NHS
Doncaster and Bassetlaw
Teaching Hospitals
NHS Foundation Trust

Registration Authority Policy
for the
Management and Issue of Smartcards

This procedural document supersedes: CORP/ICT 19 v.3 - Registration Authority Policy for the Management and Issue of Smartcards & CORP/ICT 18 v.3 – Registration Authority Strategy

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, <u>it is only valid for 24 hours.</u>**

Executive Sponsor(s):	Chief Information Officer (CIO) & Senior Information Risk Owner (SIRO)
Name and Title of author/reviewers	Roy G Underwood, Information Governance Manager Jo Hall – IT Ops ICT Support Supervisor David Linacre – IT Ops Security & Continuity Manager
Date revised	March 2021
Approved by (Committee/Group)	Information Governance Committee
Date of approval	26 April 2021
Date issued	21 May 2021
Next review date	April 2024
Target Audience	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
Version 4	21 May 2021	• Tri-annual review • Amended to accommodate the UK GDPR & the latest innovations within the Care ID System (CIS)	Jo Hall David Linacre Roy Underwood
Version 3	June 2016	• Tri-annual review • Amended to accommodate the new Care ID System (CIS) rationale	Roy Underwood
Version 2	November 2011	• Tri-annual review • Integrated & User Identity Management (IIIM & UIM) • Approval by the Information Governance Team	Roy Underwood

Contents

Page No.

1. INTRODUCTION

1.1 Rationale

Authorised end-users will access many NHS applications using electronic Smartcards. A national system for registering end-users of applications is well established, comprising a hierarchy of Registration Authorities that culminates in the devolution of responsibility for authorising and registering individual staff as end-users to their employing authority. Accordingly the Trust is required to set-up a Registration Authority of its own to undertake this function.

1.2 RA Governance

Details of the policy framework for registering users for NHS national (Spine) services, the requirements for organisations to establish RAs for the governance of registration, and the responsibilities of RAs were published in the DH document Registration Authorities: Governance Arrangements for NHS Organisations - Gateway Reference 6244 (PDF, 37.6kB). This answers the question, "Why do we have to have a Registration Authority".

Information governance (IG) is an integral part of NHSD service delivery and it is embedded within all its programmes. It is important that organisations protect patient confidentiality and rigorous registration and access control can help support a consistent and high quality audit framework. All NHS organisations are required to have a RA, as part of their overall IG arrangements. Therefore, RA should be seen as embedded in IG, not separate from it.

A RA is the governance framework within which organisations register individuals as users of the NHS national services, in order to maintain the confidentiality and security of patient and service user information at all times. Having a common and rigorous approach to how users are registered and are given access to national services is an integral part of protecting the confidentiality and security of every patient's and services user's personal health and care details.

Registration is the process by which users of Smartcard-enabled IT applications are authorised (enabled to have particular levels of access to particular patient and service user data) and authenticated (proved who they are beyond reasonable doubt for each access session).

1.3 Scope

The Trust Registration Authority Policy will apply to all processes, procedures and activities carried out by the Registration Authority and staff members who are authorised by the Registration Authority to access National & Local Smartcard associated applications.

1.4 Principles

The following principles apply:

- The Trust is required to ensure that all National Policy requirements of Registration Authorities are met and maintained.
- The Registration Authority is a vital aspect of information governance for the Trust since its primary responsibility is to maintain confidentiality of service user personal data.
- The only way the Trust can use National & Local Smartcard associated applications is through staff who are duly registered through the registration authority.

The Trust will base its policy on:

- NHSD Registration Authority Guidance: https://digital.nhs.uk/services/registration-authorities-and-smartcards

2. THE REGISTRATION AUTHORITY

A Registration Authority (RA) has been established by the Trust with the following remit, where it will:

- Ensure that the National Registration Authority processes are adhered to in full, including undertaking regular audits of processes and procedures.
- Ensure that any local processes developed to support the National Registration processes are adhered to in full and are integrated with other local workforce registration policies.
- Ensure that resources are available to operate the registration processes in a timely and efficient manner to meet the Trust's organisational requirements.
- Ensure that the RA team members are adequately trained and familiar with the local and national RA processes.
- Ensure that an indexed and secure audit trail is maintained of applicants' registration information and profile changes[1].
- Ensure that all completed application forms and associated documents are kept secure in an area to which the RA and human resources teams have access. (NB: RA records need to be retained for 25 years.)
- Ensure RA members are familiar with and understand "Registration Policy and Practices for Level 3 Authentications - NPFIT-NCR-DES-0294.02"[1].
- Notify the national Registration Authority of the creation and revocation of RA managers[2].
- Ensure that there are sufficient Smartcards and Smartcard issuing and maintenance equipment to meet the requirements of the Trust.
- Define criteria for selecting and deselecting Sponsors.

