Ashford and St. Peter's Hospitals
NHS Foundation Trust

REGISTRATION AUTHORITY (Smartcard) POLICY

Compiled by: Dave Thompson, IT Training Lead

In Consultation with: Information Governance Steering Group, Workforce Information Administrator, Choose and Book Manager

Status:

Approval date: February 2018

Ratified by: Information Governance Steering Group

Review date: February 2021

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Approved by
1	Feb 2012	New policy	Information Governance Steering Committee
2	Feb 2018	Additional details in respect of maintenance of equipment, and provision of consumables	Information Governance Steering Committee

For more information on the status of this document, please contact:	
Policy Author	Dave Thompson, IT Training Lead
Date of issue	February 2018
Review due	February 2012
Ratified by	Information Governance Steering Committee
Audience	All Staff

REGISTRATION AUTHORITY (SMARTCARD) POLICY

1. INTRODUCTION

1.1. Ashford & St. Peter's Hospitals NHS Foundation Trust (ASPH) is a local Registration Authority (RA) authorised to carry out on behalf of the NHS:- registration of individuals; issuance of smartcards; and granting of access to patient data held by the Health and Social Care Information Centre (HSCIC).

The local Registration Authority (RA) ensures that individuals providing healthcare services to the NHS directly, or indirectly, have access to NHS CRS compliant applications and information in accordance with their role. It is the Trust's responsibility to ensure that the requirements of RAs are met and maintained, to adhere to the NHS Confidentiality Code of Practice and the NHS Care Record Guarantee.

1.2. The Registration Authority Policy describes how the Trust will meet its obligations as an NHS RA, by complying fully with the national policies, guidance and procedures for the management of RAs issued by the Department of Health and HSCIC.

2. PURPOSE

2.1. The policy provides the basis for the standards and procedures that are to be adopted when anyone is given access to HSCIC or other smartcard-enabled applications for the purposes of their work.

3. SCOPE

3.1. The national policy requires everyone accessing Connecting for Health applications to be registered with an individual identity on the national NHS database (the Spine), and to have their access authorised by a Registration Authority Sponsor appointed by the Trust Executive. The individual can then be issued with a personal "chip-and-PIN" smartcard, which gives them the access authorised for their role in the Trust.

3.2. This document states how ASPH will operate the Registration Authority, and carry out registration of staff within the Trust.

4. DUTIES & RESPONSIBILITIES

4.1. **Trust Executive and Caldicott Guardian**

4.1.1. To ensure that the necessary systems and resources are in place for the successful implementation and ongoing operation of this policy.

4.1.2. To review and determine action on security incidents involving the registration of staff and the use of smartcards to access information.

4.2. **Director responsible for the Registration Authority**

4.2.1. Simon Marshall, Director of Finance and Information has been identified to HSCIC as the director responsible for the RA in the Trust.

4.3. **Managers and clinical leads**

4.3.1. Managers and clinical leads are required to be aware of this policy, its purpose and its operational implications.

4.3.2. Managers need to ensure that all staff who need access to CRS-compliant systems for their work are properly identified and are associated with a relevant position in the Care Identity System (CIS).
4.3.3. Managers should take positive action to promote the security of electronic records and the correct use of smartcards, and should take supervisory or disciplinary action where infringements take place, or report the security incident for attention by higher authority. The Trust's Incident Reporting policy must be followed as a minimum.
4.3.4. The Trust's RA Manager will be responsible for providing advice and guidance. This will be facilitated partly by creating and maintaining a Registration Authority section on the intranet.

