Humber Teaching
NHS Foundation Trust

STANDARD OPERATING PROCEDURE
REGISTRATION AUTHORITY

Document Reference	SOP19-010
Version Number	1.1
Author/Lead **Job Title**	Sarah Fearnley - RA Officer Julie Crockett – RA Manager
Instigated by: **Date Instigated:**	
Date Last Reviewed:	24 May 2023
Date of Next Review:	May 2026
Consultation:	IG Group RA Managers Digital Delivery Group
Ratified and Quality Checked by: **Date Ratified:**	Information Governance Group 24/05/23
Name of Trust Strategy / Policy / Guidelines this SOP refers to:	Registration Authority Policy

VALIDITY – All local SOPS should be accessed via the Trust intranet

CHANGE RECORD

Version	Date	Change details
1.0	*April 2019*	*New SOP*
1.1	*July 2022*	*Review and Minor Amendments. Approved at Information Governance Group (24 May 2023).*

Contents

1. INTRODUCTION

The purpose of this document is to provide guidance to individuals working at Humber Teaching Hospitals NHS Foundation Trust on using smartcards including the national obligations, roles and responsibilities of the Registration Authority (RA) and the Registration process to issue and update NHS Smartcards to Users. This document should be read in conjunction with the RA policy which can be found on the Trust's Intranet.

The RA will ensure that all aspects of Registration Authority services and operations are performed in accordance with the Registration Authorities Process Guidance (NPFIT-SI-SIGOV-0114.10) published on the 1 May 2013, together with supporting, related guidance and the Trust's local RA policy.

This document provides the standard operating procedures for the use of smartcards and access to systems which require them, these are:

Care Identity Services (CIS) standalone.
ESR
SystmOne1 (S1)
Lorenzo
Summary Care Records (SCR)
Data Landing Portal

2. SCOPE

This document is applicable to all individuals who utilise a smartcard in order to access NHS CRS compliant applications.

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

3. DUTIES AND RESPONSBILITIES

Chief Executive
Overall accountability for Registration Authority (RA) processes lies with the chief executive who has overall responsibility for establishing and maintaining effective and safe systems to manage and support access to electronic record systems through the use of Smart Cards.

The responsibility for the processes within the Trust is delegated to the following individuals:

Director of Finance
As the Senior Information Risk Owner (SIRO) is also responsible for and accountable to the Trust Board for any information risks identified in relation to this and other Information Governance policies and procedures. The director of finance also has delegated responsibility for managing the development and implementation of information management and governance policies and chairs the information governance committee.

The executive medical director and responsible officer as the **Director of Nursing** acts as the conscience of the organisation in relation to the use and protection of all health and social care records.

Registration Authority Manager
The senior Informatics Managers are the Trust's **Registration Authority Manager** and is the designated lead for the Registration Authority process. The RA manager has accountability for developing the Policy and maintaining the processes. The RA manager also provides strategic leadership and direction to the Trust's RA Team.

Registration Authority Officer
Registration Authority Officer is responsible to the RA Manager for ensuring that the National and local processes are followed and for the accurate input of information on RA forms onto the Care Identity Service (CIS). In addition to the RA Manager, as a contingency, the RA Officer is assigned RA Manager Access within the system. The RA Officer is the Information Asset Owner (IAO) in relation to all aspects of the Registration Authority.

Registration Authority Agents
Registration Authority Agents are responsible to the RA Manager for ensuring that the National and local processes are followed and for the accurate input of information on RA forms onto the Care Identity Service (CIS). The Trust's four nominated members of the HR Recruitment Bureau are the Trust's RA Agents, and together with the RA Manager and RA Officer form the Trust RA Team.

Registration Authority Sponsors
Sponsors are appointed and entrusted to act on behalf of the Trust in determining who should have what access and maintaining the appropriateness of that access.

To support the day to day running of the RA Service and to carry out the RA responsibilities outlined in 4.1, the Trust's RA Manager, RA Officer and RA Agents have also been assigned the role of RA Sponsor. There are different levels of Registration Sponsors.

Traditionally the role of RA Sponsor would have been assigned to a number of managers within services who could authorise and sponsor the setting up of new users, authorise changes to job roles, access rights and terminations. Now we are using the CIS, which is only accessed by staff working within the Trust's Registration Authority, it has been agreed with the Information Governance Committee that all line managers will effectively act as RA Sponsors and will provide the necessary authorisation either via email or via the agreed forms, i.e. new starter, change, termination forms to enable new users to be set up on the system, or to inform RA of any changes, suspensions or terminations. Mentors/Educators will act as RA Sponsors in respect of students they are mentoring and providing the necessary request and authorisation for students in their charge to be issued with a smartcard where these are required.

The role of **Local Smartcard Administrator** has been allocated to a number of staff out in the various work bases. The through the specifically assigned activity B0263 the Local Smartcard Administrators are able to:

- Unlock smartcards and reset passcodes
- Renew a users' smartcard certificate up to 90 days before they are due to expire.

Applicant (Healthcare professionals/workers requiring smartcards)
The applicant for a smartcard is responsible for the safe use and storage of their smartcard. The card should be treated with care and protected to prevent loss, damage

or theft. **It is also the user's responsibility to ensure that no other person uses or has access to their smartcard, account or passcode.** In addition, users should not leave their smartcards in the smartcard readers if they are away from their workstation/computer.

The applicant is also responsible for immediately notifying the Trust's RA Officer if they lose their smartcard or if they suspect this has been stolen. This will be classed as a Serious Incident. **For details of how to manage a lost or stolen smartcard see section 5.11**

The applicant is also responsible for notifying the Trust's IT Service Desk if they have any problems/issues with their smartcards.

IT Operations Manager and IT Service Desk
The IT Operations Manager is responsible for ensuring that there is sufficient computer equipment to support all users of CRS applications (including those for registration).

Any failure or unavailability in NHS CRS compliant applications are reported to the IT Service Desk in the first instance. The IT Service Desk is responsible for logging the incident with the National Service Desk, where applicable.

The IT Service Desk will forward any RA related problems/issues to the Clinical Systems Team, via their call handling system ServiceDesk Plus, where these will be picked up and dealt with by either the Trust's RA Officer or another member of the Clinical Systems Team.

Trust RA Staff Responsibilities

- 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.
- Ensure they are adequately trained and familiar with the local and national RA policies and processes.
- Be familiar with and adhere to RA Process Guidance and "*Registration Authorities:*
- *Governance Arrangements for NHS Organisations".*
- Complete the relevant e-Learning modules available via the Health and Social Care Information Centre (HSCIC) CIS Training Site or the Oracle Learning Management (OLM) system in Electronic Staff Record (ESR).
- Complete the required Information Governance training.
- Complete any local training requirements.
- Report all RA related security incidents and breaches to the organisation's Risk Management Team in line with the Trust's Risk Management Strategy and Adverse Incident and Serious Untoward Incident Procedures as outlined later in this document.
- Ensure there is a sufficient supply of NHS Smartcards and RA hardware, including access to the CIS for Local Smartcard Administrators (Smartcard unlocking and certificate renewal), and communicate technical requirements to the IT Operations Manager/IT Service Desk.
- Produce NHS Smartcards, renew NHS Smartcard certificates and unlock NHS Smartcards for anyone at the same level or lower within the RA hierarchy.
- Ensure Users have only one NHS Smartcard issued to them showing their UUID and photograph, and that Users are aware of their responsibilities relating to Information Governance and NHS Smartcard Terms and Conditions. The issue of more than one NHS Smartcard to a User is not permitted. (Temporary Access Smartcards are not NHS Smartcards in this context
- Associate the ESR record with the NHS Smartcard UUID. To allow ESR to manage person details, and where possible NHS CRS Access, staff need to have their

Smartcard UUID associated to their ESR record. Association can only be completed once the applicant has been hired by the Trust.