[1] All RA Documentation is either held securely on paper (for historical and pre-CIS records) or within the CIS System itself by local RA Agents in their Divisional or Corporate location.

[2] RA Managers must be sponsored by the Trust CEO or the Caldicott Guardian.

Appoint Sponsors in line with defined criteria:

- Define, agree and establish appropriate working relationships with partner organisations.
- Communicate operational service level issues to appropriate RA staff and the user community, notified by NHSD.
- Define and identify local Job Roles, Areas of Work and Business Functions in line with national definitions and notify these to relevant authorities within the Cluster
- Monitor the performance of RA systems and processes, making improvements where required.

3. IMPLEMENTATION AND COMPLIANCE

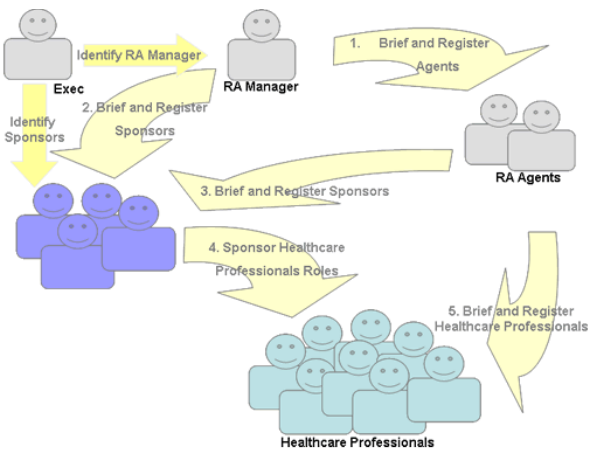
3.1 Key Registration Authority Roles – see also Appendix 1 for ToR's

The key roles and responsibilities within the Registration Authority are as follows:

Role Responsibilities

RA Manager - The RA Manager is responsible – through the Head of Information Governance & the Information Governance Committee - to the Trust Board, the CEO and the Caldicott Guardian for ensuring that the required Registration Authority processes and procedures are in place and adhered to. The role will be undertaken by the IT Service Desk Manager.

People involved in the registration process


Identify RA Manager
Exec
RA Manager
1. Brief and Register Agents
2. Brief and Register Sponsors
Identify Sponsors
RA Agents
3. Brief and Register Sponsors
4. Sponsor Healthcare Professionals Roles
5. Brief and Register Healthcare Professionals
Healthcare Professionals

RA CIS Agent(s) - RA Agents are primarily responsible for registering users and issuing Smartcards. The RA Manager may also act as an RA Agent.

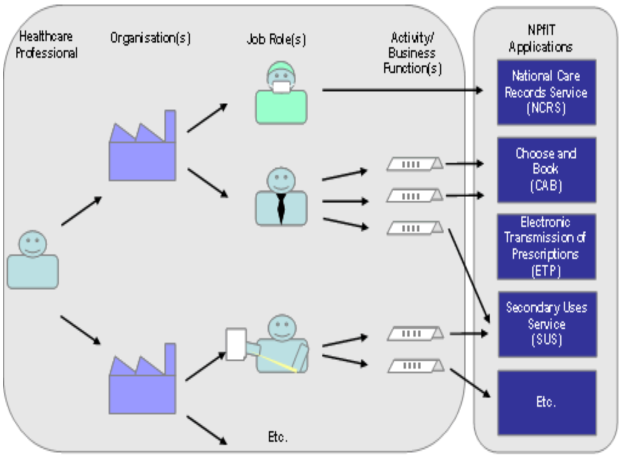
User Registration Sponsors - A Sponsor will typically be a senior manager to whom the user reports directly or indirectly. Sponsors have three key responsibilities:

Role Responsibilities (referred to as Sponsors hereafter)

1. Determine which National or Local Smartcard associated applications and therefore which Position Based Access (PBAC) role a member of staff is to be given (Sponsored) as a basis for their registration as an end-user.

