

**Operation of the Registration Authority Policy**

**Policy: GV12**

**Description**

Policy to highlight roles and responsibilities in relation to Registration Authority processes and links to existing Trust policies, practices and systems.

If you require this document in a different format or language

please speak to a member of Trust staff.

If you would like to provide feedback about our services

Contact PALS – 01392 675686 or email dpn-tr.pals@nhs.net

| **Document Control** |  |
| --- | --- |
| Ref No & Title: | GV12 Operation of the Registration Authority |
| Version: | v3.0 |
| Replaces / dated: | Previous policy dated 28th November 2019 |
| Author(s) Job Title: | IT Service Support & RA Manager |
| Ratifying Committee: | Digital Strategy Board |
| Director / Sponsor: | Chief Information Officer |
| Primary Readers: | All Managers and Administration staff |
| Additional Readers | All staff |
| Date ratified: | 09 June 2022 |
| Date issued: | June 2022 |
| Date for Review / Ratify by: | Commence Review January 2024 Approval by June 2024 |
| Date archived: |  |
| Other Relevant Standards met: | Data Security and Protection Toolkit: under Assertion 1.3.1 |

**Contents**

[**1. Introduction 3**](#_Toc494273596)

[**2. Purpose 3**](#_Toc494273597)

[**3. Scope 3**](#_Toc494273598)

[**4. Duties 4**](#_Toc494273599)

[**5. Confidentiality 7**](#_Toc494273600)

[**6. Registration Process 7**](#_Toc494273601)

[**7. Training 7**](#_Toc494273602)

[**8. Disciplinary Issues 8**](#_Toc494273603)

[**9. Incident Reporting 8**](#_Toc494273604)

[**10. Leavers 8**](#_Toc494273605)

[**11. Monitoring 9**](#_Toc494273606)

[**12. References 9**](#_Toc494273607)

# Introduction

* 1. As part of the NHS Digital Programme, the Electronic Patient Record (EPR) system was introduced throughout the NHS. This system helps transform the way in which health care records are accessed and managed. Electronic records give authorised healthcare professionals faster, easier access to accurate patient information and protect patient confidentiality. Over time, centrally stored information will be accessible from any healthcare provider location in England. Ultimately well-managed electronic records will lead to improvements in the quality of patient care and the patient experience.
	2. The Trust has currently implemented the CareNotes clinical records system which has the capability to link to national patient records systems. CareNotes users who need to have access to the NHS spine need to formally register for an NHS Smartcard. This document applies to both national and local electronic databases that require a national Smartcard for access, and that adhere to Role Based Access Controls (RBAC) and Position Based Access controls (PBAC) as part of the Care Identity Service (CIS).
	3. All new starters and existing employees require clearance to access Trust Applications and other national applications by issue of a Smartcard. Clearance can be defined by being sponsored through HR or line management arrangements.
	4. All employees that require access to Trust Applications or other National applications must be registered to obtain this card, which has a chip and a personal identification number (PIN).
	5. The Smartcard will be issued with varying levels of access to patient records dependent on the job/position role undertaken and the need to view details, change details or enter clinical information. Access to information will be granted in accordance with the Position Based Access Templates (PBAT) ratified by the Trust’s Caldicott Guardian. The Trust adheres to the latest National RBAC specification mapping.
	6. The Trust’s IT Service Support Team are responsible for managing Smartcards and developing local procedures that adhere to national guidance. The management of the Registrations Authority (RA) currently resides with the RA Manager accountable to the Technical Design Group.
	7. The Safer Information team are responsible for providing general advice and support in relation to medical records, information governance and confidentiality.
	8. HR Connect are fully integrated into the use of the Care Identity Service (CIS) system and have appropriate processes for registering new starters.

# Purpose

* 1. The purpose of this policy is to highlight the roles and responsibilities in relation to the RA processes and explain how these processes link into existing policies, practices and systems.