- Ensure Users are aware of the self-service functionality available to them, including how to Change Passcodes, update profiles and renew Smartcard certificates.
- Ensure that they are aware of the appropriate identification documentation guidelines at NHS Employers as per National Policy. The NHS Employment Check Standards are mandatory for 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. When appointing locums and agency staff we will need to ensure that their providers comply with these standards. Failure to comply with these standards could potentially put the safety, and even the lives, of patients, staff and the public at risk.

  http://www.nhsemployers.org/Aboutus/Publications/Documents/Verification%20of%20ide ntity%20checks.pdf

- Record the outcome of the checks using ESR, confirming that identity has been verified in accordance with these standards.
- Approve User registrations upon completion of the User's Identity Checks in line with the above, and the Trust's Recruitment and Selection Policy and Procedures.
- Be familiar with the different types of Access Control Positions to approve. Ensure that the appropriate position outlining a user's access rights are added in the CIS to a User's smartcard in line with their job role within the Trust, or to enable them to carry out the services they have been contracted to provide. Registration Authorities cannot directly add access profiles for users who are not part of an organisation they are responsible for.
- Ensure, before adding an access profile to a user's smartcard that they have completed the necessary systems training.
- Grant the creation and modification of the Access Control Position once they have been approved.
- Perform CIS requests (which are in the baseline for all RA Personnel).
- Renew a User's Smartcard certificates if confident of the User's identity.
- Unlock a User's Smartcard and reset logon Passcodes.
- Maintain access to NHS CRS compliant applications within their area of responsibility that is consistent with the *"NHS Confidentiality Code of Practice"*. This includes Access Control Position assignment and removal, and the revocation of NHS Smartcards and NHS Smartcard certificates.
- Submit a request relating to a change in their own access rights but **not** approve.
- An RA manager or RA agent can only close a person entry in an organisation outside of their administrative control if there are no open roles associated with that entry. If there are roles open, then attempting to close the person entry will close all entries belonging to the RA's organisations but leave open the entries associated with open roles belonging to organisations outside of the RA's control.
- Implement the process identified by the RA Manager for enabling locum, agency, and bank staff access to NHS CRS compliant applications.
- Ensure that you are updated regularly on RA topics by requesting your email address to be added to the RA distribution list *ramanagers.agents@hscic.gov.uk*. (RA Managers and RA Officer only)
- Join the RA Community Site on NHS Networks to share knowledge and gain useful information as recommended by the NHS Connecting for Health *http://www.networks.nhs.uk/nhs-networks/registration-authority-community*.
- Ensure your (RA Agent) contact details including email address and telephone numbers are recorded in the Spine User Directory.
- Adhere to the Audit policy and ensure that all RA forms and associated information is maintained and securely stored according to national policy.

- Adopt and maintain the Terms and Conditions.
- All RA queries / issues to be reported via the IT Servicedesk, logged in ServiceDesk Plus and assigned to the RA Category where these will be dealt with by the RA Officer.
- HR RA to respond and deal with RA calls logged in ServiceDesk Plus in line with the agreed rota in the absence of the RA Officer.
- For walk-ins and ad hoc calls re an RA request / query /issue. RA to check ServiceDesk Plus to establish if the request/query/issue is logged. If not, call to be logged in ServiceDesk Plus and assigned to the RA Category. RA to deal with the request/query/issue, where possible, then close the call in ServiceDesk Plus or where not able to resolve assign to the RA Officer. Individual raising the request/query/issue to be advised process is to report all RA requests/ queries / issues direct to the IT Servicedesk where these will be picked up and dealt with by RA and this is the process they should follow for future queries / issues / requests.
- Ensure the Temporary Access Card process is followed as and when required

Confidentiality of Information
All personal data processed by the RA relating to the registration process will be processed in accordance with the Data Protection Act 2018. Measures the RA Staff will adhere to include:

Maintain the confidentiality of personal information provided to them as part of the authentication process.

- Log the User identity details used on ESR (passport number, driving licence number, or national insurance number); any additional identification verified being noted in the Request Notes.
- RA managers and RA agents who are not HR staff should not take and retain photocopies of ID evidence.
- Do not copy, or store details of active in the community documents, only report they have been seen in the CIS request notes.
- RA01 forms once completed will be scanned and stored in the RA folder on the v drive and the originals disposed of.
- All RA forms will be stored in a locked and secure environment.
- Access is limited to RA staff who actively process registration information

RA Manager Responsibilities – As specified in National RA Policy
Organisations need to identify and appoint a RA manager as in section 2: *"Assignment of RA Managers, Agents and Sponsors*" of the RA Process Guidance. The responsibilities an RA manager has for their organisation in addition to those set out in section 4.1 above are: The following section highlights the RA Manager's responsibilities that **cannot be delegated** as described in the HSCIC RA Policy.

Responsible for running RA Governance in their organisation

- 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 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.

Audit Process

- As part of the RA Manager responsibility of running RA Governance, RA Managers should develop the organisation's RA audit process and conduct annual audits on NHS Smartcard usage.
- RA Manager must implement a process to run the RA reports available in CIS on a regular basis.
- 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.

Implements RA Policy and RA Processes locally adhering to national guidances

- 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.

Assign, sponsor and register RA Agents and Sponsors

- New roles have been created in the new Registration Authority software, Care Identity Service, 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.

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
- 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 2018. 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.

Facilitate the process for agreeing the organisations access control positions

- Once the organisations Access Control Positions have been agreed by the organisation's 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. In Humber this is delegated to the Information Governance Committee
- On approval by the organisation's Information Governance Committee, the RA Manager has the required agreement to create and modify Access Control Positions in CIS.

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 RA 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.

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

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 RA 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.

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 sooner.
- Furthermore, as per the above, 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 2018. 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

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, Director of Nursing, 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.

Ensure a maximum of three Users have Secondary Uses Service (SUS) access and that appropriate guidance for Summary Care Record, Electronic Transfer Prescriptions and SUS are observed.

RA Manager CAN delegate

- Creation 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
- Operation of core RA processes of registering a user, the approval and granting of access, the modification of personal details and the modification of access rights
    - The implementation of the local auditing process
    - Ensuring users accept terms & conditions of Smartcard use when registering them
    - Operational security of (old) paper-based RA records
    - Raising service issues as appropriate and through the correct channels

RA Audit and Reports
Ensure the RA service retains sufficient records to be able to determine, at a later date, the supporting evidence and methods used to verify and validate identity. In particular, all of the following information must be recorded by Registration Authorities for all Certificate Holders registered:

- The identity requirements that were met.
- The unique document numbers of identity documents that contain such numbers.

The following aspects will be investigated:

- Duplicate NHS Smartcards issued
- All Registered users have ID details completed to e-GIF level 3 status
- Lost Smartcards have the incident numbers logged within CIS
- Smartcard serial numbers are all accounted for (Damaged card serial numbers, issued serial numbers and in stock serial numbers)

- Leavers removed from the system
- Review the Approvers and Grantors of requests
- Users positions or access profiles are up to date and relevant
- Users' acceptance of NHS Smartcard Terms and Conditions

The RA Officer produces the quarterly and annual RA Update reports to the Information Governance Committee.

