Shropshire Community Health NHS Trust

# Local Registration Authority (Smartcards) Policy

**Controlled document**

**This document is uncontrolled when downloaded or printed**

| | |
|---|---|
| **Author(s)**<br>**Owner(s)** | Author: Gill Richards, Head of Information Governance/RAM and Tracy Jenkins, IG Compliance Officer/RAM<br>Owner: Gill Richards, Head of Information Governance |
| **Version No.** | Version 2.1 |
| **Approval Date** | June 2023 |
| **Review Date** | June 2026 |

| Document Details | |
|---|---|
| **Title** | Local Registration Authority (Smartcards) Policy |
| Trust Ref No | |
| Local Ref (optional) | 2.1 |
| Main points the document covers | Aims to ensure SCHT complies with the requirements of the National Registration Authority Policy. |
| Who is the document aimed at? | This policy is aimed at all staff |
| Author | Head of Information Governance |
| **Approval process** | |
| Who has been consulted in the development of this policy ? | Selection of managers/staff |
| Approved by (Committee/Director) | Data Security and Protection Assurance Group |
| Approval Date | 16 June 2023 |
| Initial Equality Impact Screening | |
| Full Equality Impact Assessment | |
| Lead Director | Director of Governance/Senior Information Risk Owner (SIRO) |
| Category | General |
| Sub Category | Information Governance |
| Review date | June 2026 |
| **Distribution** | |
| Who the policy will be distributed to | The Head of IG will submit this document to the Risk Management Team for publication on the Trust Websites<br>The IG Team will notify all Trust Staff of the publication of this policy |
| Method | Websites and email |
| Keywords | RA Policy, Smartcards, System Access |
| **Document Links** | |
| Required by CQC | Yes – Well Led |
| Other | |
| **Amendments History** | |
| No / Date | Amendment |

| | | |
|---|---|---|
| 1 | 21/04/2023 | Update Author – IG Manager to Head of Information Governance, Director of Finance to Director of Governance<br><br>IAO description amended |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

**This copy is uncontrolled unless printed on 'Controlled' paper.**

# CONTENTS

1. Purpose ..... 5
2. Scope ..... 5
3. Introduction ..... 5
4. Governance ..... 7
5. Roles and Responsibilities ..... 7
6. Authentication Token Use ..... 8
7. Temporary Access Cards (TACs) ..... 8
8. Replacement Cards (Lost/Stolen/Damaged) ..... 9
9. Position Based Access Control (PBAC) and Access Control Positions (ACPs) ..... 9
10. New Starters (including non-employed workers) ..... 9
11. Leavers (including non-employed workers) ..... 10
12. Identity Verification ..... 10
13. Additional Smartcard Configuration ..... 10
14. Incident Reporting ..... 11
15. Monitoring and Auditing ..... 11
16. Training ..... 11
17. Confidentiality ..... 11
18. Future Developments ..... 12
19. Related Document ..... 12

**Appendix 1 Local RA Operational and Process Guidance** ..... 13

# 1. Purpose

1.1 It is the policy of the Shropshire Community Health NHS Trust to ensure that the approach to data protection and security is met as follows:

- the Trust adheres to and complies with the National Registration Authority Policy, the Data Security and Protection Toolkit (DSPT) and the Data Protection laws
- the Registration process for the national Care Identity Service (CIS) must meet the current Government requirements. Such applications must use a common security and confidentiality approach. This is based upon the Users, the organisation and position
- that appropriate steps are taken to investigate incidents
- takes full advantage of existing authority and responsibility structures where these are fit for this purpose
- associated tasks with appropriate management levels
- avoids unnecessary impacts on day-to-day business
- ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner

# 2. Scope

2.1 This policy relates to all Shropshire Community Health NHS Trust systems that are Smartcard enabled, both clinical and corporate, such as the Electronic Patient Record (Rio) and the Electronic Staff Record (ESR).

2.2 This policy applies to all Trust staff (including non-employed workers (agency, locums, students, contracted from other organisations) who require access to national applications which are Smartcard controlled and are working in Shropshire Community Health NHS Trust.

