Registration Authority Smartcard Policy

Document Summary

This policy provides guidance for the effective management of the Registration Authority Service

POLICY NUMBER	**POL/002/066**
DATE RATIFIED	24 January 2018
DATE IMPLEMENTED	February 2018
NEXT REVIEW DATE	November 2019
ACCOUNTABLE DIRECTOR	Director of Strategy & Support Services, Michael Smillie
POLICY AUTHOR	RA Manager

Important Note:
The Intranet version of this document is the only version that is maintained.

Contents

1. Scope

This is the Trust’s local RA policy which is based on the National Policy and its principles which apply to all staff of Cumbria Partnership NHS Foundation Trust (CPFT) including contracted third parties (including agency staff – where appropriate), students/trainees, people on secondment and other staff on placement with CPFT and staff of partner organisations with approved access covered by contracted Service Level Agreements (SLAs).

The policy applies also to those under contract with CPFT to provide RA services (i.e. primary care via Local Area Team and CCG).

2. Introduction

With the introduction of the NHS Care Records Service (NHS CRS) compliant applications, it is of paramount importance that NHS patients are confident their medical records are kept secure and confidential in line with the National and regulatory frameworks as described in the Cumbria Partnership NHS Foundation Trust (CPFT) IG policies and procedures.

To achieve this, all employees requiring access to NHS CRS compliant applications must be registered with a smartcard and have appropriate access profiles. The registration process for NHS CRS compliant applications must meet current Government e-GIF Level 3 authentication requirements to ensure the identity of the individual applying for registration and access. All the NHS CRS compliant applications use a common security and confidentiality approach. This is based upon care setting, areas of work and business functions.

The primary method by which users will access an NHS CRS compliant application is via a smartcard issued during the formal registration process. Once an applicant has been successfully registered they will have a User ID, pass-code and smartcard issued to them, which will permit their individual access to the appropriate application(s) and information. The registration process is operated at a local level by an authorised Registration Authority (RA) that is required to conform to NHS Digital standards. The operation of the Registration Authority has been integrated, where possible, with Trust functions covering the Human Resources administration of staff starters/leavers processes and network access requests to non NHS CRS Compliant systems.

In Public Key Infrastructure (PKI) terms there is a single Registration Authority (NHS Digital). All organisations that run a local Registration Authority do so on a delegated authority basis from NHS Digital. As NHS Digital is the single Registration Authority it needs to assure itself that organisations are operating appropriately and discharging their duties in an effective and consistent fashion. This paper sets out the policy and procedures under which all aspects of the RA function will be processed, managed and monitored locally to ensure compliance with national guidance and organisational responsibilities.

3. Statement of Intent

The organisation needs a Registration Authority function to administer the registration process; to manage the distribution and use of Smartcards, and individual NHS CRS compliant applications system access rights.

At this time there are no plans for the NHS CRS compliant smartcard to become the CPFT staff identification card. However, this may be subject to change in line with any associated National Guidance.

All staff will be required to complete the registration process before being issued with a smartcard.

Staff who do not require access to ESR or NHS CRS compliant applications will **NOT** be issued with a Smartcard. However, staff who are nominated to the role of RA Sponsor will be registered on the National SPINE following normal registration procedures and will be issued with a smartcard for the sole purpose of carrying out this role.

CPFT will comply fully with the latest published NHS Digital National RA Policies and Guidance Procedures available from the NHS Digital Website. Depending on the extent of the changes that latest NHS Digital guidance introduces, this may result in a review of this policy.

4. Definitions

The use of the word “staff” in this document means people who are directly employed by, contracted to provide services to, or are part of a contractual agreement with CPFT (i.e primary care). CPFT will operate the Registration Authority on behalf of the following organisations and groups of staff that operate within the geographic boundaries of Trust. This applies to: -
Staff directly employed by CPFT (Cumbria Partnership NHS Foundation Trust
Staff directly employed by CCG (Cumbria Clinical Commissioning Group)
Staff employed in primary care (under auspices of Local Area Team, i.e. GP Practices, Pharmacists etc).

Any other clinical or non-clinical person who is contracted by CPFT who requires access to NHS CRS compliant applications in order to perform the duties for which they are employed.

All staff who require access to NHS CRS compliant applications and who are not directly employed by CPFT but where CPFT is responsible for the provision of Registration Authority services across geographical responsible areas.