Sponsor Responsibilities
The range and respective responsibilities of the different types of Sponsors in CIS, and who these are assigned to are as follows:

RBAC Code	Description of activities
B0267 Approve RA Requests (Registration Only)	Approve Smartcard issue only. **Trust RA Team**
B1300 Approve RA Requests	Approve granting of non-restricted access rights to single Users - own or RA child organisation Approve registration of single User own or child RA child organisation (because of included activity B0267) Unlock Smartcards of all Users except RA Agents, RA Managers and Root RA Managers Assign Users to positions which they have been allocated to manage within their assigned Access Control Position Remove (multiple) staff from any position as constrained by RA restrictions, i.e., only for own and RA child organisations. Remove (multiple) staff from any Workgroup as constrained by RA restrictions, i.e., only for own and RA child organisations **Trust RA Team**
B0002 Approve RA Requests (Sponsorship Rights)	Approve who can be a Sponsor (Granted using normal B1300 Approve RA Requests). **RA Managers**
B0272 Approve RA Requests (Advanced)	Approve multiple profile updates (including Workgroup membership for any Workgroups, i.e., not just allocated ones) Approve granting of restricted attributes Approve creation and modification of positions (RBAC and Workgroups) Directly manage internal Workgroup hierarchy. This includes the assignment of Workgroup membership managers to these Workgroups Approve creation of linked workgroups and linking between Workgroups. This was formerly called pseudo-linking of cross organisational Workgroups. **RA Managers & RA Officer**
B0263 Unlock Smartcard (When available)	Unlock Smartcards and Renew Certificates of Users belonging to their NACS Org Code or child organisation. **Trust RA Team plus assigned to number of 'Local Smartcard Administrators' in bases across the Trust –**

All Sponsors who have the Sponsor activity B1300 or higher have the following activities automatically:

RBAC Code	Description of activities
B0262 View RA Information	View person profile View User Role Profiles (including Workgroup membership) Run basic RA reports **Trust RA Team**
B0265 Make RA Requests	Complete RA forms / CIS requests in order to request changes to other Users' access rights. Approval and granting of requests is controlled separately **Trust RA Team**

A User can only perform unlocking on profiles equal or subordinate to them in the RA hierarchy. The hierarchy consists of the RA Manager, RA Agent, Sponsor and then the Smartcard User.

4. PROCEDURES

Creation and Registration

Creation of a National Digital Identity
Health and Social Care Information Centre (HSCIC) as the single Registration Authority needs to be assured that users who have a digital identity created are subject to the same standards of identity verification, to prove identity beyond reasonable doubt, irrespective of which local organisation creates the identity. This is vital as the identity created is a national identity and must be trusted by each organisation where an individual is required to access the National Spine to access data. To achieve this, identity is required to be verified to the previous inter-governmental standard known as eGIF Level 3. This provides assurance that the identity is valid across any organisation that an individual works within.

In order to ensure this the following requirements in creating a digital identity are mandatory:

- 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 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.
- 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.
- 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.
- It has been agreed within Humber that a temporary access card can only be issued when the identity of the requester has been verified and it has been confirmed that they do hold a current smartcard which, for whatever reason is not working and there is a requirement to access or to enter information on to the patient's record in Lorenzo / SystmOne or, where there are extenuating circumstances and the director on call has approved the use of a TAC card by a user without a digital identity (for example Opel Level 4).

In respect of new starters, the necessary authorisation will be the completion of the Authorisation to recruit form.

All individuals should be asked to complete the CIS Create New User RA Use Only. The form must be completed by the individual who should then make an appointment with the RA Team to take in the completed form, together with their relevant original identification documents (ID) as per the process outlined below.

CIS Create New User RA Use Only Form: to be completed and signed by the RA.

Before the smartcard can be printed and the User registered, the applicant must have presented their ID documents as outlined in Figure 1 below. There are a number of routes which the RA Team can take to confirm an individual's identity, taking into account an individual's circumstances. If in doubt about what ID to take the individual should confirm this either with their line manager or a member of the RA Team.

All new applicants must provide at least one of the following: National Insurance number, Passport and/or Driving Licence which must be recorded on the smartcard spine user directory to check for duplicate users.

Once the ID has been checked, for new staff, the HR Recruitment Team will input this information into ESR raising the status to eGIF authentication level 3. All blank fields on the forms must be scored out to prevent tampering. For the process for temporary or agency staff please see section 3.1.7 below

All individuals in Humber Teaching NHS Foundation Trust will have their Smartcard produced in CIS, the individual's smartcard will then be printed and handed to them in person. For new starters, they will be provided with the smartcard in person at the Trust Induction.

An applicant should be advised how to maintain the security of their Smartcard, and how to obtain support when their Smartcard is issued through the issuing of the RA Smartcard user guide.

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 for the time being. If it becomes clear that the NHS Smartcard cannot be issued to the User, the NHS Smartcard should be cancelled in CIS, the User closed, and the NHS Smartcard physically destroyed.

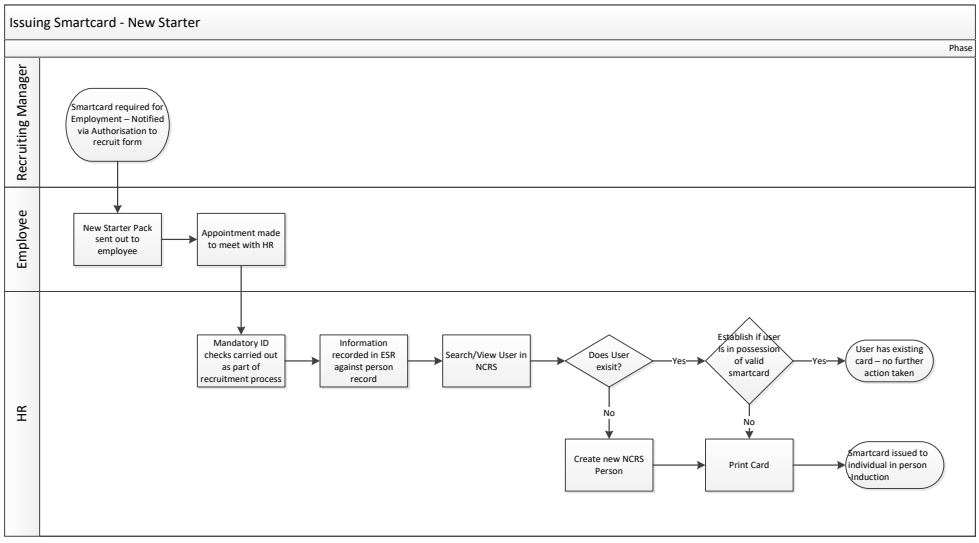


Figure 1 Issuing Smartcard - New Starter process

Registration Process

The following RA roles have the function to verify and create the identification of a 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 can be located below:

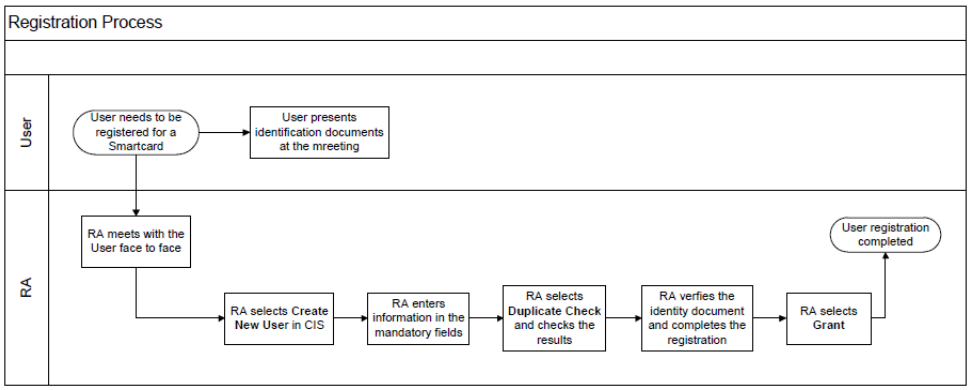


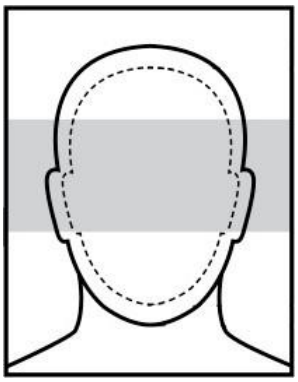
Figure 2 Registration Process

Photos

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:

- Size matches or exceeds the minimum size (420 x 525 pixels)
- 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)

Registration of Students
Undergraduate students undertake a number and range of clinical placements. As a result, students require an 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 an NHS Smartcard.

