South East Coast Ambulance Service NHS Foundation Trust

Registration Authority Policy

Contents

1. Introduction

1.1. The national Registration Authority is the overall controlling body for the issue and management of Smartcards which enable NHS employees to access the Care Records Service (CRS) and other national clinical applications as part of NHS Digital The CRS is an interactive patient record service being phased in across England which will be accessible by healthcare professionals twenty-four hours a day, seven days a week. It will also provide access for patients to key information in their medical record.

1.2. Responsibility for access to the systems for local healthcare professionals and other users has been devolved to local Registration Authorities set up within the Trust. These operate within a set of policies and guidelines set out at national level and it is the responsibility of each local Registration Authority to define clearly how they will implement and manage their Smartcard operations in order to ensure adherence.

1.3. All healthcare professionals will have their access profile approved by a sponsor assigned by the Trust Management Team.

1.4. The protection of clinical data is a major issue for all Trust staff and a robust authentication system has therefore been developed to ensure that users gain access only to the information they are entitled to use, and that everyone having access to patient information has been through the same rigorous identity checks before access is granted.

1.5. The NHS is obliged to provide the same level of protection to staff information as it does to its patients' personal details. To this end, some users requiring access to the Electronic Staff Record (ESR) may need to be issued with an NHS CRS Smartcard. This is dependent on the type of access which is required.

1.6. ESR Self Service offers individuals the facility to update some of their information using a unique password and without the need for a smartcard. This include address / contact details, telephone numbers and payment information.

2. Aims and Objectives

2.1. This policy applies to all South East Coast Ambulance Service NHS Trust ('the Trust') employees and other staff granted access, who use Smartcards when accessing CRS, NHS Spine and ESR applications.

2.2. The Trust is responsible for registering all users including non-NHS staff, to ensure adequate safeguards are in place to maintain the confidentiality of information held on individual patients and staff.

- Sponsors of Smartcard users.
- Smartcard issue, updating, cancellation, expiry, loss and security processes.
- The Spine and card management system.
- Hours of operation.
- Controls.

3. Definitions

3.1. **The following terms and abbreviations are used in the document:**

3.1.1. **E-GIF** - The e-Government Interoperability Framework sets out the government's technical policies and specifications for achieving interoperability and Information and Communication Technology (ICT) systems coherence across the public sector. The e-GIF defines the essential prerequisites for joined-up and web-enabled government.

3.1.2. **ESR** – Electronic Staff Record is the primary system procured by the Department of Health to manage all Human Resources and Payroll functions across the NHS

3.1.3. NHS Digital - NHS Digital

3.1.4. **NHS Spine** - The NHS Spine is a national system which holds patient information. This is predominantly Summary Care Record (SCR) and Patient Demographic Service (PDS)

3.1.5. **RA -** Registration Authority

3.1.6. **RA Manager** - Responsible for providing a comprehensive RA service and governance of RA in the organisation. They are also responsible for registering RA staff in their own organisations and any RA Managers in child organisations. They are also responsible for ensuring the effective training of RA Agents and Sponsors within their organisation.

3.1.7. New roles have been created in the Registration Authority software, Care Identity Services, 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.

3.1.8. **RA Sponsor** - Responsible for nominating users of the systems requiring Smartcard access and assigning the appropriate level of access. **This includes:**

- Can raise requests for new users
- Approve users assignment to access control positions, or,
- Directly assign users under position management
- Unlock Authentication Tokens and renew
- Certificates for non-RA staff
- **DO NOT** verify users ID

3.1.9. **RA Agent** - Responsible for checking that application forms are completed correctly and signed by the appropriate authorities. Where these are in order, to set up access to the required system at the nominated level. **This includes:**

- Verify users ID to GPG45 Level 3 or 4.
- Register users and provide them with.
- Authentication Tokens.
- Grant users access assignment.
- Renew Smartcard certificates for users if self - service functionality not used.
- Responsible for ensuring users at the time of Regisration.
- Registration or assigned a role in the organisation.
- Comply with the individual terms and conditions.
- Applicable to access to the NHS Care Records.
- Service Ensuring leavers from an organisation have their access rights removed in a timely way.

- Adhere to local processes that meet policy and guidance for the creation of Authentication Tokens, digital identities, production of smartcards, allocation and registration of other approved devices, assignment of access rights, modifications to access and people and certificate renewal and card unlocking.

