University Hospitals of Leicester NHS
NHS Trust

UHL REGISTRATION AUTHORITY LOCAL POLICY AND PROCEDURE

Approved By:	Policy and Guideline Committee
Date Approved:	16 February 2009
Trust Reference:	**B2/2009**
Version:	6.0
Supersedes:	5.0 – October 2021 Policy and Guideline Committee
Author / Originator(s):	Taff Webb, Registration Authority Manager
Name of Responsible Committee/Individual:	Andrew Furlong, Medical Director and Caldicott Guardian
Latest Review Date	17 May 2024 – Policy and Guideline Committee
Next Review Date:	November 2027

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

8 April 2024	Updated links. Changed name of CIS/CIS 2 to Care Identity Management (CIM). Amended contact information. Removed use of Temporary Smartcards	TW

KEY WORDS

Access, spine, Smartcard, Summary care record, login, authentication, identity, NHS Care Identity Management (CIM)

1. INTRODUCTION

1.1 This document sets out the University Hospitals of Leicester (UHL) NHS Trusts Policy and Procedures for access to Spine enabled applications as required for use by the Trust. The local Registration Authority manages this access.

1.2 The Spine is a collection of national applications, systems and directories that support the NHS in the exchange of information across national and local systems. It includes such applications as Summary Care Record and the Electronic Prescription Service.

1.3 The process of gaining access to spine enabled applications is called Registration. Once an applicant has been successfully registered they will have a User ID, pass-code and Smartcard. The primary method by which users then access applications is via the Smartcard issued during the registration process.

1.4 All spine enabled applications use a common security and confidentiality approach. Access to the appropriate applications and information is defined by the user's role, area of work and business function.

2. POLICY AIMS

2.1. This policy aims to ensure that the UHL Registration Authority (RA) performs all aspects of registration services and operations in accordance with National policies and procedures.

2.2. The RA will ensure tight control over the issue and maintenance of electronic Smartcards, whilst providing an efficient and responsive service that meets the needs of the users. It ensures that access to systems is only granted to staff who are approved to ensure that medical records are kept secure and confidential in line with the 'Care Records Guarantee'.

3. POLICY SCOPE

3.1. This policy and supporting procedures are applicable to all staff at UHL who need access to spine enabled systems.

3.2. Verification of identity for Registration applies the NHS Employment Check Standards to all prospective NHS job applicants and staff in NHS employment. This includes permanent staff, staff on fixed-term contracts, temporary staff, volunteers, students, trainees, contractors and agency staff. This includes IM&T Managed Business Partner personnel.

4. DEFINITIONS

4.1. **Care Identity Management (CIM)**

4.1.1. Care Identity Management is the electronic registration application that is used to perform Registration Authority activities.

4.2. **Care Record Guarantee**

4.2.1. Sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. It covers peoples access to their

own records, controls on others access, how it will be monitored and policed and access in emergency and if people cannot make decisions for themselves

4.3. **E Gif level 3**

4.3.1. E Gif level 3 defines the access controls to be applied to sensitive/personal information, broadly on the basis on the use of local user names and passwords, and the use of nationally managed electronic certificates and Personal Identification Numbers (PIN's).

4.4. **Position Based Access Controls (PBAC)**

4.4.1. Position Based Access Control defines the posts within an organisation that require spine application access and what the scope of that access is. Access requirements to a system are grouped into Access Control Positions based on the job that users are assigned to.

4.4.2. PBAC provides a simple and effective mechanism for providing users with the access they need in the course of their work and ensures greater consistency within NHS organisations about how access to care records is controlled and managed.

4.4.3. Analysis of access requirements is required when deploying new systems in the Trust i.e. who needs access and for what purpose.

4.5. **Registration Authority**

4.5.1. In Public Key Infrastructure terms there is a single Registration Authority – NHS England. All organisations that run a local Registration Authority undertake on a delegated authority basis from NHS England.