# Scope

* 1. This policy applies to all Trust employees, including those working at the Trust on an honorary or temporary basis (i.e. locums, bank and agency staff). This will include any employees who are on secondment to a role that requires access to Trust Clinical applications or other national Clinical systems.

Posts that require access to the spine through the Trust’s EPR system will require post holders to be registered and be issued with a Smartcard in accordance with national guidelines. It will be the Line Manager’s responsibility to identify the roles within each respective department which will require access to Trust clinical applications or other national clinical applications.

* 1. As detailed in section 4 below, the Line Manager will also be responsible for ensuring that individuals are aware that their post will require RA registration. HR Connect and the RA team are responsible to ensure the appropriate information is registered on CIS.

# Duties

* 1. **Caldicott Guardian –** The Medical Director the executive level of governance for confidentiality and security including responsibility for RA.
	2. **Directorate Managers/Clinical Directors/Medical Directors**
* To identify and agree all roles within their area of responsibility which require access to CareNotes, or other National Clinical applications, in conjunction with the relevant Managers. This function is supported by the Informatics, Safer Information (Governance) and the Trust’s RA Manager.
* To identify relevant Sponsors and ensure on an on-going basis that there are sufficient Sponsors in place within their area of responsibility in order to support the registration process. The IT Service Support Team support the RA Registration across the Trust.
* To ensure that Sponsors are correctly registered with the Registration Authority using the full authentication process in accordance with National guidance.
* To ensure that the Registration Authority is notified immediately if any Sponsor ceases to fulfil this role. For example: following a change of employment circumstance or change of manager and advice of the nominated replacement and, if this individual is not already a Sponsor, ensuring that they are correctly registered using the full authentication process. The IT Service Support will perform a delegated sponsor function aligned to the production of cards, following training.
	1. **RA Manager**
		1. To be responsible for ensuring that all Sponsors and Line Managers understand the RA procedures and the need to ensure that staff register in a timely manner.
		2. The RA Manager has ongoing responsibility for the following areas:
* To be responsible, on behalf of the Trust, for ensuring that adequate numbers of Smartcards are available and to maintain the Smartcards throughout their useful life in accordance with national policy.
* To ensure that all pre-CIS application forms are stored in a secure area and destroyed by an appropriate means in line with agreed Trust policies and procedures in accordance with national policy.
* Records will be kept within the CIS system of all cards that have been returned and destroyed by the IT Service Support Team in accordance with national policy.
* To liaise with the Head of Safer Information (Governance) with regards to ensuring that audits of the RA process are undertaken and any appropriate action(s) arising from the outcome of these audits is put in place.
* To ensure that any necessary HR policies and procedures reference the Registration Authority e.g. Recruitment and Selection Policy. This will include when policies come up for renewal or revision.
* To ensure that the RA process is included with the Trust’s Corporate Induction programme.
	1. **RA Agent**
* Be familiar with and adhere to this document and Registration Authorities: Governance Arrangements for NHS Organisations.
* Check the staff member’s identity according to the NHS Employers Identity guidance to e-GIF level 3 for non-substantive employees.
* Ensure staff have only one NHS CRS Smartcard issued to them showing their User's Unique Identifier (UUID) and photograph, and that staff are aware of their responsibilities relating to Safer Information (Governance) and Smartcard use. The issue of more than one NHS CRS Smartcard to a staff member is not permitted. (Fallback Smartcards, Short-term Access Smartcards, and ETP01 cards are not NHS CRS Smartcards in this context).
* Grant previously approved and granted positions, to staff who have been approved by a sponsor to be assigned to that position.
* Enable access for locum, agency, and bank staff access in accordance with the CareNotes SOP’s.
* Adhere to the audit policy and ensure that all RA forms and associated information are maintained and securely stored according to national policy.