4.4. **Registration Authority Sponsors**

4.4.1. Sponsors are (usually managers) appointed as people entrusted to act on behalf of the Trust, authorising access to electronic records, and deciding the appropriate level of that access consistent with job roles and organisational changes.
4.4.2. Under this policy, Sponsors are appointed by a generic statement based on the organisational position or status of the person's role in the Trust – anyone holding or appointed to such a position or status is required to fulfil the role of RA Sponsor for the staff working under their supervision.
4.4.3. The role and responsibilities of Registration Authority Sponsor within this Trust is assigned by this Policy to all departmental clinical leads and their deputies for clinical staff, to all divisional matrons and ward sisters for nursing staff, and to departmental managers / supervisors for other roles.
4.4.4. The role and responsibilities of Registration Authority Sponsor is also assigned to subordinate officers nominated by a departmental manager, providing that the departmental manager has notified the RA Manager in writing of the nominee.
4.4.5. RA Sponsors may also be nominated by the Chief Executive or the Caldicott Guardian by notification in writing to the RA Manager.
4.4.6. Sponsors are required to understand the interaction of positions, job roles and activities and the resulting scope of access they enable to systems and data
4.4.7. Sponsors are required to manage and update user access levels, using the ESR system to record changes of position, leavers and new starters in a timely manner.
4.4.8. Sponsors are required to retrieve the smartcard from staff when there is no further requirement of their job to use it. In the case of persons leaving the Trust the Sponsor should confirm proof of further NHS employment before allowing a leaver to retain his/her smartcard. Sponsors must pass any smartcard retrieved or handed in to them directly to IT Training where appropriate action will be taken to cancel the smartcard.
4.4.9. Sponsors must ensure that staff undertake specific training in the use of any smartcard-enabled systems they are required to use.
4.4.10. Sponsors must report to the RA Manager any breaches of smartcard security, and must request the revocation of any smartcard they consider unsafe.

4.5. **Individual staff members**

4.5.1. Each member of staff needing a smartcard is required to attend a registration meeting with an RA Agent to provide documentation verifying his/her identity to e-GIF Level 3 in accordance with Government requirements, and to be photographed by the RA Agent.

At the registration meeting the RA Agent reviews the user's identity document and records electronically in the CIS system the type of document and document number/reference.

The user's photograph is taken and uploaded to the CIS system where it is stored electronically on the user's record.

These checks are in addition to the NHS Employment and identity checks performed by HR at the time of recruitment.

4.5.2. By accepting a smartcard, staff confirm their identity and agree with the conditions of registration and the use of smartcards and electronic records. This policy is in addition to the Trust's published policies on information security and information governance.

4.5.3. Staff are required to:-

- devise and use passcodes known only to themselves for the function of the smartcard.
- Ensure that they have their smartcard and passcode available at all times when on duty.
- Keep their smartcard safe and secure and use it only in accordance with Trust policies and procedures.
- Ensure that they respond properly and correctly to system prompts to update smartcard certificates and / or passcodes.
- Report promptly to the RA Agent, RA Manager or Sponsor the loss of or damage to their smartcard so that remedial action can take place.
- Never allow any other person to use their smartcard under any circumstances.
- To report promptly in line with the Trust's Incident Reporting Policy any observed breach of smartcard policy or procedure.

4.6. **Lead RA Manager**

4.6.1. The Lead RA Manager:

- will ensure that policies and procedures support the national policy and procedures for Registration Authorities and the use of Smartcards.
- may implement local policies and/or procedures which supplement the national policy and procedures.
- will ensure access requirements and deployment plans for NHS systems are supported.
- will select and appoint RA Agents as deemed appropriate to the requirements of the Trust.
- will ensure that adequate training and information is available to RA Agents
- will ensure that appropriate hardware and software is available to enable the provision of a suitable registration and smartcard issuing/maintenance service.
- will ensure adherence to Information Governance requirements by carrying out audits of registration records and smartcard use.

4.7. **RA Managers**

4.7.1. The Trust authorises two other senior managers to be RA Managers to provide continuity in terms of day to day management whenever the Lead RA Manager

is not available.

4.8. **RA Agents**

4.8.1. RA Agents will provide registration and smartcard issuing service to sponsors and all Staff requiring smartcards.
4.8.2. RA Agents will provide smartcard maintenance services to Staff such as card unlocking, passcode renewal, certificate renewal and card replacement.
4.8.3. RA Agents are empowered by this policy to revoke access or cancel a smartcard on instruction from a manager, RA Manager or sponsor.
4.8.4. RA Agents will follow RA guidance issued by HSCIC, and adopt notified changes to guidance.
4.8.5. RA Agents will follow local RA procedures notified by the RA Manager.
4.8.6. RA Agents will work with HR staff members to comply with and maintain good working practices in respect of the ESR / CIS interface to ensure that smartcards are issued in a timely manner to appropriate personnel.
4.8.7. RA Agents will ensure registrations and smartcard operations are conducted in a way that protects the confidentiality and security of personal data, and in a way that respects the Trust's Equal Opportunity and Diversity policies.
4.8.8. RA Agents will ensure that the Trust maintains an adequate supply of new smartcards available for issue, and will keep smartcards under secure storage until their issue.