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

5. ROLES AND RESPONSIBILITIES

5.1. **The Executive Lead** for this policy is the Medical Director.

5.2. **The Caldicott Guardian (Medical Director)**

5.2.1. Accountable for the Registration Authority at UHL with overall responsibility for security of clinical and operational information.

5.2.2. Send notification of creation and revocation of RA Managers to NHS England.

5.3. **UHL Head of Privacy**

5.3.1. Oversee compliance with national and local governance requirements within UHL for RA mechanisms.

5.3.2. Ensure effective review of RA policies and procedures is completed as required.

5.3.3. Initiate and co-ordinate audits to ensure that all RA services comply with the Information Governance Framework.

5.3.4. Ensure UHL can maintain its RA obligations where inter-organisational agreements are in place.

5.3.5. Escalate breaches and report to the Caldicott Guardian.

5.4. **Registration Authority Manager**

5.4.1. This post is within UHL i.e. is not part of the IM&T Managed Business Partnership. The holder of this role is selected by the Executive nominated by the UHL Caldicott Guardian who is the UHL Medical Director

5.4.2. Efficient and timely day to day operation and capacity planning of RA services, ensuring that all RA procedures are carried out in accordance with local and national policy and processes. Disseminate national RA information to interested parties.

5.4.3. Assign, sponsor and register Advanced RA Agents and RA Agents, ensuring they are trained.

5.4.4. Carry out RA Agent tasks and maintain effective operational provision of RA at UHL, complying with eGIF Level 3 credential checking standards.

5.4.5. Ensure that only staff who meet the specified criteria are granted access to national spine enabled systems.

5.4.6. Ensure they have only one NHS smartcard issued to them and are aware of their responsibilities relating to information governance and smartcard use.

5.4.7. Ensure there is a process for the renewal of smartcard certificates

5.4.8. Maintain and store all registration and associated information in accordance with the Data Protection Act 2018 and national RA record retention policy.

5.4.9. Develop the Trust's RA Audit guidance and conduct annual audits of Smartcard usage. Report all RA related security incidents and breaches in accordance with Trust policy.

5.4.10. Escalate all queries that cannot be resolved locally to NHS England.

5.4.11. Ensure there is sufficient supply of smartcards and RA hardware including access to Care Identity Management for sponsors and communicate technical requirements to the UHL Design Authority.

5.4.12. Ensure users are aware of self-service functionality to unlock smartcards, reset passcodes and renew smartcard certificates available in CIM.

5.4.13. Ensure RA Managers contact details including email address and telephone number are recorded in the Spine User Directory.

5.4.14. Ensure sponsors are adequately trained and know how to unlock smartcards. Ensure sponsors are aware of the Organisational roles agreed for PBAC.

5.4.15. Maintain and publish the list of RA sponsors on INsite.

5.5. **Advanced RA Agent**

5.5.1. Ensure that national and local processes are followed to:

- Register and close Smartcard users, search and view closed users, Re-open closed users
- Cancel smartcards, Unlock smartcards and renew certificates
- Create and modify positions and workgroups, Modify positions, Assign individual to positions, Review positions definitions including assigned users
- Assign individuals to workgroups

- Manage request lists, Access reporting and run reports, Assign users to positions
- Use batch functionality
- View all requests

5.6. **RA Agent**

5.6.1. Maintain a list of active sponsors and any restrictions to assist the registration of users and RA processing

5.6.2. Ensure that national and local processes are followed.

5.6.3. Accurate input of information into Care Identity Management. Duties include

- Appropriate sponsorship has been applied
- Verification of the users identity
- Unlock a user's smartcard and reset passcodes

5.7. **RA Sponsors**

5.7.1. Ensure that application users are given the minimum appropriate level of access needed to perform their job

5.7.2. Utilise the Care Identity Management for registering, amending and deleting users of the RA smartcard service.

5.7.3. Approve registration and profiles to be granted to users (who can access what healthcare information) as defined by the UHL RA Policy

5.7.4. Be familiar with the different types of access profiles to approve and ensure that access profiles are appropriate.

