Humber Teaching
NHS Foundation Trust

Registration Authority Policy
(F-008)

Version number:	1.6
Author (name and job title)	Sarah Fearnley – RA Officer Julie Crockett – RA Manager
Executive Lead (name and job title):	Peter Beckwith, Director of Finance
Name of approving body	Governance Committee
Date full policy approved:	Sept 2013
Date Ratified at Trust Board:	Sept 2013
Next Full review date:	June 2025

Minor amendments made prior to full review date above (see appended document control sheet for details)	
Date approved by Lead Director:	*30th June 2022 - Peter Beckwith, Director of Finance*
Date EMT as approving body notified for information:	*June 2022*

Policies should be accessed via the Trust intranet to ensure the current version is used

Content

1. INTRODUCTION

Purpose

The purpose of this document is to provide guidance on the national obligations, roles and responsibilities of the Registration Authority (RA) and the Registration process to issue and update NHS Smartcards to Users.

Further information regarding the procedures for the issuance, use, security and withdrawal of smartcards used across Humber Teaching NHS Foundation Trust can be found in the Registration Authority Standard Operating Procedure document which should be read in conjunction with this policy

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 and related guidance.

This document provides an overview of registration and the assignment of access to NHS Smartcard applicants by the local Registration Authority and Sponsors using the current available processing systems:

- Care Identity Services (CIS) standalone.
- ESR Interface to CIS (This interface is activated for Humber Teaching NHS FT but not yet fully implemented).

Background

Since the introduction of the NHS Care Records Service (NHS CRS) compliant applications, it is of paramount importance that NHS patients are confident that their medical records are kept secure and confidential in line with the *"Care Record Guarantee"*. To achieve this objective all healthcare professionals/workers requiring access to NHS CRS compliant applications must be registered and issued with a NHS Smartcard and have appropriate access profiles.

What is the Registration Authority?

The Registration Authority consists of the RA Manager, RA Agents, Sponsors and Local Smartcard Administrators who have a responsibility to individuals providing healthcare services to the NHS directly or indirectly, to ensure timely access to NHS Care Records Service applications in accordance with their healthcare role.

The mandatory requirements in relation to organisational set up and appropriate governance oversight are:

1. There needs to be a Board/EMT level individual who has overall accountability in the organisation for RA activity. The responsible individual must report annually to the organisation on this activity.

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

RA Managers within organisations running their own RA activity are accountable for the running of RA activity in their organisation. They need to set up the systems and processes that ensure that the policy requirements contained in this document are met and local processes meet these requirements and cater for local organisational circumstances (NOTE: deviation from these policy requirements due to a local preference is not permitted).

1. RA Managers and Agents need to keep up to date with national policy requirements, initiatives and changes. In order to do this it is mandatory that their email address is entered as part of their personal details held within the database of Smartcard users. They are also required to subscribe to the national email address list by sending an email with their details to ramanagers.agents@hscic.gov.uk

2. RA Managers have a line of professional accountability to uphold good RA practice to HSCIC.

It is important that all members of the Registration Authority are aware of the confidential nature of some of the information captured during registration and preserve its confidentiality. All data and personal information about NHS Smartcard Users must be used in accordance with the Data Protection Act 2018 principles. An organisation's RA operates within the governance framework identified in *"Registration Authorities: Governance Arrangements for NHS Organisations"*.

What are NHS Smartcards?

NHS Smartcards are a plastic card containing an electronic chip (like a chip and PIN credit card) that is used to access the NHS Care Records Service (NHS CRS) and other National Programme for IT applications, along with a Passcode. The chip stores the Unique User Identifier (UUID), providing a secure link between the NHS CRS and the database holding the Users information and access rights. The combination of the NHS Smartcard and the Passcode together, help protect the security and confidentiality of every patient's personal and healthcare information.

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

The primary purpose of NHS Smartcards is to provide identification and system authentication to local informatics applications.

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

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

This document only endorses the use of NHS Smartcards and, in exceptional circumstances, the use of Temporary Access Cards in the Trust's inpatient units as described in Section 4 of the Trust's Registration Authority Standard Operating Procedure document

What is the Care Identity Service?

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

What is the ESR Interface to CIS?

The ESR Interface to CIS, also known as Integrated Identity Management (IIM) combines the separate processes, maintained within Registration Authority and Human Resource teams, for capturing and managing an employee's identity and access to the Spine. This interface is activated for Humber Teaching NHS FT but not yet fully implemented.