* Report incidents of misuse, anomalies, or problems to the RA Manager and initiate local Risk Management procedures.
* Ensure that the issue and use of Fallback Smartcards adheres to the organisation's Fall-back Smartcard policy.
* Renew a staff members Smartcard certificates if confident of the staff members identity. Note: the local RA should encourage staff to self-renew their Smartcard certificates via the Self Service Portal.
* Unlock a user's Smartcard and reset logon Passcodes.
* Ensure staff are aware of the self-service functionality available to them, including how to unlock Smartcards, reset Passcodes, and renew Smartcard certificates.
* Ensure RA Agent contact details including email address and telephone number are recorded in the Spine User Directory.
	1. **Sponsors**
* Be familiar with the different types of access positions to approve, making reference to the nationally approved set of access rights and baseline policy in the [national RBAC database](http://systems.hscic.gov.uk/rasmartcards/planning/rbacoutline/index_html). This is supported by the RA Office.
* Work with RA agents to maintain access to NHS compliant applications within their area of responsibility that is consistent with the [Confidentiality: NHS Code of Practice](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253), Department of Health, Gateway reference: 2003. This includes access profile change and removal, and the revocation of Smartcards and Smartcard certificates.
* All DPT staff requiring access to Smartcard enabled systems must be sponsored by their line manager or delegated sponsor. The IT Service Support team will support the sponsor function.
	1. **Line Managers**
* To identify all staff within their area of responsibility who require access to the Trust Applications system and ensure that all employees, including temporary/agency/bank and locum employees, are provided with appropriate access.
* To ensure for all roles that involve access to the Trust Applications or other National application systems that job descriptions and any recruitment materials make reference to the need to be registered and the role’s responsibilities in relation to using the system.
* To ensure that current/future employees attend the appropriate meetings with a member of the IT Service Support Team to enable the Smartcard to be issued, providing employees with authorised time away from the department where applicable.
* To ensure that all new clinicians within their area of responsibility, including agency/temporary employees, receive Trust EPR training in order to be able to access the system. EPR training will include an overview of confidentiality and instruction on how to use the Smartcard if access is required.
* To ensure that all employees are aware of the contents of this policy and other trust information policies.
* To immediately inform the Sponsor and, in the absence of the Sponsor, the IT Service Support Team, of any leavers, starters and staff changes including details of staff taking a period of leave (such as maternity leave) or suspension.
	1. **Employees**
		1. Are responsible for the use of their smartcard in accordance with the Trust’s:
* Smartcard terms and conditions as set out within the system
* [G03 Information Management and Technology Security Policy](https://www.dpt.nhs.uk/resources/policies-and-procedures/general/information-management-and-technology-security)
* [GV03 Confidentiality](https://www.dpt.nhs.uk/resources/policies-and-procedures/governance/confidentiality)
* [GV06 Records Management Policy & Strategy](https://www.dpt.nhs.uk/resources/policies-and-procedures/governance/records-management-policy-strategy)
	+ 1. Informs the Sponsor (who in turn must inform the RA Agent) immediately should their Smartcard be lost, stolen or misplaced and report this as an incident on the [RMS system](https://rms.dpt.nhs.uk/) in line with the Trust’s [R01 Incident Reporting Policy](https://www.dpt.nhs.uk/resources/policies-and-procedures/risk/incident-reporting) and guidance which is on the trust intranet.
		2. To ensure that he/she reports any misuse of the system in line with this policy.
		3. To ensure that he/she keeps his/her Smartcard and log-in details confidential. In particular he/she must not leave his/her PC logged in and unattended; must not leave Smartcards unattended; must not share or provide access to his/her Smartcards or passwords. Any breach of the above could lead to action being taken in line with the Trust’s Disciplinary Policy – see [Promoting a Positive Working Environment (HR01)](https://www.dpt.nhs.uk/resources/policies-and-procedures/hr/promoting-a-positive-working-environment).
		4. To ensure that he/she accurately completes the necessary process, provides suitable identification and attends any appropriate appointments in order to register on the system or have his/her Smartcard updated/re-issued.