3.1.10. **Smartcard** - The NHS Smartcard is a 'Chip and PIN' card that requires a card reader and a Personal Identity Number (card pass-code) to enable access to NHS systems such as the NHS Care Records Service.

3.1.11. **PBAC** - Position Based Access Control.

4. Policy Statement

4.1. The role of the RA Manager at the Trust is to ensure that individuals providing healthcare services at the Trust and Workforce / HR related services staff have timely access to NHS Digital compliant applications and information in accordance with their role. It is the Trust's responsibility to ensure that all the requirements of Registration Authorities are met and maintained so appropriate access and confidentiality can be maintained.

4.2. This will be achieved by verifying beyond reasonable doubt the identities of Trust staff and the application of specific Position Based Access Controls (PBAC) to an individual's profile. It is the RA's responsibility to ensure that all the requirements of identity and PBAC are met and maintained so that Trust staff only have access to the patient and staff information and software functions needed to perform their role.

4.3. It is important that all members of the RA Team, Manager, Sponsors and RA Agents are aware of the confidential nature of some of the information captured during registration and preserve its confidentiality.

5. Arrangements

5.1. The RA role encompasses a hierarchical structure where the approval of Smartcards is delegated to departmental managers.

5.2. Smartcards are issued under a number of very stringent policies and procedures, published by NHS Digital that must be adhered to. These are designed to assist the Trust meet its obligations to the Care Records Guarantee published by the Department of Health.

5.3. The Trust is obliged to comply fully with these in order to support the requirement to meet the Care Records Guarantee, which clearly outlines how the NHS will treat patient records confidentially.

5.4. There is a hierarchal structure to enforce security and adhere to the required governance arrangements.

5.5. Healthcare professionals within the Trust will be registered and granted access to the NHS Care Records Service applications made by the Trust.

5.6. The Trust RA Manager will be registered by the NHS England Registration Authority Manager.

5.7. RA Agents will be registered by the Trust RA Manager.

5.8. Sponsors will be appointed by the Trust's Caldicott Guardian / CEO / Executive Director of the Registration Authority process and can be registered either by the Trust RA Manager or Agents.

5.9. Cardholders can be registered by either the Trust RA Manager or Agents.

5.10. Where RA Manager or RA Agents are created, the RA Manager will add the newly registered person to the appropriate distribution list at RAManagers.agents@nhs.net.

5.11. Smartcards will be issued to new employees on a 'needs must' basis to be identified early in the recruitment process and directly linked to the Workforce / HR pre-employment procedures for new staff.

5.12. The control and issue of Smartcards will fully comply with strict national policies and procedures and will be managed by the RA team.

5.13. The applicant must have completed an RA01 form and supplied identification to the satisfaction of the RA Agent before a card can be issued.

5.14. Smartcards will not be issued until all conditions have been satisfied and access to the systems will not be granted until the user has received appropriate training in the applications identified in their RBAC.

5.15. Existing employees will be registered under the same rules and conditions for the issue of Smartcards as and when access is required.

5.16. The requirement for existing staff to be issued with Smartcards will be identified by Sponsors.

5.17. Temporary staff will be sponsored and Smartcards issued in the same way as for permanent staff.

5.18. As soon as the Smartcard is no longer required, it will be the responsibility of the Line manager to notify the Sponsor, RA Manager or RA Agent immediately to ensure that access is revoked.

5.19. Where the Trust determines that an individual, who is not employed directly by the Trust, is required, as part of their duties, to have a Smartcard, **the following conditions shall apply:**

- They will be issued with an honorary contract of employment.
- They will sign a confidentiality agreement.
- They will complete mandatory Data Protection and Cyber Security Awareness training.
- They will provide evidence of identity to E-Gif Level 3.
- They will abide by all Trust policies and procedures.
- The will affirm that in any case of misuse of a Smartcard that it will immediately be revoked, and their contract with the Trust may be terminated.

5.20. A list of external staff with cards will be held and maintained in an up to date manner by the RA.

5.21. Smartcards will be updated whenever a user’s role changes or responsibilities are added to their existing role which requires them to have access to additional data from the spine enabled applications. It will also apply to employees who no longer require access to a dataset or application and therefore must have that access revoked.