The Registration Process

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

A user is identified for a NHS Smartcard – this can be via

- an individual (sponsor – within Humber the sponsor is an individual's line manager/Head of Service) explicitly requesting the individual be registered in CIS or
- other means such as employment into a role or requirements of a job changing

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

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

Further information on appropriate identification documents and guidelines is found on the NHS Employers website:
http://www.nhsemployers.org/~/media/Employers/Documents/SiteCollectionDocuments/Identity%20checks%2022%20July.pdf

2. SCOPE

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. POLICY STATEMENT

The Trust's Registration Authority ensures that individuals providing healthcare services to the NHS directly, or indirectly, have access to NHS CRS compliant applications/information in accordance with their role. The Trust's Registration Authority will ensure that all aspects of Registration Authority services and operations are performed in accordance, and comply, with the following:

4. DUTIES & RESPONSIBILITIES

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.

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 are 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. The RA sponsor responsibilities and who these are assigned to is shown in 4.3

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 work station/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.

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. (Fall-back smartcards and short-term access smartcards are not NHS smartcards in this context – Fall-back and short-term access smartcards are not used in Humber Teaching NHS FT).
- 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%20identity%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 service desk, logged in ServiceDesk Plus and assigned to the RA stack 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 /issues. 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 Stack. 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 service desk 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.
- CIS – Create New User 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 organization

- 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 CIS - Create New User 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 guidance's

- The local RA policy and local RA processes should be implemented by the RA manager and all RA staff in the organisation and child organisations should be both made aware of them and have access to them.
- The organisations RA processes should reference CIS forms or temporary access cards if used by the organisation or child organisations, as well as the approve and grant process and the direct assignment of positions to a user's access profile.

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 organisations key stakeholders, RA managers must ensure that the organisation formally approves the positions in writing before creating the positions in care identity service.

- RA managers must identify in the organisations local processes the process for the executive management team to approve new and modifications to existing positions in the organisations. 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 – Unlockers

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.

5. PROCEDURES RELATING TO THE POLICY

The policy and procedures listed in Section 11 of this policy will be to be used to manage and monitor all aspects of RA compliance.

6. EQUALITY & DIVERSITY

An Equality and Diversity Impact Assessment has been carried out on this document using the Trust approved EIA. In conjunction with their line manager / project manager / mentor an assessment would need to be carried out, seeking advice from Occupational Health as appropriate, for any users who may have a medical condition, i.e. sight impairment, dyslexia, and actions taken as appropriate to enable a user to use the respective system.

An Equality Impact Assessment has been carried out by the author which confirms that this policy does not impact on any equality group (Appendix 4).

7. IMPLEMENTATION AND MONITORING

This policy will be disseminated by the method described in the Document Control Sheet (Appendix 3).

This policy will be disseminated by the method described in the Policy and Procedural Documents Development and Management Policy.

8. MONITORING AND AUDIT

RA Activity Audit

The RA Officer will produce reports from the Spine User Directory and Electronic Staff Record to ensure accuracy of access rights and staff list.

RA is monitored and reported to the Trust Information Governance Committee who will receive quarterly reports together with an annual report.

Independent Audit

The management and use of smartcards may be subject to internal and external audit to ensure that national and local policies are being followed. Specifically, auditors may look to confirm that:

- Smartcards are handled securely by users
- RA documents are used and stored appropriately
- Access to Clinical Systems applications and records is controlled appropriately
- Unused smartcards are stored safely and appropriate records are kept
- Role allocation and de-allocation is performed appropriately

To aid audit the following records will be maintained:

- The number of smartcards held
- Details of Smartcards issued.

9. 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 P096
Humber Teaching Hospitals NHS Foundation Trust Registration Authority Standard Operating Procedures

10. LEGISLATIVE AND POLICY REQUIREMENTS

There are various legislative and policy imperatives that apply to all care organisations, in all matters concerning the storage and use of person identifiable information. These include:
The Data Protection Act 2018 The Computer Misuse Act 1990 E Communications Act 2003
Electronic Signatures Regulations 2002 NHS Confidentiality Code of Practice
The Records Management NHS Code of Practice The Freedom of Information Act 2000
The NHS Care Record Guarantee for England (PDF, 128.2kB)

11. MONITORING COMPLIANCE

See Appendix 3.