5. POSITION-BASED ACCESS CONTROL AND THE INTERFACE WITH ESR

5.1. This Trust has implemented the integrated ESR/CIS Position-Based Access Control (PBAC) methodology as recommended by HSCIC.
5.2. In summary, this methodology assigns predetermined levels of system access to defined job roles, enabling the Trust to simplify control of access to systems by placing a staff member into a position in ESR. The position (e.g. Consultant, Staff Nurse, IT Support) has a defined and limited set of access permissions associated with it. Should the staff member be assigned to a different position at a later stage, their access permissions will be replaced with the permissions associated with the new position.
5.3. With the introduction of PBAC early in 2011, smartcards are now requested by the employees' manager at the time of appointment to a position. The HR Department records the requirement for a smartcard which pushes a registration request through to the RA Agent in IT Training via the CIS.
5.4. The RA Agent in IT Training takes a photograph of the applicant and verifies their identity before completing the registration request and issuing a smartcard.
5.5. The RA Manager will retain oversight of all CIS/ESR positions; changes to positions, and the creation and definition of new positions, must be agreed with the RA Manager, in discussion with the Information Governance Manager and HR Representatives before being implemented in CIS / ESR.
5.6. Suspension or cancellation of a Smartcard is managed through the ESR to CIS interface. When an employee is flagged as leaving on ESR or if their employment is suspended for a variety of reasons then their smartcard access is automatically revoked.

6. EQUIPMENT

6.1. The effectiveness of the RA process at the Trust depends on the availability of suitable hardware, consumables and software:
- Datacard printer(s) for printing of Smartcards
- blank Smartcards
- Smartcard enabled keyboards or other means of reading smartcards
- Authentication software installed on all smartcard-enabled PCs

6.2. The Lead RAM is responsible for ensuring that the Trust has adequate equipment to fully support the RA operation, and for ensuring that the equipment is properly maintained and usable at all times

6.3. The Lead RAM is responsible for ensuring that hardware and software changes and upgrades advised to the Trust by the SHA and/or Department of Health are promptly applied

6.4. The Lead RAM is responsible for security of all equipment and consumables

6.5. **Provision of Consumables**

6.5.1. Smartcards, Printers and Printer Consumables must be ordered in order to ensure the continuation of the Smartcard service at the Trust

6.5.2. New Smartcards are obtained by completing an order request via *https://smartorder.oberthur.com/HSC/* . At the time of writing smartcards are provided free of charge

6.5.3. New Smartcard Printers, and Printer Ribbons and Cleaning equipment can be ordered from:

Specialist Computer Centres PLC
James House
Warwick Rd.
Tyseley
Birmingham B11 2LE

7. TRAINING

7.1. Training will be provided by the RA Manager through the IT Training Team to all Sponsors, RA Agents, Managers, Supervisors and Staff as required

8. DISSEMINATION AND IMPLEMENTATION

8.1. This policy will be disseminated to staff through the Trust's usual communications channels.

8.2. Information and guides referring to the Registration Authority and Smartcards will be published and maintained on the Trust's intranet

9. MONITORING OF COMPLIANCE

Managers and Supervisors are responsible for monitoring the use of smartcards and must take relevant action if any instances of abuse are discovered. Guidance may be sought from the RA Manager or IG Manager.

10. KEY CONTACTS

The RA Manager, the Information Governance Manager and the IT Training Lead can be contacted for any advice or guidance on all aspects of this policy.

11. EQUALITY IMPACT ASSESSMENT

The purpose of this assessment is to minimise and where possible remove any disproportionate impact on employees on the ground of race, sex, disability, age sexual orientation or religious belief. A baseline assessment of this policy identified no detriment and is attached at Appendix 1.