5.7.5. Access profile change and removal, and the revocation of Smartcards and Smartcard certificates.

5.7.6. Appropriate (where confident of users identity), Passcode resetting, Smartcard certificate renewal and unlocking Smartcards and resetting passcodes.

5.7.7. Return Smartcards to the RA Office which have been reclaimed from staff leaving the NHS.

5.8. **Users**

5.8.1. Provide credentials to meet eGIF Level 3 standard and agree to abide by the RA Terms and Conditions concerning the care and use of Smartcards and operations of SCR applications.

5.8.2. Successfully complete eLearning or other training as directed prior to accessing applications.

5.8.3. Adhere to the Terms and Conditions of Smartcard use. Keep the smartcard secure and report lost/stolen cards to the RA office as soon as possible.

5.9. **IM&T**

5.9.1. Implementing RA changes and upgrades etc

5.9.2. Technical support for RA hardware/software environments in agreement with RA Manager.

5.10. **IM&T Change Team**

5.10.1. Recommend PBAC profiles to Clinical Risk Group for validation.

5.10.2. **UHL Information Governance Steering Group**

5.10.3. Approve appropriate PBAC profiles at UHL taking regard to risk of including/not including business functions within specific roles.

6. POLICY STATEMENTS, STANDARDS, PROCESSES, PROCEDURES AND ASSOCIATED DOCUMENTS

There are RA webpages on INsite which hold a list of current sponsors and guidance to users including terms and conditions.

http://insite.xuhl-tr.nhs.uk/homepage/clinical/clinical-systems-and-applications/registration-authority

There are Registration Authority offices at the three main hospital sites for UHL access management. Opening times are available on the Trust's RA Website page.

6.1. Establishing Identity to issue a Smartcard

6.1.1. New staff will have their identification verified and those credentials are then made available electronically as the national verified digital identity to RA Agents for card issuance. This removes the task of checking identification credentials from Sponsors, unless they carry out this task as interview on behalf of HR.

6.1.2. The only permissible identification documents are listed under *Identity checks* on the NHS employers website

6.1.3. An applicant must use the same name for registration as for their employment. 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.

6.1.4. The preferred name (different to the user's First Name and Family Name) will be printed on the smartcard. If a preferred name is being used, the RA must be assured that this is the name by which the individual is known. Additionally, the RA Manager may agree to the use of abbreviated names for front line staff where there may be a risk to the personal security of the user. In both instances the RA must update CIM.

6.1.5. Any changes to a users' name, date of birth or National Insurance Number. must go through the same face to face check with a person holding an RA role and provide appropriate documentary evidence.

6.1.6. A passport standard photograph is assigned to a user's profile and is printed on the smartcard. http://www.gov.uk/photos-for-passports. The photograph is imported into Care Identity Management and no local copies are kept.

6.2. NHS Smartcard Passcode

6.2.1. The NHS Smartcard Passcode is set only by the user during the registration meeting. It is entered by the user in conjunction with their NHS Smartcard to log on to the Spine.

6.2.2. Only the end user for whom the Smartcard is intended must know their passcode for their Smartcard, no-one else must, including RA staff. If anyone else knows the end users passcode it breaches the Smartcard terms and

conditions of use and Computer Misuse Act 1990. RA Staff and Sponsors are not permitted to assign a new user a temporary Passcode and/or login with the user's NHS Smartcard for any reason, including checking the viability of the NHS Smartcard.

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

6.2.4. Only the user must set and know their NHS Smartcard Passcode. The Passcode cannot be shared or disclosed to anyone else and must be a strong passcode. Since October 2023 the passcode needs to consist of between six to eight numbers.