Appendix 1: Glossary of Terms

Term	Definition
CIS	Care Identity Services. Software which provides the paperless electronic management of access control (Replaced CMS, Calendra and UIM)
CRS	(National) Care Records Service aims to create the integrated electronic care record
ESR	Electronic Staff Record
ServiceDesk Plus	IT Service desk software used to report and manage calls to the IT Service desk.
HSCIC	Health and Social Care Information Centre; sometimes known as 'The Information Centre' (for Health and Social Care) or 'the IC'. The prefix (existing) is used to refer to the current organisation and (new) to refer to the organisation post April 2013.
National Role Based Access Control(RBAC) Database	This contains the national approved RBAC Attributes (Job Roles, Areas of Work and Activities) along with Baseline definitions, information on particular deployed applications and an integrated set of guidance tools, called the RBAC Assistant.
NHS Care Records Service (NHS CRS)	The NHS Care Records Service will help NHS organisations in England to store patient health care records on computers that will link information together quickly and easily. An NHS Smartcard will give a User access to the NHS CRS and other National Programme for IT applications such as Choose and Book and the Electronic Prescription Service.
NHS Employment Check Standards	Mandatory checks employers must carry out in the appointment, and on-going employment, of all individuals in the NHS.
ODS	Organisation Data Service
Position Based Access Control (PBAC)	The ability to assign access rights per post within an organisation.
Registration Authority (RA)	The organisational structure within an NHS organisation that is responsible for registering and verifying the identity of health care professionals/workers who need access to the NHS Care Records Service (NHS CRS) and other applications.
RA Forms	Forms to support RA administration

Roles Based Access Control (RBAC)	Defines a national standard set of Job Roles and related Activities and Areas of Work which can be approved by a Sponsor and granted by the RA to a User. Each application, such as Choose and Book, uses these definitions to enable access to specific functionality and information in their system.
Smartcard	A plastic card containing an electronic chip (like a chip and PIN credit card) that is used to access the NHS Care Records Service (NHS CRS) and other National Programme for IT applications, along with a Passcode. The chip does not contain any personal information, providing only a secure link between the NHS CRS and the database holding the Users information and access rights. The combination of the NHS Smartcard and the Passcode together, help protect the security and confidentiality of every patient's personal and healthcare information.
Spine User Directory (SUD)	Repository which stores Users profiles and registration information both current and historic e.g. includes roles and organisations that an individual may have previously worked for.
Secondary User Service (SUS)	SUS is a single repository of person and care event level data relating to the NHS care of patients, which is used for management and clinical purposes other than direct patient care. These secondary uses include healthcare planning, commissioning, public health, clinical audit, benchmarking, performance improvement, research and clinical governance.

Appendix 2: RA Hardware Monitoring Procedures

Introduction

This procedure is to comply with the policies and procedures set out in the RA procedure for Humber Teaching NHS Foundation Trust.

This procedure only applies to Registration Authority staff based within the Trust.

The Trust RA manager and Agents have a duty to meet legislative and statutory requirements in relation to IT security. These include the Connecting for Health Information Governance Toolkit and statement compliance.

Duties and Accountabilities

RA Staff

All RA staff have a responsibility to adhere to this procedure
Information Governance Committee
The Information Governance Committee is responsible for agreeing to any changes to this process and receiving a quarterly report on the position of the asset register from the Lead RA.

RA Manager

The RA manager is responsible for ensuring that this procedure is followed by the RA team. They are also responsible for ensuring that there is sufficient supply of smartcards and smartcard hardware, including the hardware required to access the Care Identity Service (CIS) for both RA Agents and Local Smartcard to unlock Smartcards. The RA manager must discuss with IT services their requirements with regard to any required hardware.

RA Team

The RA Team based within Humber Teaching NHS Foundation Trust is responsible for the recording of all RA related equipment in the asset register and for ensuring that the asset register is kept up to date. The RA Team are responsible for ensuring that when equipment is moved or used or allocated to staff then the asset register must be updated

RA Equipment Asset Register

Registration Authority Equipment Requirements

The Registration Authority team requires the use of the following equipment in order to be able to issue smartcards:

- PC or Laptop with 5 or more USB ports
- HSCN or NHSnet network connection
- Supply of Blank Smartcards
- Smartcard Printer/Ribbon
- Digital Camera
- Smartcard Readers

Registration Authority Managers, Agents and Local Smartcard Administrators require the following set of equipment so that they may perform maintenance of user's access.

- PC or Laptop with access to CMS Portal

- HSCN or NHSnet network connection
- Two smartcard readers

All smartcard users require the following equipment to be able to connect to applications requiring a smartcard:

- Pc or Laptop
- HSCN or NHSnet network connection
- 1 Smartcard reader

Mobile RA equipment is to be locked in a secure area at all times when not in use. The equipment should not be left unattended on site or in the boot of a car.