12. ARCHIVING ARRANGEMENTS

This is a Trust-wide document and archiving arrangements are managed by the Quality Department

13. REVIEW OF THE POLICY

This policy will be reviewed at three-yearly intervals unless there are significant changes to systems or procedures which warrant earlier review.

14. GLOSSARY OF TERMS

CIS	**The Care Identity System** *A system managed and maintained by HSCIC to provide for all aspects of Smartcard and Position Management.*
CRS-ENABLED	**Care Records Service-enabled** *Describes a computer system which can only be accessed using a Smartcard, helping to ensure the security and confidentiality of patient and employee data. Choose & Book and ESR are examples of two systems used at the Trust which are CRS-Enabled.*
e-GIF Level 3	*Anyone requiring a smartcard must have their identity checked beyond all reasonable doubt to the Government's e-GIF Level 3 standard. This standard lists the proof which must be supplied by the individual to the RA Agent when applying for a Smartcard. A Smartcard cannot be issued if the individual fails to provide proper acceptable proof of identity.*
ESR	**Electronic Staff Records** *The Electronic Staff Records system records details of all employees and their position within the Trust. The employee's position identified within ESR links directly to UIM and thereby associates the correct levels of access to the employee's smartcard.*
PBAC	**Position-based Access Control** *PBAC is a method of associating levels of system access with a position in the organisation. Thus, the position of 'Medical Secretary' has a different set of access rights than the position of 'IT Analyst'. The link between ESR and UIM automatically determines an employee's level of access by reference to the PBAC position.*

RA	**Registration Authority** *Organisations that deliver NHS care and need to access patient information within NHS systems and other national services must set up Registration Authorities to manage this process. The roles and responsibilities of Registration Authorities are defined by NHS policy. Their key tasks are first to verify the identity of all healthcare staff who need to have access to sensitive data, and second to establish and provide only the degree of access they need to do their jobs.*
RA Agent	**Registration Authority Agent** *A member of staff appointed by the RAM to carry out the day-to-day activities of smartcard issue and maintenance.*
RAM	**Registration Authority Manager** *A member of staff appointed to control the entire scope of the Registration Authority function at the Trust.*
SPONSOR	*A sponsor is appointed as a person entrusted to act on behalf of the Trust, authorising access to electronic records and deciding the appropriate level of that access consistent with job roles and organisational changes.*
UIM	**User Identity Manager** *A computer system which enables the RA Agent to create and maintain records of users requiring Smartcard access, to print smartcards and to cancel or modify access.*

15. LIST OF ROLES

Sponsors:	All Divisional General Managers and their direct reports are sponsors for the purposes of this policy. In addition, any line manager may be appointed as sponsor as business needs, roles and positions dictate. A list of sponsors will be maintained by the RA Manager and reviewed at least annually
RA Lead:	Director of Finance and Information
Lead RAM:	Associate Director Informatics
Deputy RAM:	IT Training Lead
RA Agents:	IT Training Lead IT Trainers HR - Workforce Information Officers HR - Recruitment Officers / HR Assistants

APPENDIX 1
EQUALITY IMPACT ASSESSMENT SUMMARY

Name: **Laura Ellis-Philip, Associate Director Health Informatics**

Policy/Service: **Registration Authority (Smartcard) Policy**

Background • Description of the aims of the policy • Context in which the policy operates • Who was involved in the Equality Impact Assessment
This policy provides guidance on how this Trust will undertake its responsibilities as a Registration Authority in the NHS, the use of Smartcards at the Trust, and the roles and responsibilities of staff involved. *The EIA was performed by the Head of Informatics Programme Management.*
Methodology • A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age) • The data sources and any other information used • The consultation that was carried out (who, why and how?)
The policy was examined and reviewed to ensure that no negative impact on equality would result from it.
Key Findings • Describe the results of the assessment • Identify if there is adverse or a potentially adverse impacts for any equalities groups
There is no impact on equality.
Conclusion • Provide a summary of the overall conclusions
The policy applies to all staff regardless of race, ethnic origin, gender, culture, religion or belief, sexual orientation and age.
Recommendations • State recommended changes to the proposed policy as a result of the impact assessment • Where it has not been possible to amend the policy, provide the detail of any actions that have been identified • Describe the plans for reviewing the assessment
The policy should be approved.