The need to verify students' identities and issue Smartcards is integrated into a single business process, coordinated between educational establishments and the RA Service Provider.

Issue Smartcard 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 as shown in Figure 3 below

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 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.

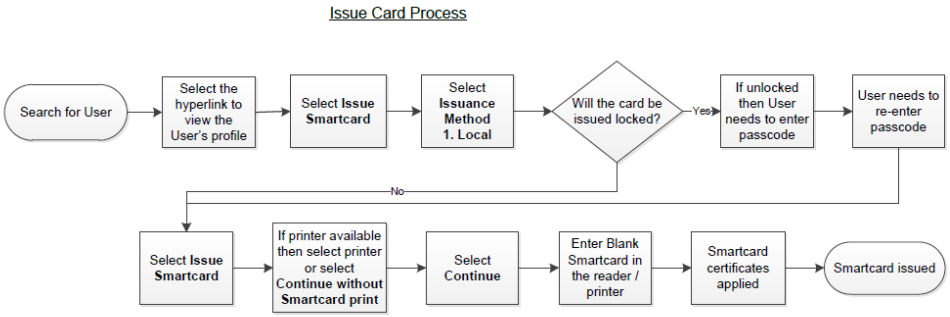


Figure 3 Issue Card Process

New Staff (Induction) Process
Individuals in Humber Teaching NHS Foundation Trust will have their Smartcard produced in CIS, the individual's smartcard will then be printed. An e-mail will be sent to the

individual from Service Desk Plus advising the smartcard is ready to collect. Following the process outlined in Figure 4 below.

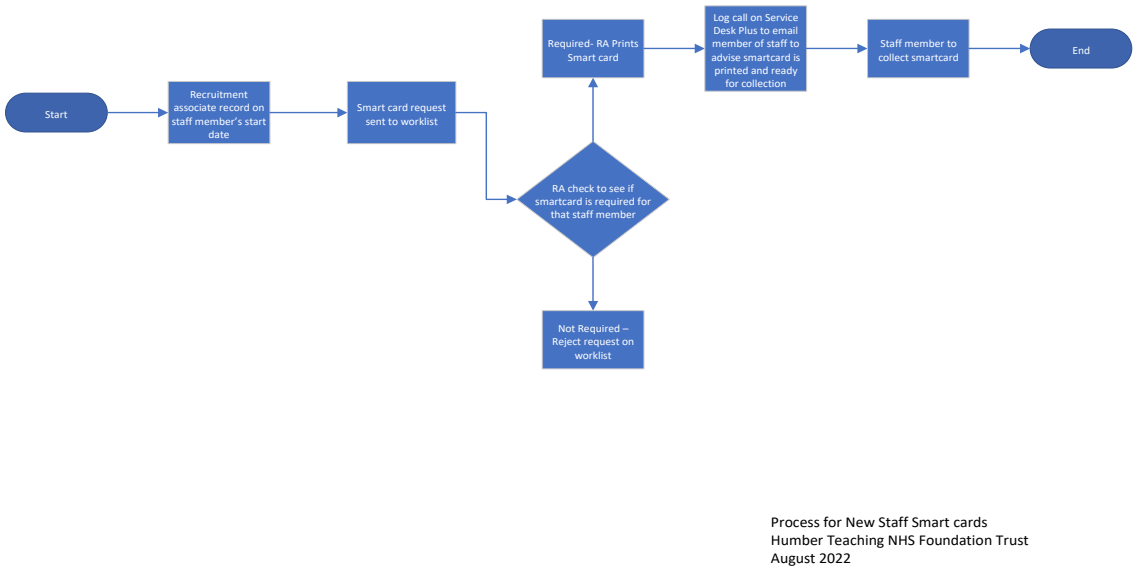


Figure 4 Process for Smartcards for new Staff

Non ESR Staff (Temporary Staff/Contractors)

For staff not employed by the Trust but working at the Trust and requiring access to Clinical Systems, Humber Teaching NHS Foundation Trusts RA staff will assign the NHS CRS Access to the non-ESR staff via CIS and a time limit of one year will be set unless notified what has been agreed on the contract length. Access for Non-ESR staff will be reviewed before date of expiration.

Where the member of staff does not already have a smartcard then the process of issuing a smartcard will be carried out by the RA team and the identity will be created directly on CIS.

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.

The Trust has made an exception to this where there are extenuating circumstances and the director on call has approved the use of a TAC card by a user without a digital identity provided the agreed ID checks have been carried out (for example Opel Level 4). Please see Registration Authority Temporary Access Cards Issuance and Usage Procedure

Process to issue Temporary Access Cards
The following process must be followed in full in order to issue a Temporary Access Card and is only to be used where access to clinical systems is required.

- Staff in charge logs a Datix and completes an RA04 form in full and emails it to the Assistant Director/Care Group Director during normal working hours or the on-call manager/director out of hours who will approve the issue of a TAC card.
- Staff in charge emails IT helpdesk with the Datix number and copy of the completed RA04 form and appropriate care group approval (as above) and the length of the shift the TAC card is required for.
- Call between the staff in charge and IT/RA or IT on call engineer who will log a call and enable the appropriate TAC card. The logged call will also be used to address the issue with the member of staff's own smartcard.

Staff using a TAC card **must** use the on behalf of functionality (this can only be used where they are already recognised in Humber Lorenzo however if all of the above have been followed then this would be the case).

The RA Officer will remove access from the TAC card at the end of the shift and immediately audit the use of the card. Any breaches in use will be reported to the Service and the Datix updated as these will need to be addressed and any corrections made to the patient record. Inappropriate use of the card will result in further investigations.

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.

NCRS Smartcard Position Based Access Control – Allocating a position and access rights to a Smartcard
Position Based Access Control (PBAC) provides a mechanism for users to be assigned the access they need in the course of their work, whilst also ensuring that these access rights are properly managed and appropriate for the job they are doing.

Instead of requiring case-by-case scrutiny for every person who requires access to care records, PBAC grants these rights according to the Access Control Position to which their job is assigned.

Humber Teaching NHS Foundation Trust has undertaken an analysis of the NHS CRS Access used within the organisation and has developed a range of Access Control Positions in consultation internally and externally with a range of staff. The access control position is assigned to an individual based on their team / service area (workgroup) and the system they will need to use; this may include SystmOne, Lorenzo, the Electronic Staff Record and / or the National Learning Management System.

It is expected that these Access Control Positions will be reviewed either on an ad-hoc basis when a request has been made or on an annual basis to ensure that the current requirements are still valid. For more information on PBAC please refer to the 'Position Based Access Control (PBAC) toolkit.

New Access Control Position
A new Access Control Position can be identified in a variety of ways as follows:

- A new NHS CRS system.
- A request to amend an existing NHS CRS Access Control Position (NHS CRS ACP);
- A new ESR Position within Humber Teaching NHS Foundation Trust.
- A new NHS CRS ACP.
- Identification through the review process.