# 3. Introduction

3.1 This policy relates to managing access to personal confidential data (PCD) held systems within Shropshire Community Health NHS Trust.

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

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

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

3.5 The Trust has implemented the Integrated Identity Management (IIM) which combines the processes within Registration Authority and Human Resources for capturing and managing employee identity. The ESR interface to CIS can be used to automatically update an individual's access rights to Spine compliant systems, reflecting the requirements of their new position. It enables the management of access control via a single point of data – the change to the employee's position in ESR.

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

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

3.8 Coordinating recruitment, HR and RA procedures via the interface supports the facilitation of issuing an NHS Smartcard during the initial induction period for new staff, enabling them to participate effectively from the start of their employment.

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

- A user is identified for an NHS Smartcard – this can be via an individual (sponsor) explicitly requesting the individual be registered in CIS or other means such as employment into a role or requirements of a job changing
- The user provides appropriate identification as per NHS Employers Identity Check standards to ensure their identity is verified and recorded to e-GIF Level 3.
- 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.
- An 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.

# 4. Governance

4.1 **Executive Management Team (EMT):** The accountable personal is Senior Information Risk Owner (SIRO) currently the Director of Governance. The SIRO has overall accountability in the organisation for RA activity. The responsible individual must report annually to the organisation on this activity.

4.2 **Registration Authority Manager (RAM):** The EMT has appointed the Head of Information Governance and Information Governance Compliance Officer to carry out this role supported by the Information Governance Team Leads. The RAM is responsible and accountable for the running of RA activity and governance in the Trust. The RAM is responsible for setting up the systems and processes that ensure that the local policy and processes meet the national requirements.

4.3 **Executive Sponsor:** The Associate Director for Workforce and Planning has been appointed to this role. The Executive Sponsor is the individual appointed by the Executive Management Team who is authorised to request and approve those digital identities be created and appropriate and specific access assigned to staff within the organisation. This is administered under the authorised combined RA and HR processes for capturing and managing employee identity.

4.4 **Privacy officers:** In accordance with the NHS National guidance on viewing the Summary Care Record (SCR) the Trust must appoint a Privacy Officer (PO).
The Trust has appointed the Medical Director as the Privacy Officer. The PO has the appropriate access assigned to their Smartcard so that they can access the Alert Viewer on the Spine and check whether SCR views were legitimate. For alerts where the clinician has self- claimed a legitimate relationship, the PO will confirm that the patient was being treated at the organisation by looking at the Patient Administration System or another record of patient attendance.
The RAAs will monitor the Alerts in accordance with the national SCR guidance and Reconciliation Tool process.

4.5 **Managing Access:** User access will be managed in accordance with the local & national RA Operational and Process Guidance and the Data Security and Protection Toolkit (DSPT). This includes monitoring and auditing compliance, alerts e.g. SCR Privacy Officer Alerts, CIS end dates.

4.6 **Processes and Procedures:** The Trust's processes and procedures are set out in the Local RA Operational and Processes Guidance (Appendix 1) and are held in SharePoint.

# 5. Roles and Responsibilities

5.1 **Registration Authority Manager (RAM)** means an individual appointed by the Executive Management Team of an organisation to set up and run the organisations Registration Authority processes and procedures. In addition, they are responsible

for ensuring good governance and report annually to the organisation's EMT on RA activity. In addition, they are required to undertake appropriate training to discharge these responsibilities and arrange training for all other RA team members. They are also authorised to undertake identity verification, identity creation, creation and assignment of authorisation tokens and assign access rights to a user. In the Trust this role is carried out by the Head of Information Governance/Information Governance Compliance Officer.

5.2 **Registration Authority Agent (RAA)** means an individual who has undertaken appropriate training who is authorised to undertake identity verification, identity creation, creation and assignment of authorisation tokens and assign access rights to a user. In addition, they can perform a range of administrative tasks to maintain good RA records and processes. In the Trust this role is carried out by the Information Governance Team.