5.22. **Smartcards must be de-activated for the following reasons:**

- When a registered Smartcard holder leaves the NHS with no intention of going to another NHS organisation, this will be linked to the Workforce / HR Leavers procedure.
- If the RA management team decide that a cardholder’s Smartcard should be withdrawn due to inappropriate access or disclosure, this may be linked to the Trust’s disciplinary policy.
- If the cardholder is going on extended leave over six months (or twelve months as in the case of maternity leave), the cardholder’s line manager is responsible for keeping the Registration Authority updated on the current status.

- Where a cardholder is on leave for more than twelve months, they will be required to re-register, satisfying the full Level 3 identification requirements.

5.22.1. Smartcards have an embedded microchip that is used to store the certificate or electronic token. The Smartcard will have an expiry date two years from the date of issue.

5.22.2. Cardholders are authorised to update their own cards, providing they have not actually expired. This can be done up to three months prior to expiry date.

5.22.3. Where cards have expired, RA Managers, RA Agents or Sponsors can update the cards following the process outlined in the national document covering this procedure.

5.22.4. Cardholders who have either lost or damaged their Smartcard or had it stolen must report the fact at the earliest possible opportunity to their Sponsor, RA Manager or RA Agent.

5.22.5. The lost or damaged card will be cancelled immediately, either by cancelling the card (if it is present), or by revoking the certificates.

5.22.6. The request for a replacement Smartcard will received by the appointed RA Agent via Trust internal systems such as email or via MS Teams.

5.22.7. If this is reported during normal hours of operation the RA Manager will issue a replacement Smartcard immediately. At the present time there is no out of hours' service.

5.22.8. Smartcards should be treated with care and protected to prevent loss or damage.

5.22.9. Smartcard security pass codes must not be divulged and must only be known to the card holder. Not even RA personnel are allowed to know the pass code.

5.22.10. Cardholders are not permitted to have more than one card.

5.22.11. Smartcards must never be shared or allocated to anyone other than the intended recipient. Employees not adhering to these rules may be subject to the Trust's disciplinary policy.

5.22.12. Users who have forgotten their pass code should contact the RA Agent or designated Sponsor in order to have their pass code changed. The Smartcard holder must be present for this to take place.

5.22.13. Users will be locked out of NHS Digital applications after three failed login attempts.

5.22.14. Employee and Account Recovery Pass codes may be set by the user during registration. Each pass code may be different but must only be known to the user. These pass codes will be used by the RA to confirm the identity of the registered user in the following circumstances:

5.22.15. Under no circumstances should anyone other than the user, set, or know their Smartcard pass code. Where the RA has to issue a new card and the user is not present, then the card must be created using a random and unrecorded pass code and locked until such time as the user sets their own pass code.

5.22.16. The National Spine and Card Management System (CMS) should be available twenty-four hours a day, every day of the year.

5.22.17. The RA Manager will be alerted by email whenever there is a problem with either of these services. These alerts detail the error state, expected time of service resumption and escalation procedures. While CMS is unavailable, Smartcards cannot be issued or maintained. While the Spine is unavailable there is no access to data on the NHS Digital systems.

5.22.18. The RA Manager at the Trust will be available Monday to Friday from 08-30 to 16-30, excluding Bank Holidays, and an RA Agent will be available during normal hours of operation.

6. Responsibilities

6.1. RA Managers The nature of the registration processes cross departmental boundaries.

6.2. In particular, it is acknowledged that the role the Human Resources division of the Workforce Development department has to play in implementation of Smartcard processes is of key importance to the Trust. Workforce Development will have a major role in the issuing and withdrawing Smartcards within the Trust in line with staff employment processes.

6.3. **Caldicott Guardians the Trust Caldicott Guardian also has significant responsibilities in connection with the Governance of Registration Authorities, namely to:**

- Ensure that Caldicott principles are maintained within the operations of the Registration Authority.

- Provide guidance on process improvements.

- Approve and countersign RA forms that appoint RA Sponsors, grant access to the Secondary User Service(SUS), Demographics Batch Services (DBS) or other restricted applications after ensuring that the sponsor has previously authorised the form.

- Approve Trust User Access Profile and Position profiles and who within the Trust can maintain them.

- Advise the RA on governance issues affecting RA operations.

6.4. RA Sponsors Authorisation of Smartcard issue is achieved by sponsorship of the user by an individual at an appropriate level in the Trust who assigns the appropriate business function and role. This determines the Position Based Access Control (PBAC) associated with an employee.

6.5. Trust Service Managers or equivalent will be authorised as Sponsors.

6.6. The use of position based templates will be provided to assist Sponsors select the appropriate access attributes for cardholders if required.