When new NHS CRS ACPs are identified the RA Manager will need to determine who requires this access. The RA Manager / RA Officer are responsible for updating and maintaining CIS.

On approval by the organisation's Information Governance Committee, the RA Manager has the required agreement to create and modify Access Control Positions in CIS.

Amendment to an existing Access control position
It is likely that Humber Teaching NHS Foundation Trust RA Manager or RA Officer will receive a notification to amend an existing Access Control Position via four separate methods.

- A request from an existing user/sponsor via ServiceDesk Plus
- Identification of amendment through the review process
- Notification from a supplier that an amendment is required
- Trust Acquisitions or Mergers

Whatever method is used for requesting the change, the process for amendment will still follow the authorisation process that has already been established within Humber Teaching NHS Foundation Trust. The process for when changes need to be made to workgroups and access control positions is as follows:

- Request for changes to be made to the RA Manager or RA Officer
- RA Manager considers the impact of the proposed changes, in consultation with relevant system / project leads / operational managers / Information Governance
- RA Manager approves changes, which are then implemented

If the request for change is denied the person that made the request will be notified of the outcome and this, in turn, could then determine whether a new Access Control Position is created.

It is necessary to ensure that any changes are evidenced within Care Identity Service Approval details under Modify Position workflow.

Removal of an Access Control Position
If, during the review process, Humber Teaching NHS Foundation Trust RA Manager / RA Officer identify that an Access Control Position is no longer required the RA Manager / RA Officer must identify who is currently assigned to the Access Control Position and determine whether the staff in question need to be assigned to a new position.

If a replacement Access Control Position is not required Humber Teaching NHS Foundation Trust RA Team will notify the staff in question that they will no longer have any NHS CRS Access associated with their Smartcard.

Once these steps have been completed the Humber Teaching NHS Foundation Trust RA Team will be able to revoke the Access Control Position to stop the position from being assigned.

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

Auto Approved Request
A request submitted by RA 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.

Auto Granted Request
In addition, a request submitted by the RA Manager, Advanced RA Agent or RA Agent in CIS can be automatically granted

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.

Personal Information Management
We have the ESR-CIS Interface activated in Humber Teaching NHS Foundation Trust, although not fully implemented, to use ESR to automatically inform CIS of any personal detail changes, ensuring that the data is kept up to date in CIS and consistent with ESR.

Amendments to the data items below, in ESR, will automatically trigger a message to be sent to CIS. RA Officer and HR RA staff within Humber Teaching NHS Foundation Trust will ensure that they regularly monitor CIS to accept/reject changes that may not receive automatic approval.

NB The personal details that are shared with CIS from ESR are as follows: -

- Title
- Surname
- First name
- Middle name
- NI Number
- Date of Birth
- Email address

Worklists

Worklists are the mechanism for managing requests that are created in CIS (or received from ESR). An organisation can have as many Worklists as required to support the needs of the business.

Worklists are used as a method of identifying the requests and RA actions which need to be processed within CIS and the Worklists will be viewable by everyone that has RA rights, such as the RA Agents and RA Managers. RA Staff are able to view requests awaiting action, their own requests, completed requests and all open requests.

FFFFF Codes

The National Information Governance Board (NIGB) originally agreed that Locum Pharmacists when logged onto the Electronic Prescription Service application need not be associated with the specific organisation in which they are working. As a result, the virtual National Locum Pharmacy organisation (FFFFF) parented by all RA Service Providers Registration Authorities was created specifically for this purpose, and no other. **Currently these are not used in Humber Teaching NHS FT.**

Maintenance of Smartcards

Assisted Unlock Smartcard Process

Users who have forgotten their passcode, or whose card has been locked due to too many failed login attempts, should contact in the first instance one of the designated Local Smartcard Administrators (a list of these can be found by work base on the Intranet).

The user will need to meet the Local smartcard administrator face to face, producing their Trust ID badge to verify identification, to have their card unlocked or passcode reset/changed. The Local smartcard administrator must establish the identity of the user by checking the photograph in CIS and also by verifying the user by checking their Trust ID badge.

If the Local smartcard administrator is unavailable or not able to unlock the card or change the passcode(s), the user should report their problem to the IT Servicedesk. The user should provide their name, contact telephone number and a brief description of the problem to the IT Servicedesk who will then assign the call to the RA Team. The RA Team will contact the user to arrange a face-to-face meeting to unlock their card or change the passcode(s).

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
- 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 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.

Local Smartcard Administrators can only unlock NHS Smartcard users and one another's NHS Smartcards and reset passcodes. 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 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 ID Checker (B0267)	None – Needs B0263 to perform this function.
Local Smartcard Administrator (B0263)	Can unlock all non RA users.

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

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.
- 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 3.24 Cancel Card Process.

Assisted Unlock Process in CIS
The process below provides an overview of the workflow in CIS when a RA 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 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 and LSAs to negate the need to search for the user first. Further information on the Manage Smartcard workflow is in section 3.18 of this document.

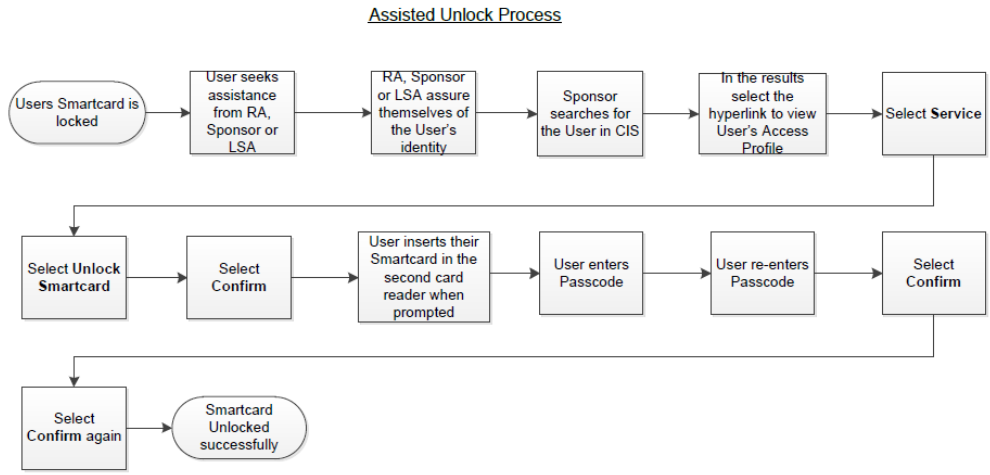


Figure 5 Assisted Unlock Process

CIS Self Service Smartcard Unlock

The CIS Self Service Smartcard unlock application enables Smartcard holders to unlock their Smartcard themselves without having to contact their local RA to do this for them.

The user needs to register on their CIS User Profile page in order to have this functionality enabled. It requires the individual to set answers to secret questions and enter their email address and an authorisation code.

Once set up, if the user then locked their Smartcard, they would open the Unlock Smartcard web page located on their desktop to request a reset.

Change Passcode

NHS Smartcard users are able to change their passcode at any time using the change passcode process in the Care Identity Service application, without additional assistance from RA or LSA. RA should recommend users do so at regular intervals.

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 and the HSCIC Identity Agent 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.

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.