5.3 **Registration Authority Agent ID Checker** means an individual who has undertaken appropriate training who is authorised to undertake identity verification and identity creation. In the Trust this role is carried out by the Information Governance Team, Electronic Staff Record Team and the Recruitment Team.

5.4 The role of the **Information Asset Owner (IAO)** will be assigned to staff that hold the position of Deputy/Associate Director, Head of Department, Service Delivery Group Manager. The IAOs will be accountable to the Senior Information Risk Owner SIRO); and will have delegated responsibility from the SIRO to oversee and support the information risk management framework within their respective areas. The role will support the SIRO in fostering a culture that values, protects and uses information for the benefit of patients, service users, employees and the Trust as whole.

5.5 The Information Asset Owner may nominate an **Information Asset Administrator (IAA)** and delegate the day-to-day responsibility of the information asset. The IAO will nominate an appropriate person to undertake the role of Data Protection Liaison Officer (DPLO).

## 6. Authentication Token Use

6.1 **Authentication Token** means Physical Smartcards, Virtual Smartcards, Authorised Devices and iPad Devices which enable healthcare professionals to access clinical and personal information appropriate to their role and the type of Identity Solution.

Authentication Tokens 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.

## 7. Temporary Access Cards (TACs)

7.1 **Temporary Access Cards (TACs)** will be issued in an emergency e.g. damaged, lost or stolen, or access for an Agency Worker, staff must follow the Trust process to administer and issue the TAC. The process is set out in the Trust's Local RA

Operational and Process Guidance. Nominated Custodians throughout the Trust (based at Trust "Hub" sites – geographically located) administer the TAC process.

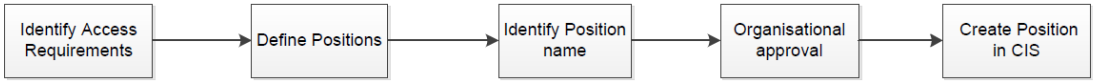
## 8. Replacement Cards (Lost/Stolen/Damaged)

8.1 A replacement smartcard can be request via the Digital Service Self-Service Portal / via the RA Mailbox – the Incident Report Datix number will be required.

## 9. Position Based Access Control (PBAC) and Access Control Positions (ACPs)

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

PBAC process




9.2 **Access Control Positions (ACPs)** are created to ensure that Users have the appropriate level of access for the role that they are employed to do in the Trust e.g. a Nurse, Receptionist, Administrator. They are developed by the Information Governance Team in conjunction with system configuration teams, such as Rio. They are then approved by the Caldicott Guardian and ratified by through the Information Governance Framework. Any queries regarding access rights should be directed to shropcom.raadmin@nhs.net

9.3 An ACP is assigned to a User's Smartcard as part of the Trust's recruitment process for employed and non-employed workers. Access is assigned through the CIS-ESR Interface or, occasionally directly through CIS in emergency situations i.e. during pandemic.

## 10. New Starters (including non-employed workers)

10.1 Staff are recruited through the HR Process and Line Managers should ensure that all relevant documentation is in place as this will activate the process for the printing and issuing of a Smartcard. The process is set out in the Trust's Local RA Operational and Process Guidance.

# 11. Leavers (including non-employed workers)

11.1 Line Managers should ensure that all relevant documentation is in place with regards to the termination of employment as this will activate the process for revoking the Smartcard access rights. The process is set out in the Trust's Local RA Operational and Process Guidance.

# 12. Identity Verification

12.1 NHS Digital's strategic aim is to create a single, non-repudiated, trusted, digital identity for healthcare workers. This will be pivotal to enabling national access to health information in a secure way.

12.2 The Trust is required to achieve the identity verification standard set out in the National Cyber Security Centre Good Practice Guide 45 (GPG45) – 'Identity Proofing and Verification of an Individual'. This provides assurance that the identity is valid across any organisation an individual works within.