# Confidentiality

* 1. All staff issued with a Smartcard must adhere to the NHS Confidentiality Code of Practice (November 2003) and the Data Protection Act (2018) and any Trust policies on Confidentiality, Information Security and the Disclosure of Confidential Information. Any breaches of confidentiality or misuse of the Smartcard may result in disciplinary action being taken up to and including dismissal, in line with the Trust’s Disciplinary Policy – see [Promoting a Positive Working Environment (HR01)](https://www.dpt.nhs.uk/resources/policies-and-procedures/hr/promoting-a-positive-working-environment).
	2. Every time an individual accesses an electronic EPR patient record an electronic audit trail is created of who they are, when they accessed information and what they did. Patients are able to request this information in accordance with the Confidentiality Policy and Subject Access Request process as managed through the Safer Information (Governance) team.
	3. In addition to specific requests for audit trails the Head of Safer Information (Governance) will audit a random sample of clinical records. Any access not deemed appropriate will be further investigated and disciplinary action taken if appropriate.

1. **Registration Process**
	1. The RA registration process will be managed by the Trust’s IT Service Support Team. Details of the procedures for registering employees with Smartcards are maintained by the IT Service Support Team and updated on the intranet in accordance with National policy.
2. **Training**
	1. RA Staff Training - Staff involved in the management and maintenance of RA functions will be equipped with the required skills to fulfil this function. This will be assessed through the Trust supervision process and additional training targeted as required.
	2. Application Training - All staff members must undertake local Electronic Patient Record system training or other appropriate National Application system training or receive information relating to the following before being allowed access to the system:
* [G03 Information Management And Technology Security Policy](https://www.dpt.nhs.uk/resources/policies-and-procedures/general/information-management-and-technology-security)
* NHS Confidentiality Guidelines and Data Protection Act (2018)
* How to access the system
* Sign on Authentication
* Using the EPR system
* Completion of ID verification checks carried out by RA Agent or HR Connect
	1. The Sponsor, with support of the IT Service Support Team, is responsible for ensuring that the appropriate training is undertaken by the user before use of the Smartcard. Training or awareness of policies and procedures is the responsibility of the Line Manager within the relevant area and should be undertaken as part of the local induction process.

# Disciplinary Issues

* 1. As stated in sections 5 and 9, any incidents resulting from the Registration Authority which relate to inappropriate conduct or behaviour will be investigated in line with the Trust’s Disciplinary Policy – see [Promoting a Positive Working Environment (HR01)](https://www.dpt.nhs.uk/resources/policies-and-procedures/hr/promoting-a-positive-working-environment)
	2. During a disciplinary investigation it may be necessary to suspend an employee’s Smartcard. If the staff member is formally suspended from duty for whatever reason their Smartcard will be suspended. The employee’s Line Manager will need to consider the impact on the service of removing access to the system and must discuss with a senior member of the HR team the impact that this will have and whether any suitable alternative arrangements need to be put in place during the period that the Smartcard is suspended. Any arrangements will be undertaken in line with the Trust’s Disciplinary Policy – see [Promoting a Positive Working Environment (HR01)](https://www.dpt.nhs.uk/resources/policies-and-procedures/hr/promoting-a-positive-working-environment)