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

6.2.6. To reset a user's Passcode, the NHS Smartcard must be locked in advance.

6.2.7. Users need to be assigned to an organisation code and position to enable them to log in with their NHS Smartcard. Once a user has been assigned a position, the RA will ensure that the user accesses the CIM application to electronically accept the Terms and Conditions of Smartcard use.

6.2.8. Users can use the NHS self service web application to unlock their smartcard as long as they have supplied an email address at Registration (this can be updated at any point). To unlock the user should access https://digital.nhs.uk/unlock .

6.3. Standards for use of Smartcards

6.3.1. All users including RA staff must have only one NHS Smartcard issued to them showing their Unique User Identify Number (UUID) and photograph. The organisation name will not be displayed. NHS Smartcards must be kept at all times with the user.

6.3.2. NHS Smartcards must not be shared.

6.3.3. Passcodes must not be shared.

6.3.4. The Smartcard must not remain in the Smartcard reader when the workstation is unattended by the user.

6.3.5. Users must sign the Terms and Conditions of Smartcard use. Disciplinary action may be taken where these are breached.

6.3.6. If the user suspects their Passcode has been compromised, the user must seek assistance from RA Staff to reset their passcode as soon as possible. This must also be reported to the UHL Service Desk.

6.3.7. Smartcards remain the property of NHS England.

6.4. Lost, Stolen and Damaged Cards

6.4.1. In the event a user has lost, damaged or had their Smartcard stolen, the user must report this immediately to the Registration Authority

6.4.2. The RA must meet the user face to face and confirm their identity by the users photograph in CIM. If the identity cannot be verified the user will be required to produce documentary evidence of their identity

6.4.3. The RA will cancel the lost, stolen or damaged NHS Smartcard and can issue a replacement.

6.4.4. For damaged cards, the RA will cancel the Smartcard, securely dispose of the card and can issue a replacement.

6.5. Staff leaving the organisation

6.5.1. Smartcards are transferable between NHS organisations and any individual leaving the UHL for another NHS post will have their UHL credentials revoked and will take their smartcard to their new organisation, where the appropriate credentials will be endorsed.

6.5.2. If a user leaves the NHS from UHL the smartcard will be retained and destroyed and all credentials for that user will be revoked.

6.6. Appointment of Registration Authority Managers

6.6.1. RA Managers are appointed by the Caldicott Guardian and this appointment is confirmed in a letter of appointment which must be held by each individual appointed to these positions. Copies of all appointment letters must be stored securely and available as necessary evidence to meet Data Protection and Security Toolkit requirements.

6.6.2. There will be a minimum of two individuals assigned to the RA Manager role for business continuity reasons.

6.7. Appointment of RA Sponsors

6.7.1. Sponsors are selected from Clinical Service Managers, Senior Managers of non-clinical departments, Ward Managers, Supervisory Staff and Managerial Staff. This appointment is confirmed in a letter of appointment which must be retained by each individual appointed to these positions.

6.7.2. All Sponsors are required to provide documentary evidence to prove their own identity meeting e-GIF level 3 credential checking standard. The areas of responsibility with respect to application user access will be clearly defined for each sponsor.

6.7.3. Sponsors are responsible for making sure that application users are given the minimum appropriate level of access needed to perform their job.

6.8. Incident Reporting

6.8.1. Incidents may be reported by any member of staff where they feel that there is a risk to patient health, confidentiality or UHL reputation. Incidents must be reported using the UHL Incident Procedure to the RA Manager.

Examples of incidents are:

- Smartcard or application misuse
- Smartcard theft
- Non-compliance of local or national RA policy
- Any unauthorised access to NCRS applications
- Any unauthorised alteration of patient data

6.8.2. Any incidents considered significant will be escalated to the UHL Caldicott Guardian, UHL Head of Privacy or Human Resources depending on the nature of the incident.

6.8.3. The Caldicott Guardian will consider incidents reported to them and decide on the appropriate action whether to escalate to the Trust Board or whether UHL systems of working practices must be reviewed as a result.