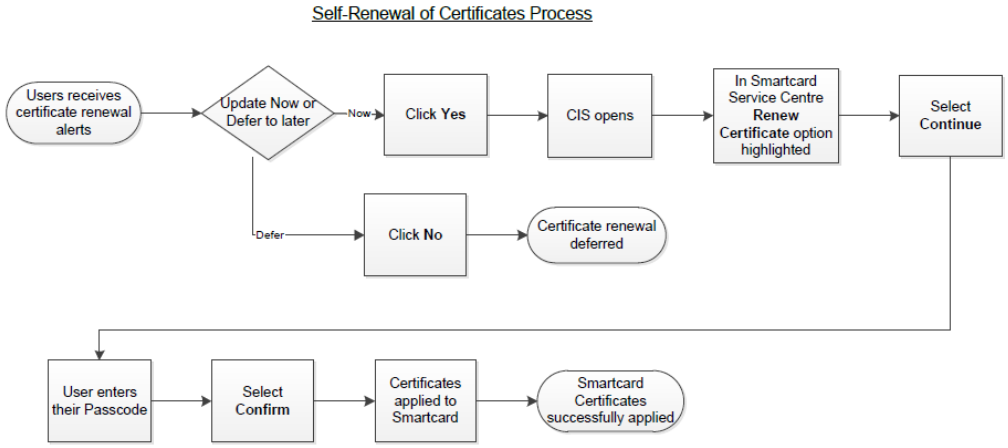


Figure 6 Self Renewal of Certificates Process

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 Local Smartcard Administrators who will assist to renew their certificates before they expire. RA staff 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 or LSA assists the user to renew their Smartcard certificates.

This option requires RA staff 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 and LSAs to negate the need to search for the user first. Further information on the Manage Smartcard workflow is in section 3.18 of this document.

The option to renew certificates is only available when the certificates are due to expire within 90 days. However, users will be prompted 90 days before the certificates expire on a daily basis.

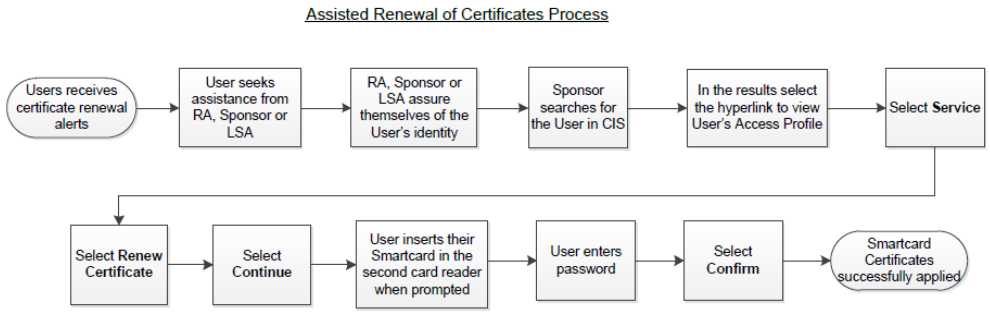


Figure 7 Assisted Renewal of Certificates process

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:

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

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.

Damaged Smartcards
If a smartcard becomes damaged the user should report this to the IT Servicedesk. The RA Team will then contact the user to arrange a face-to-face meeting to issue the user with a new smartcard

Lost/Stolen/Misplaced Smartcards
In line with national Serious Incident requirements a lost, misplaced or stolen smartcard is classed as a Serious Incident (SI). The SI Intranet pages can be found at http://intranet.humber.nhs.uk/directorates/new_page_3.htm.

It is a requirement that all lost, misplaced or stolen smartcards are reported via the Trust's Serious Incident reporting procedures immediately it is established they no longer have their smartcard. To report an incident to the Trust's Risk Management Team the user must complete the Trust adverse incident form on paper Adverse Incidents or online via Datix-Web - https://datix.xvictoria.nhs.uk/datix/humber/. The user must also report this to the Humber IT Servicedesk.

Serious incidents involving the loss or theft of, or misplaced smartcards also have to be reported to the Trust Information Governance Group, the Trust Board, the Council of Governors and to a number of external organisations. Every attempt should be made therefore by the user to find the smartcard prior to reporting via Datix this as lost, stolen or misplaced.

When a User reports a lost/stolen/misplaced Smartcard to the RA Team, the Smartcard should be cancelled immediately.

The RA Team will then:

- Where necessary, meet the User face-to-face to verify their identity and issue a replacement NHS Smartcard. The User's identity should be confirmed by the photograph in CIS. If the identity still cannot be verified the User will be required to produce documentary evidence of their identity.
- Cancels the old lost/stolen/misplaced/damaged NHS Smartcard.
- Issues a replacement NHS Smartcard – Documenting the Datix Web Ref number against the UUID using the 'notes' field.

Note: Under NO circumstances should individuals 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 Team

within the organisation must cancel the NHS Smartcards and follow the recommended process for disposing NHS Smartcards that are no longer required.

Incident Reporting
Incidents may be reported by any member of staff where they feel that there is a risk to patient health, confidentiality or Trust reputation. Incidents should be reported as outlined in section 3.3.10 above.

Examples of incidents, in addition to those in 5.10 above are:

- Smartcard or application misuse
- Non-compliance of local or national RA policy
- Any unauthorised alteration of patient data
- Disclosure of smartcard passcode to a person other than the cardholder
- Use of smartcard or application by a person other than the cardholder
- Access to application or data for an unauthorised purpose
- Disclosure of data without justification or for an unauthorised purpose.

The RA Officer, together with the Trust's Risk Management Team will consider all incidents reported to them. A major breach of security will also be reported by the RA Manager to the Regional RA / IG Lead and Health and Social Care Information Centre to ensure any risks resulting from the event can be taken into account and mitigated against.

A significant incident is an isolated incident or a series of less significant incidents that could lead to a serious degradation of healthcare or information security. The Operational Risk Management Group, the Information Governance Committee, Trust Board and Council of Governors will consider incidents reported to them and decide whether Trust systems or working practices should be reviewed as a result.

Incidents involving breaches of security or demonstrate that a User may not be considered trustworthy should also be reported to HR and the Director of Nursing by the RA Manager so that any disciplinary measures required may be taken. HR will decide which other members of staff need to be involved (e.g., line manager, IT Manager).

Smartcard Misuse
If it is suspected that a smartcard is being misused, it is the responsibility of the person suspecting this to raise it as an incident, and to report it directly to the Risk Management Team and RA Manager/RA Officer in line with reporting arrangements in 3.3.10 above.

The Line Manager/Project Manager and Information Governance Manager will be contacted, and Disciplinary action could follow. In relation to students, the students Mentor and one of the Practice Learning Facilitator will be contacted. Smartcard misuse could constitute gross misconduct.

If the member of staff has roles in more than one organisation, all other organisations will be informed. In respect of students the respective University would be informed.

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:

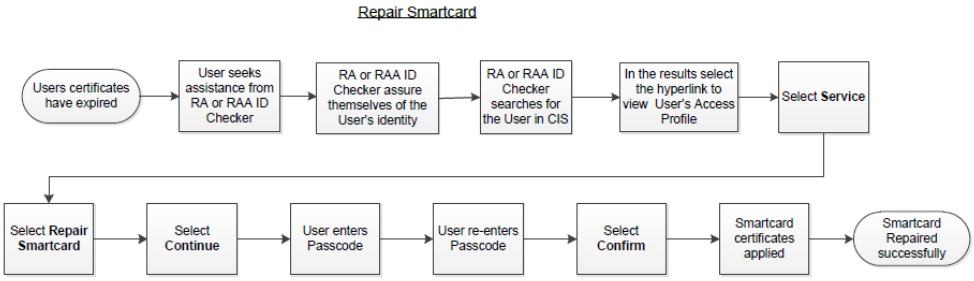


Figure 8 Repair Smartcard process

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)

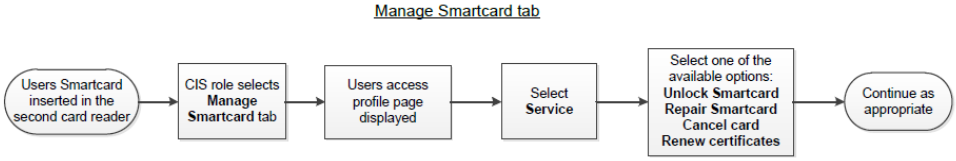


Figure 9 Manage Smartcard tab process

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).