6.6.1. **RA Sponsor responsibilities:**

- To ensure that users are provided with the appropriate role based access to applications.

- Ensure that they are familiar with the users need for access to functionality and information.

- Ensure that the user role profile associated with a user is appropriate.

- Escalate any user role profile problems to the Trust RA Manager.

- Complete documentation that supports the issue/revocation/amendment of a Smartcard and the role profiles associated with the card.

- Sponsors may be asked to unlock Smartcards or renew certificates of Trust staff if they become locked through the incorrect use of the security pass code.

- Assist in ensuring cardholders are aware of their responsibilities in keeping cards secure and not sharing cards or pass codes.

- Reporting any untoward incident relating to Smartcard use to the Trust RA Manager.

6.6.2. RA Agents The RA Agent is responsible for receiving the completed RA forms, for checking that these are completed correctly and countersigned by an authorised RA Sponsor. Where these are in order, and the appropriate level of identification documents have been produced, access is granted to the user and the database of users is updated.

6.6.3. RA forms either incorrectly completed or unsigned will not be processed but referred back to the sponsor for correction.

6.6.4. Where there is a persistent pattern of incorrect forms emerging RA Agents will notify the RA Manager, so that remedial training and action can be taken.

6.6.5. **RA Agents are managed by the RA Manager and may have the following responsibilities:**

- The day to day support of the local Registration Authority.
- Issue Smartcards to users who have been sponsored and have proven identities as detailed above.
- Ensure that access profiles specified by the sponsor use the appropriate method identified by the Trust.
- Update user Smartcard profiles in accordance with the sponsor’s requirements.
- Revoke Smartcards from users when they leave the Trust.
- Provide support to users experiencing access problems and escalate to RA Manager as appropriate.
- Ensure that national RA processes are adhered to within the Trust.
- Escalate any process, hardware and application problems to the RA Manager.
- Ensure that all any other documentation supporting the issue/amendment/revocation of Smartcards and role profiles associated with Smartcards are retained in accordance with the national RA processes via the RA Manager.
- Maintain an audit trail of all Smartcards.

- Ensure that users only have one NHS CRS Smartcard associated with their Unique User Identification (UUID) at any time. The issue of more than one Smartcard to a user is not permitted.

- Promptly report all incidents of misuse, anomalies or problems to the RA Manager.

- Apply common sense checks and challenge the content of RA forms and take appropriate action if required.

- Provide a service for the entire Trust (currently within the hours of operation of 9.00 to 17.00 Monday to Friday).

7. Competence

7.1. The RA Manager is required to understand NHS Digital guidance and requirements relating to the RA process.

7.2. The RA Manager will train RA Agents and Sponsors in the registration policies, procedures and use of the RA equipment and documentation as appropriate. This will be supported by the use of the NHS Digital E-Learning website.

8. Monitoring

8.1. Audit trails covering all cards issued, updated and cancelled, and all roles and business functions granted or revoked, will be available to Sponsors and/or Line Managers on request.

8.2. Access to all spine enabled functions using a smartcard are fully auditable. Access audits will take place in instances where inappropriate access is suspected.

8.3. Ad-hoc reports will be produced by the RA Manager for presentation to the Information Governance Working Group. These reports will detail the number of cards issued, the levels of access requested, and forecasts for card usage to assist with stock control and capacity planning.

8.4. Quality reviews should be carried out on the RA processes by a manager who is independent of the RA, for example by a performance Manager or similar role. The review should undertake spot checks on the processes and produce a summary report for the RA Manager who will action any recommendations/ changes required.

9. Audit and Review

9.1. This policy is to be reviewed every three years or sooner if new legislation, codes of practice or national standards are introduced.

9.2. The RA Manager will be responsible for ensuring that an audit trail of all RA activity is maintained.

9.3. In accordance with national Registration Authority requirements, all RA forms and supporting documentation must be retained in a secure environment in accordance with the Department of Health policy requirements.

9.4. Audit requirements will include those that are issued to the Trust by the NHS England as part of its remit to maintain governance.

9.5. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

9.6. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

9.7. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

10. References

- Registration Authorities: Operational Process and Guidance
- Confidentiality: NHS Code of Practice
- NHS Digital Registration Authority website
- NHS Care Record Guarantee
- Registration+Authority+Policy+v2.5 (3).pd
- NHS Digital Caldicott Guardian website