# Incident Reporting

* 1. Incidents must be reported by any employee where they feel that there is a risk to the Trust, the health of people using Trust Services or confidentiality. Incidents should be reported in line with the Trust’s [R01 Incident Reporting Policy](https://www.dpt.nhs.uk/resources/policies-and-procedures/risk/incident-reporting) and then notified immediately to the RA Manager, Line Manager or the IT Service Support Team.
	2. Examples of incidents are:
* Smartcard or application misuse
* Theft of a Smartcard
* Any unauthorised access of CareNotes or other applications
* Any unauthorised alteration of patient data.
* The sharing of Smartcards for access to Trust Clinical Applications or other National Clinical Applications.
	1. The Directorate Manager, or equivalent, or the Sponsor will consider all incidents reported to them. Any incidents considered significant will be escalated to the Caldicott Guardian, Head of Safer Information (Governance) and the Human Resources department depending on the nature of the incident. A significant incident is defined as an isolated incident or a series of less significant incidents that could lead to a serious degradation of healthcare or Information Security. The RA Manager and Caldicott Guardian will consider incidents reported to them and make recommendations as to whether Trust systems or working practices should be reviewed as a result and, if appropriate, the Information Governance Manager will report the incident in the Data Security and Protection Toolkit in accordance with NHS Digital guidance.
	2. A major breach of security will also be reported by the RA Manager to the local service provider and NHS Digital to ensure that any risks resulting from the event can be taken into account and mitigated against.
	3. Incidents involving breaches of security must also be reported to HR and the Chief Information Officer (CIO) by the RA Manager so that any disciplinary measures required may be taken. The HR department will contact the relevant Directorate Manager, or equivalent, who will be responsible for ensuring an appropriate and timely investigation is undertaken in line with the Trust’s Disciplinary Policy – see [Promoting a Positive Working Environment (HR01)](https://www.dpt.nhs.uk/resources/policies-and-procedures/hr/promoting-a-positive-working-environment) In the event that a Smartcard is reported lost or stolen, the IT Service Support Team will initiate the Trust’s incident process.

# Leavers

* 1. It is the responsibility of the Sponsor to ensure that staff members who leave or take an agreed period of leave from the organisation have their status recorded by the IT Service Support Team. The IT Service Support Team will process leavers/absentees by either suspending or revoking the Smartcard. It is then the Sponsor’s or HR Department’s responsibility to notify the IT Service Support Team of any staff who require their Smartcard and User ID to be re-activated.
	2. Suspension of Smartcards is appropriate for members of staff who will not be in a position to use the Smartcard for a short period of time e.g. sickness absence, short career break. Ideally suspension should not cover a period greater than 3 months, although the Sponsor has the discretion to request suspension for longer periods, depending on the circumstances. In all other circumstances the Smartcard should be revoked and association to the Trust removed.
	3. It is the responsibility of the IT Service Support Team to ensure appropriate destruction of returned smartcards in timely manner.
	4. In order to ensure that all leavers are being captured by the IT Service Support Team, a list of leavers will be supplied to the RA Agent by HR Connect by electronic notification from ESR.

# Monitoring

* 1. The RA policies and procedures will be audited. Regular audits would typically cover:
* The issue of Smartcards
* The management of Smartcards
* The profiles associated with staff in relation to what they do
* The use of appropriate applications
* Identity management – deferred to HR for substantive employees
* Exception reporting – to highlight users who consistently try to or do access information which they have not been authorised to view/use.
	1. It is the responsibility of the Head of Safer Information (Governance) and IT Service Support Team to ensure that these audits are undertaken and any action resulting from them put in place. In addition, the Head of Safer Information and IT Service Support Manager is responsible for undertaking an audit immediately following implementation to assess the consistency and appropriateness of levels of access assigned to staff groups and grades.
	2. The Trust will annually assess and update training needs and review programmes and materials to ensure these continue to reflect the roles and responsibilities of staff.

# References

[G03 Information Management And Technology Security Policy](https://www.dpt.nhs.uk/resources/policies-and-procedures/general/information-management-and-technology-security)

[GV03 Confidentiality](https://www.dpt.nhs.uk/resources/policies-and-procedures/governance/confidentiality)

[GV06 Records Management Policy & Strategy](https://www.dpt.nhs.uk/resources/policies-and-procedures/governance/records-management-policy-strategy)

[HR01 Promoting a Positive Working Environment (HR01)](https://www.dpt.nhs.uk/resources/policies-and-procedures/hr/promoting-a-positive-working-environment)

[R01 Incident Reporting](https://www.dpt.nhs.uk/resources/policies-and-procedures/risk/incident-reporting)

[HR54 Agile Working Policy](https://www.dpt.nhs.uk/resources/policies-and-procedures/hr/agile-working)