All CIS Create new user forms must be clearly marked with the users UUID number and the following secure steps taken:

All CIS Create new user forms must be filed securely in area that only RA staff have access to

Retained in accordance with Governance guidelines and policies

RA Asset Register

Equipment is not to be utilised until its details are recorded in the RA asset register. All RA equipment is to be listed in the RA asset register showing each make and model in use, the asset registers are broken down into different categories of equipment and each category can be subdivided.

The data items needed for each category should include the following details:

- Serial number
- Make and Model
- Issued to name
- Smartcard batches/numbers to be recorded
- Location

Damaged, Lost and Returned Items

RA equipment that is damaged, lost or returned as no longer required is to be listed in the RA asset register against the original equipment log entry.
Please see criteria below:

- Damage equipment, date of return, if sent for repair and when returned and re issued.
- Lost equipment/cards – date of loss, how reported and any incident issues recorded. RA staff to check that an incident form has been completed
- Returned items must be logged back into the system with all relevant paperwork to provide the necessary audit trail.

Implementation

It is the responsibility of the Information Governance Committee to support the implementation of this procedure within the RA Team through action planning, awareness raising and training.
The RA manager is responsible for ensuring RA staff are aware of this procedure and its implications and that a range of training methods will be considered in relation to identified needs.

Monitoring Compliance

Standards and Key Performance indicators

Health and Social Care Information Centre; Information Governance Toolkit:

- RA must assess their performance in information security and other areas of information governance using the toolkit and monitor progress and improvement.
- RA Manager to check that the RA assets register is updated each quarter by providing a report to the Information Governance Committee
- The Information Governance Committee to review the quarterly report in conjunction with the RA Manager and audits will be undertaken on a regular basis by the Information Governance Team.

Appendix 3: Document Control Sheet

This document control sheet, when presented to an approving committee must be completed in full to provide assurance to the approving committee.

Document Type	Policy		
Document Purpose	The purpose of this document is to provide guidance on the national obligations, roles and responsibilities of the Registration Authority (RA) and the Registration process to issue and update NHS Smartcards to Users.		
Consultation/ Peer Review:	Date:	Group/Individual	
List in right hand columns consultation groups and dates	09/04/19	RA Managers	
	13/06/19	Digital Delivery Group	
	18/06/2019	Information Governance Group	
Approving Committee:	Governance Committee	Date of Approval:	April 2013
Ratified at:	Trust Board	Date of Ratification:	N/April 2013
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)*	Not applicable	Financial Resource Impact	None
Equality Impact Assessment undertaken?	Yes [✓]	No [ ]	N/A [ ] Rationale:
Publication and Dissemination	Intranet [✓]	Internet [ ]	Staff Email [✓]
Master version held by:	Author [ ]	HealthAssure [✓]	
Implementation:	*Describe implementation plans below - to be delivered by the Author:*		
	Once approved, the policy will be communicated to all staff		
Monitoring and Compliance:	As per policy		

Document Change History:			
Version Number/Name of procedural document this supersedes	*Type of Change e.g. Review/Legislation*	*Date*	*Details of Change and approving group or Executive Lead (if done outside of the formal revision process)*
1.0		*Sept 2013*	*New document to replace former Humber Teaching Foundation Trust Registration Authority Procedures Pro 465 and the Legacy Policy from NHSERY Community Services Registration Authority Policy Pol 165*
1.1		*Oct 2013*	*Section re broken smartcards added and formatted as required as discussed Governance Committee 07/10/13*
1.2		*Mar 2016*	*Changes made to reflect new system, update to National RA Policy and Operating Guidance* *Section on Account Recovery Password removed*
1.3		*Jan 2017*	*Text on page 9 concerning staff not sharing smarts cards has been made bold.*
1.4		*Sept 2018*	*Update references to Data Protection Act 2018 and General Data Protection Regulation.*
1.5		*April 2019*	*Document reviewed and updated in line with review schedule*
1.6	*Review*	*June 2022*	*Document reviewed and minor amendments made.*

Appendix 4: Equality Impact Assessment (EIA)

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

1. Document or Process or Service Name: Registration Authority Policy
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? Policy

Main Aims of the Document, Process or Service
This policy sets out to provide guidance on 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 policy 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.

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
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 Registration Authority Policy does not impact on anyone with protected characteristics.	
EIA Reviewer: Sarah Fearnley	
Date completed: 24/06/2022	Signature: S. Fearnley