2. A Sponsor will vouch for a user's identity.

3. An RA Sponsor or an Agent may unlock a user's Smartcard if that user forgets their pass-code.


Healthcare Professional
Organisation(s)
Job Role(s)
Activity/ Business Function(s)
NPfIT Applications
National Care Records Service (NCRS)
Choose and Book (CAB)
Electronic Transmission of Prescriptions (ETP)
Secondary Uses Service (SUS)
Etc.
Etc.

With the implementation of CIS and its 'paperless/paper-light' intention, staff with the RA Sponsor activity will have to work in parallel with their RA Agents. Many of the historical (Calendra/UIM) RA Management processes required actions by two unique individuals (a Sponsor and an Agent), however some staff enjoyed and continue to enjoy both Roles within the CIS. Where they Users are sponsored through the historical RA01 form, the CIS application itself, or an email of authority from a registered RA Sponsor, then those records should be kept safe and secure by individual Divisional & Corporate RA Agents for audit and monitoring purposes in line with Trust records management policy[3]

Sponsors will authorise their Agents and vice versa electronically to aid this cumbersome administrative process, provided they are properly authorised by their Divisional or Corporate Directorate Management.

Application end-users
The key responsibilities for application end-users are as follows:

1. Keep their pass-codes secret and not share them with anyone, including colleagues.
2. Always have their Smartcard available when required and to take reasonable steps to protect it from misuse.
3. Not to share login sessions with other users. In practice this will require logging in and out at the start and end of each session.

Full details of the end-user's responsibilities are listed in the conditions on the initial RA01 registration forms and end-users must sign up to Terms & Conditions (electronically) when prompted to do so by the Care ID System.

3.2 Registration Authority Reporting Group

The Registration Authority will report directly to the Information Governance Committee (IGC), as an integral element of the Information Governance Assurance Framework, which is chaired by the Head of Information Governance/DPO within the IGC Terms of Reference approved by the Trust. (See APPENDIX 1).

3.3 Corporate Oversight

The Caldicott Guardian, on behalf of the Chief Executive, will take steps to ensure that all registered staff adhere to this Policy. A failure to adhere to this Policy may result in disciplinary action.

3.4 Training

The Registration Authority CIS itself provides intuitive training opportunities and self-help guides.

[3] CORP/ICT 14: Information Records Management - Code of Practice (NHSD CoP 2016)

3.5 RA Support

In the first instance through local RA Agents. If they cannot solve the problem, then calls should be logged with the IT Service Desk at dbth.it.servicedesk@nhs.net or Ext 644190.

4. REFERENCE DOCUMENTS

1. Registration Authorities Operational and Process Guidance https://digital.nhs.uk/services/registration-authorities-and-smartcards
2. Registration Authorities historical RA Forms
   a. RA01 Short Form & Conditions
   b. RA01 New User Registration Form
   c. RA02 Form – User Profile and Profile modification
   d. RA03 Form – Request to cancel Smartcard or revoke certificates; and re-issue Smartcard
   e. RA04 Form – Interim Fallback Smartcard Solution
   f. RA05 Form – Change of Details

The CIS has an inbuilt audit trail not requiring the use of paper forms, however the Trust has agreed that the RA01 forms may continue to be used and held for local admin and audit purposes. Where RA Agents opt to do this, then those documents should be held for a period of 18 months.

5. DISTRIBUTION

This Policy will be available through the Trust APD[4] Management Process, including the Trust's Extranet.

6. MONITORING

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
End Users – Are all leavers checked against an active RP5 Position	RA Manager	As required by the staff leaver lists	IG Committee
Sufficient RA Agent Provision and Training	RA Manager	3 monthly using MS Forms	IG Committee

[4] APD – Approved Procedural Documents

7. REVIEW

This Policy will be reviewed tri-annually or when required by changes in national policy.

8. TRAINING & SUPPORT

Training & Support is facilitated 'on-line' within the CIS itself, with further operational guidance through the RA Webpages which can be found on the Trust Extranet.