An applicant should use the same name for Smartcard registration as for their employment in an organisation. If this name differs from the documentary evidence provided, proof through a **marriage certificate, divorce certificate, deed poll, adoption certificate, or statutory declaration** is required. In these circumstances only it is not necessary for all identity documentation to show a consistent name.

When a user changes their personal details, for example when they get married, he or she should complete a 'Personal change of details' form, available on the Trust intranet, and send to HR - Recruitment in Mary Seacole Building at Willerby Hill, Willerby. Only documents listed in the 'Use of Name' section above are acceptable as proof of name change. Changes will then be made to the staff members electronic personnel file held in the Electronic Staff Register (ESR). This automatically notifies the Registration Authority staff via a worklist in CIS that the user has been modified and that a new card needs printing.

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

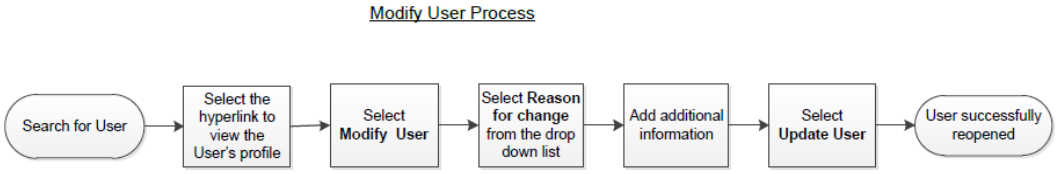


Figure 10 Modify User process

Leavers/Cancellation Process
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 an 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 an 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 an 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.

It is the responsibility of the person's line manager/project manager to make sure that they complete the relevant section of the Trust's termination form, or notifies RA, to request revocation of the Humber Teaching NHS Foundation Trust organisational profile. The termination form should be sent to the Hn-tr.terminationforms@nhs.net

The RA Team will then end date or revoke the individual's access effective from the date of the individual's last day of employment.
In respect of students an email should be sent to the RA Manager or RA Officer by the Mentor/Educator to notify the student is changing or leaving their placement. The RA Manager/RA Officer will then revoke this access in CIS.

Where the revocation has been requested by HR because of security related events the RA Manager/RA Officer will authorise the appropriate action and inform the following staff as appropriate:

- If reported to the RA Officer, RA Officer to notify RA Manager
- The HR Manager/Adviser
- User's Line Manager
- Risk Management Team (this may also include the Clinical Safety Officer)
- The User

As an additional control, the RA Officer will run a report from ESR on staff leaving on a weekly/monthly basis. This will be used to check and terminate access, if not done already, to Humber Teaching NHS Foundation Trust systems.

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 3.26 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.

Leavers transferring to another NHS organisation
If the user is transferring to another health organisation, for example a GP practice or Acute Trust then the user must retain their NHS Smartcard, but their current position assignment must be set an end date.

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.

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.

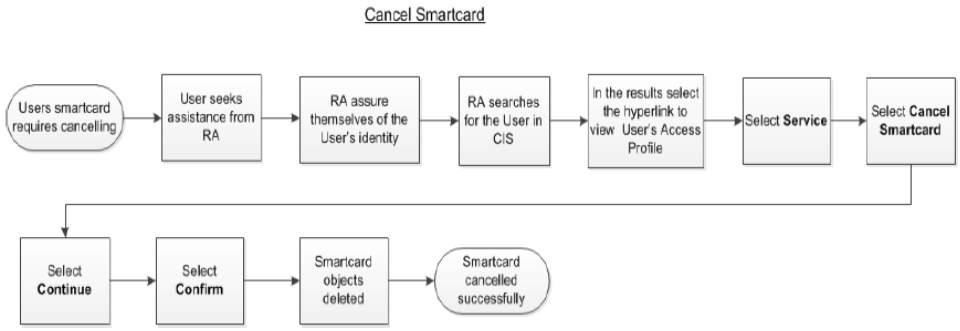


Figure 11 Cancel Smartcard process

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.

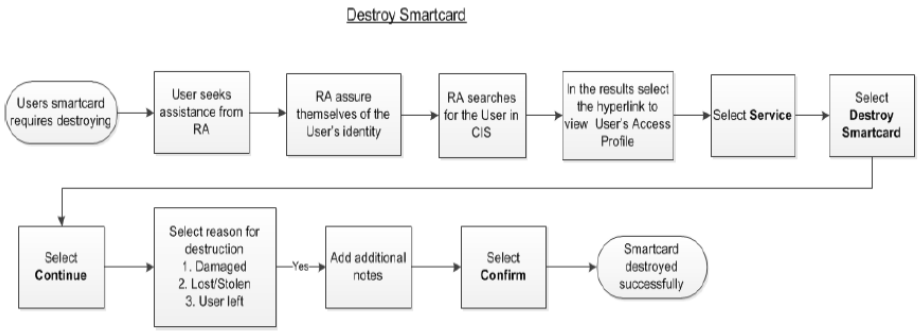


Figure 12 Destroy Smartcard process

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 colleague's department in advance to agree appropriate wording.

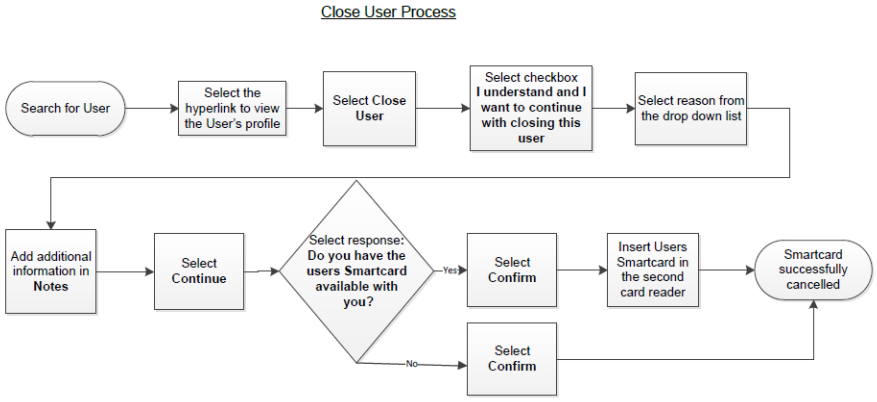


Figure 13 Close User process

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
Returned from long leave
Closed by mistake
Joined back
Other

RA staff must reconfirm identification where reasons 1, 3 or 4 from the above list are selected.

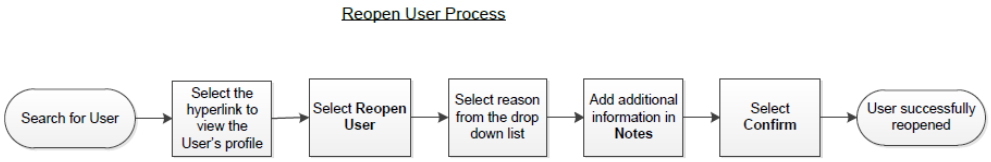


Figure 14 Reopen User process

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	No	Yes	No	No
Leaving the organisation	No	No	No	Yes
Leaving Healthcare	No	No	Yes	No
Deceased	No	No	Yes	No
Suspended	No	No	No	Yes

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 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

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.