12.3 The documents that can be used to verify an identity have been jointly determined by NHS Digital and NHS Employers and the list is contained in the NHS Employers 'Verification of Identity Checks' standard which can currently be found at www.nhsemployers.org/your-workforce/recruit/employment-checks/identity-checks

12.4 RA roles responsible in the creation of a digital identity are effectively trained to do so and adhere to the identification documentation guidelines set out in the NHS Employers guidance. Staff undertaking RA roles must verify User's identity to e-GIF level 3 standard when they register Users.

# 13. Additional Smartcard Configuration

13.1 Assigning access involves a number of work-streams that must be co-ordinated and completed to ensure that the User's Smartcards is fully activated, including:

- HR Team – recruitment process
- Smartcard Team – printing and issuing the card
- Rio Configuration Team – the User will need to set up, configured and activated
- IT Team – PC log in access

13.2 For non-Smartcard enabled systems the User access is assigned by the Information Asset Administrator (IAA). Approved and pre-defined role-based access controls for all systems are in place. The Service Manager will act as sponsor and authorise assignment of access.

## 14. Incident Reporting

14.1 Staff must comply with the Trust's Incident Reporting Policy and report any incident related to system access, Smartcards and usage, such as unauthorised or inappropriate access, sharing Smartcards and passwords that may have been compromised. Incident Report Datix number will be required for any Lost Smartcards.

## 15. Monitoring and Auditing

15.1. The Information Governance Team will conduct a monitoring and auditing programme on an annual basis in accordance with the national and local RA Operational and Process Guidance, and the Data Security and Protection Toolkit (DSPT). The programme of work will be set out and approved by the Data Security and Protection Assurance Group.

15.2 Spot checks will take place to monitor compliance. This programme of work will be set out by the Information Governance Team and approved by the Head of Information Governance.

## 16. Training

16.1 The RAM will ensure that all staff who undertake a role within the scope of the RA activity are fully trained, such as RA Agents, RA Agent Identity Checkers.

16.2 All staff must complete current Information Governance Mandatory Training (Data Security Level 1) in a timely way. The Information Governance Team will monitor compliance and liaise with Line Managers. Access may be revoked if the IG training is not completed in a timely way.

16.3 All staff that have access to Trust systems must receive appropriate training from the Information Asset Owner/Information Asset Administrator in a timely way before access is assigned to their Smartcard, such as Rio, ESR.

## 17. Confidentiality

17.1 New employees must sign the Trust's Confidentiality Form under the terms of employment**.**

17.2 All non-employed workers must sign the Trust's Confidentiality Form when working in the Trust this should form part of the Local Induction managed and monitored by their Line Manager.

17.3 Staff must understand the term “legitimate relationship” - a relationship that exists between health and care professionals and non-clinical staff who have a legitimate relationship with the patient or service user, providing or supporting their care, will have access to their record.

## 18. Future Developments

18.1 The Trust will continue to explore the use of products and functionality in accordance with the Identity Agent Management (IAM) Roadmap and national RA Team. The Trust will consider the deployment of new products and functionality when available and when technical and financially feasible.

For example, Virtual Smartcard - a solution that provides access functionality, but the card itself may be stored on a device, approved for use by NHS Digital and or its partners.

## 19. Related Document

Data Protection Policy

Information Security Policy

Information Risk Policy

Data Quality Policy

Records and Document Management Policy

Clinical Record Keeping Policy

# Appendix 1 Local RA Operational and Process Guidance

The following is a list of guidance that has been developed by the Information Governance Team, this list is not exhaustive.

- Joiners (New Starters) including employees, non-employed and redeployed workers
- Movers (those moving within the Trust)
- Leavers including employees, non-employed and redeployed workers
- Temporary Access Cards (TACs)
- Identity Checks (following NHS employer's guidance)
- Change of Personal Details and Photo
- Acceptable Photo Guidance
- Replacement Smartcards (Lost/Stolen/damaged)
- Position Based Access Control Approval Panel
- Registering RA Equipment and Consumables
- Care Identity Service End Dates
- Duplicate Smartcards
- User Suspension