9. ASSOCIATED TRUST PROCEDUREAL DOCUMENTS

- CORP/ICT 2 – Information Management and Technology (IM&T) Security Policy
- CORP/ICT 7– Data Protection Policy
- CORP/ICT 9 – Information Governance Policy
- CORP/ICT 10 – Confidentiality Code of Conduct
- CORP/ICT 11 – Information and Communications Technology (ICT) Business Continuity Policy
- CORP/ICT 14 – Information Records Management – Code of Practice
- CORP/ICT 21 – Information Risk Management Policy

10. DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

11. EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment For All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 2)

APPENDIX 1 - REGISTRATION AUTHORITY MANAGEMENT TEAM – TERMS OF REFERENCE

REGISTRATION AUTHORITY MANAGEMENT TEAM – TERMS OF REFERENCE

The Trust is required to set up a Registration Authority (RA) to register and authorise users of the computer applications that were either derived from the historical National Programme for IT (NPfIT), or which have been purchased directly by the Trust. The requirements, management structure and detailed roles and responsibilities are described in the Trust's Registration Authority Policy.

The policy requires the RA to be managed on a day-to-day basis by the RA Management Team with a remit outlined in this Policy.

The RA Policy and trust Extranet pages reflect the 'split' responsibilities for:

- RA Smartcard Management across the Divisions and Departments under the RA Manager
- RA/IT Technical Infrastructure under the Head of IT Services

REMIT

The requirements of a local Registration Authority are defined in the NHSD documents identified in Section 4. Registration Authority Management will be under the direct control of the Trust Information Governance Group (IGG), based on national policy and guidance will be as follows:

- Ensure that the National Registration Authority processes are adhered to in full, including undertaking regular audits of processes and procedures.
- Ensure that any local processes developed to support the National Registration processes are adhered to in full and are integrated with other local workforce registration policies.
- Ensure that resources are available to operate the registration processes in a timely and efficient manner to meet the Trust's organisational requirements.
- Ensure that the RA team members are adequately trained and familiar with the local and national RA processes.
- Ensure that an indexed and secure audit trail is maintained of applicants' registration information and profile changes.

- Ensure that all CIS completed application forms and associated documents are kept secure in an area to which the RA Management Team have access. (NB: RA records generated under Calendra and UIM need to be retained for 25 years.) Where Divisions or departmental RA Sponsors and Agents choose to use the catalogue of RA forms, then those forms need to be held for a minimum of 18 months.

- Ensure RA members are familiar with and understand the Registration Policy and Practices for eGIF Level 3 Authentication.

- Notify the national Registration Authority of the creation and revocation of RA managers.

- Ensure that there are sufficient Smartcards and Smartcard Printers and maintenance equipment to meet the requirements of the Trust.

Define criteria for selecting and deselecting Sponsors

- Appoint Sponsors in line with defined criteria:

- Define, agree and establish appropriate working relationships with partner organisations.

- Communicate operational service level issues to appropriate RA staff and the user community, notified by NHSD.

- Sponsors/ Project Leads will define and identify local RBAC Job Roles & Activities, Areas of Work and Business Functions in conjunction with the Trust RA Manager, and in line with national definitions.

- Monitor the performance of RA systems and processes, making improvements where required.

MEETINGS

The RA Management Team will report to the Caldicott Guardian through the Information Governance Committee agenda.

APPENDIX 2 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
RA Policy – CORP/ICT 19 v.4	Digital Transformation	Jo Hall / Roy Underwood	Existing Policy	19/03/2021

1) **Who is responsible for this policy?** Name of Division: Digital Transformation

2) **Describe the purpose of the service / function / policy / project/ strategy?** All RA Smartcard users

3) **Are there any associated objectives?** NHSD & National eGIF Systems Access Controls

4) **What factors contribute or detract from achieving intended outcomes? None compliance**

5) **Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief?** No

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation]

6) **Is there any scope for new measures which would promote equality?** [any actions to be taken

7) **Are any of the following groups adversely affected by the policy?**

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) **Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box**

Outcome 1 ✓	**Outcome 2**	**Outcome 3**	**Outcome 4**

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form in Appendix 4

Date for next review: **April 2024**

Checked by: Jo Hall **Date:** March 2021