Lorenzo/SystmOne Change Request Form
These forms are used to request changes to an existing CRS Application User's position. Wherever a change to a user's position is identified the relevant sponsor must authorise the required change.

Once the relevant Sponsor has authorised the change(s) the Systems form will be processed by the RA team upon notification that the User has completed the necessary training.

Should there be any problems with the form these will be referred to the authorising Sponsor, prior to being processed by the RA Team. See Figure 15 for further information on the workflows for change request forms

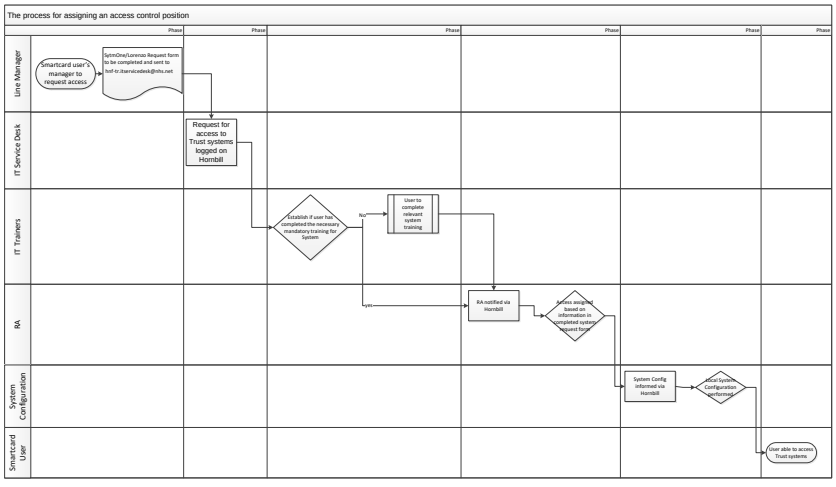


Figure 15 Assigning Access process

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 RA Operating Guidance Document.

During disciplinary investigations the RA Manager may complete a CIS Cancel Smartcard Form to ensure immediate revocation of their access rights and to minimise the risk to the organisation.

Smartcards should be destroyed as soon as is practical after the employee leaves the organisation.

Training

It is the responsibility of the RA Manager to ensure that all RA staff they keep up to date with developments and attend available training. Training on both the ESR and Registration Authority systems is a mandatory element of Humber Teaching NHS Foundation Trust Recruitment and RA staff. This will maximise the staff's knowledge of the two systems to ensure that they have the ability to use the systems as per the requirements specified by Humber Teaching NHS Foundation Trust, ESR and HSCIC.

ESR Training for RA Manager, RA Officer, Recruitment RA

ESR – CIS interface users can access the necessary eLearning via the NLMS

ESR-CIS Interface users can also access the ESR online user manual and other learning material via Kbase.

CIS Training for RA Manager, RA Officer, HR RA and Local Smartcard Administrator

Humber Teaching NHS Foundation Trust's Registration Authority staff will ensure that the HSCIC e- learning material, available http://hscic.premierittask.com/ is completed by everyone that has a requirement to access CIS.

Following the completion of the relevant e-learning material the trainee must notify the RA Officer so that this can be documented in accordance with the latest version of the IG Toolkit.

National Administrative Codes Service (NACS)/Organisational Data Service (ODS) Codes in ESR

The NACS Code is a crucial element of the ESR-CIS Interface. Humber Teaching NHS Foundation Trust has identified one main NACS Code for the organisation (RV9) which is available in ESR and has been added to the Trust level of the hierarchy. If the NACS code was to change or a new one added Humber Teaching NHS Foundation Trusts, ESR staff must raise an SR with McKesson to ensure that the correct NACS Code is made available for use within the Humber Teaching NHS Foundation Trust VPD. Once this has been completed the NACS Codes must be updated/added in line with the ESR guidance. (For further information see ESR_setup_quick_reference-guide v l 0.doc). As a minimum the NACS Code must be placed at the Trust level of the organisations hierarchy and can only be altered or amended by the ESR Work structures administrator. If required in the future, Humber Teaching NHS Foundation Trust can assign multiple NACS codes within ESR at the topmost level of the hierarchy where it is required. This will ensure that ESR sends messages to the correct CIS instance.

RA User Role Profiles (URP's) in ESR

Humber Teaching NHS Foundation Trust has allocated the required RA URPs to all relevant staff within the HR & Diversity Directorate whose NHS CRS access contains the requisite RA Manager and RA Agent role. These URP's have been allocated to staff to ensure that multiple people have the ability to carry out tasks within the functionality of the ESR-CIS Interface.

The RA Manager, in conjunction with the Workforce Performance and Information Adviser will review the allocation of these URPs on an annual basis, or on an ad-hoc basis if staff/Line Managers identify a need for it, to ensure that they are appropriately assigned and to ensure business continuity

5. EQUALITY AND DIVERSITY

The Trust aims to ensure that all of its policies are equitable with regard to age, disability, gender, race, religion and belief or sexual orientation.

An Equality Impact Assessment has been carried out by the author which confirms that this policy does not impact on any equality group (Appendix 1).

6. BRIBERY ACT

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf.

If you require assistance in determining the implications of the Bribery Act please contact the Trust Secretary on 01482 389194 or the Local Counter Fraud Specialist on telephone 0191 441 5936 or email counterfraud@audit-one.co.uk.

7. MONITORING AND AUDIT

The Information Governance Group will be responsible for monitoring the effectiveness and reviewing the implementation of this policy, regularly considering its suitability, adequacy and effectiveness taking into account legal development and changes in the Trust's business. Any improvements identified will be made as soon as possible.

8. REFERENCE TO ANY SUPPORTING DOCUMENTS

Registration Authority Policy V1.0
Registration Authorities Operational and Process Guidance V5.1
Registration Authorities: Governance Arrangements for NHS Organisations
Information Security and Risk Policy N-051

Appendix 1 - Equality Impact Assessment (EIA)

Equality Impact Assessment (EIA)

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: RA Standard Operating Procedure
2. EIA Reviewer (name, job title, base and contact details): Gary Walton, RA Officer, Mary Seacole Building, 01482 477893
3. Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other? Standard Operating Procedure

Main Aims of the Document, Process or Service
This procedure sets out to provide guidance to individuals working at Humber Teaching Hospitals NHS Foundation Trust on using smartcards including the national obligations, roles and responsibilities of the Registration Authority (RA) and the Registration process to issue and update NHS Smartcards to Users.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed?	How have you arrived at the equality impact score?
1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender re-assignment	Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	Low	There is no evidence to suggest that the RA Standard Operating Procedure will have a negative effect on groups with the protected characteristics contained within the Equalities Act.
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory Physical Learning Mental health (including cancer, HIV, multiple sclerosis)	Low	As above.
Sex	Men/Male Women/Female	Low	As above.
Marriage/Civil Partnership		Low	As above.
Pregnancy/ Maternity		Low	As above.

Race	Colour Nationality Ethnic/national origins	Low	As above.
Religion or Belief	All religions Including lack of religion or belief and where belief includes any religious or philosophical belief	Low	As above.
Sexual Orientation	Lesbian Gay men Bisexual	Low	As above.
Gender Reassignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	Low	As above.

Summary

Please describe the main points/actions arising from your assessment that supports your decision. There is no evidence of potentially negative effect on groups with protected characteristics. Applying the measures set out in the RA Standard Operating Procedure Policy does not impact on anyone with protected characteristics.	
EIA Reviewer: Sarah Fearnley	
Date completed: 24/05/2022	Signature: S. Fearnley