6.9. **Non-Availability of Systems**

6.9.1. Non availability of applications and systems will be notified to users via Email or on UHL's internet site. In the event of national systems not being available manual procedures will need to be followed and the spine updated when it becomes available at the soonest opportunity. These procedures will be defined by system managers for each application.

6.10. **Management of PBAC Profiles**

6.10.1. PBAC profiles are created by the UHL MBP Change Team and ratified by the UHL Chief Medical Information Officer, Chief Medical Nursing Officer and signed off by the Caldicott Guardian for each professional group.

6.10.2. Sponsors may need to allocate additional business functions to meet operational requirements. These will be agreed in collaboration with the MBP Change Team, RA Manager and ratified as 6.11.1 and forwarded to the Clinical Risk Group for validation.

6.10.3. Profile templates are available for operational roles on the Trust's RA Insite pages. The approval authority for each of the Trust's PBAC profiles is documented on CIM.

6.11. **RA Audit**

6.11.1. RA Managers are required to develop the organisations RA audit policy and conduct annual audits on NHS Smartcard usage.

6.11.2. UHL RA Authority will ensure that processes supporting the identification, registration and management of staff will be integrated with other UHL processes as appropriate.

6.11.3. All RA policies and procedures will be auditable by internal auditors as well as external auditors. Audits would typically cover:

- Issuance of Smartcards
- Management of Smartcards
- Profiles associated with users in relation to what they do
- Use of Smartcards
- Use of SCR applications
- Identity management
- Security of supplies and equipment

7. EDUCATION AND TRAINING REQUIREMENTS

7.1. Information governance training is mandatory for all UHL employees, training materials can be found on the UHL training website at https://uhlhelm.com/

7.2. The CIM system requires all users to undergo on line training modules designed around job profiles e.g. RA Manager, RA Agent. At the end of each training module the user has to undertake a test to prove efficiency before they can use the system.

8. PROCESS FOR MONITORING COMPLIANCE

POLICY MONITORING TABLE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements
Compliance with this policy	In-house Audit	Random Audit of implemented controls	Annually	UHL Audit Committee
Registration Authority processes to be monitored to detect non-compliance	Caldicott Guardian	CIM, Physical audit	Monitoring results must be reviewed on a regular basis as determined by the Caldicott Guardian	Information asset owners are responsible for monitoring their access control processes to detect non-compliance with this Policy and to record evidence in case of security incidents.
Audit on Smartcard usage	RA Manager	CIM	Annually	UHL Audit Committee

9 EQUALITY IMPACT ASSESSMENT

9.1. The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

9.2 As part of its development, this Policy and its impact on equality have been reviewed and no detriment was identified.

10 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

Principles of information security

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance

The NHS Confidentiality Code of Practice
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

NHS Employers website

https://www.nhsemployers.org/

National RA Policy:

https://digital.nhs.uk/services/registration-authorities-and-smartcards

Registration Authority INsite pages

UHL Information Security Policy A10/2003

https://digital.nhs.uk/services/registration-authorities-and-smartcards (includes link to NHS Care Record Guarantee)

http://insite.xuhl-tr.nhs.uk/homepage/clinical/clinical-systems-and-applications/registration-authority/ra-help-for-staff/about-smartcards List of systems that require NHS Smartcards

11 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

The updated version of the Policy will be uploaded and available through INsite Documents. It will be archived through the Trusts SharePoint system

This Policy will be reviewed every three years

Contacts & Assistance

For information and guidance on the implementation of this policy, contact:

- The IM&T Service Desk on x18000
- Service Delivery & Transition Manager/RA Manager: taff.webb@uhl-tr.nhs.uk
- Deputy RA Manager: bryan.morgan@uhl-tr.nhs.uk
- Head of Privacy: saiful.choudhury@uhl-tr.nhs.uk