will log in with their NHS Smartcard to access the Spine to review and accept the Terms and Conditions of Smartcard use.

The above process will minimise the need for RA staff based in the Trust to make site visits to child organisations reducing the time to issue NHS Smartcards and reducing overall organisational costs. NHS Smartcards will be printed at the Trust as a centralised function by a small number of experienced Advanced RA Agents benefitting from increased efficiency and economies of scale.

RA Managers at the Trust will ensure that users assigned to the RA roles complete the HSCIC e-learning material on RA Policy and RA Processes,

Challenges

Adopting this approach should minimise the challenges of implementation. The only major challenge foreseen are ensuring all users assigned RA roles complete the HSCIC RA e-

learning, implement local RA processes and advise existing NHS Smartcard users on the local RA Processes. If the Trust does not implement the RA model above, the impact will be a need to recruit additional centralised RA staff and compromise on the delivery of the RA service to manage existing and new NHS Smartcard users.

Conclusion

The Trust will achieve the RA service model they are seeking to reduce the day to day burden on the central RA team. The following RA processes will greatly reduced the day to day burden on the central RA team and minimise overall organisational costs:

- Implement ‘Assignable Positions’
- Localise the identification check function by appointing RA Agent ID Checkers in child organisations
- Centralise the bureau printing function of NHS Smartcards at the Trust

The strength of CIS will enable RA Service Providers to offer effective RA services to organisations despite large geographical areas.