Glossary of Terms:

CRS	(National) Care Records Service aims to create the integrated electronic care record
C&B	Choose & Book
CIS Forms	Various forms used in the RA process
EPS	Electronic Prescription Service
ESR	Electronic Staff Record
HR	Human Resources Department within CPFT
IIM	Integrated Identity Management combines the currently separate processes within Registration Authority and Human Resources for capturing and managing employee identity
IR	Incident Reporting Form

e-health	e-health Department within CPFT
IT	Information Technology
LPC	Local Pharmaceutical Committee
LSP	Local Service Provider – Primary contractor and provider of applications, systems and solutions as contracted through HSCIC
PBAC	Position Based Access Controls
RA	Registration Authority
Role Profile	Term used to define system access levels for individual users Systems
SLA	Service Level Agreement
Smartcard	Photo ID Card issued to individual system users that holds information relating to levels of system access assigned.
SUD	(National) Spine User Directory is where user registration details are held. When users access systems with their smartcard, the details on the SUD are authenticated against their smartcard as part of the login process
UUID	The User's Unique Identifier which is a number allocated to the user's UIM account and which is printed on the individual's smartcard along with their photograph

5. Duties

CPFT Registration Authority is made up of the following personnel: -

Post	**Action**
Chief Executive	The **Chief Executive** has overall responsibility for the Trust RA Department and how it operates.
Director for Finance, Strategy & Support Services	The **Director of Finance Strategy and Support Services** is the accountable Director for this policy and (as Senior Information Risk Owner) leads in the responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level
Caldicott Guardian	The **Caldicott Guardian** has a responsibility for reflecting patients' interests regarding the use of patient identifiable information, will provide organisational and clinical assurances that the Registration Authority arrangements within the Trust comply with statutory requirements
Head of Information Governance	The **Head of Information Governance** will provide overall quality assurance on the procedure to confirm that it complies with the Information Governance Toolkit requirements and National Health Service Litigation Authority and Care Quality Commission standards and regulations. The Registration Authorities actions play a key role in Information Governance controlling who has access to what information within smartcard enabled patient and staff information systems. The Head of Information Governance is overall responsible for the RA function.
Registration Authority Manager	The **Registration Authority Manager** has responsibility for the day to day management of the RA within and on behalf of the Trust in line with HSCIC National guidelines. They are responsible for the RA staff and their actions to ensure the effective delivery of all RA services
Registration Authority Agents	The **Registration Authority Agents** have responsibility for the day to day administrative function of the Registration Authority service including issuing, revocation and modification of cards to CPFT staff and those from associated organisations (including GP Practices, Pharmacies, Social Services, Independent Providers) across Cumbria to allow access to clinical and staff systems.
Identified RA staff	Staff with RA positions (Sponsor, ID Checker, Local Smartcard

	Administrator) Are responsible for assisting the RA team in the delivery of RA services and support
All Smartcard Holders	All smartcard holders have a responsibility to comply with the RA Policy for the safe and secure and appropriate use of their smartcards.
IT Service Staff	Providing support to end users on standard smartcard issues and application problems

6. Policy Detail

The Registration Authority needs to have at the heart of its thinking protecting patients' interest and the obligations placed on staff through the National and Regional guidelines.

6.1 RA Overview

Smartcards enable an individual to access sensitive patient data and therefore how they are issued and ensuring safe receipt and appropriate use are of vital importance. To provide operating assurance all RA services will be routinely monitored and audited.

6.2 User registration and authentication - e-GIF level 3

The UK electronic Government Interoperability Framework (e-GIF) defined the standards to be applied in order to promote interoperability in information systems. One aspect of this Framework covers user access controls.

e-GIF Level 3 defines the access controls to be applied to sensitive/personal information, broadly on the basis of the use of local user names and passwords, and the use of nationally managed electronic certificates and personal identification numbers (PINs).

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 http://www.nhsemployers.org/case-studies-and-resources/2009/01/verification-of-identity-checks.

6.3 Smartcard use

Smartcards and passcodes are similar to a chip and PIN debit card but are more secure as there is no account information on the Smartcard and the passcode is more complex.
A user's Smartcard is printed with their name, photograph and unique user identity number. The photograph is stored centrally, and is always available for an organisation to verify that the Smartcard holder is indeed the person to whom it was issued.

It is mandatory that users accept the Terms and Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.

Users have a responsibility to manage their own Smartcard are reminded to renew their certificates when advised to do so

All NHS healthcare staff know that it is a disciplinary offence to tamper with Smartcards, share passcodes, or use a Smartcard that does not belong to them, and that they may lose their jobs if they do so.

When Smartcard users leave an organisation they should have their access assignment end dated in that organisation. However unless it can be reasonably foreseen that they will not require access in another organisation in the future, leavers should retain their Smartcard.

6.4 Access Control

Individuals are granted access to patient information based on their work and level of involvement in patient care. This means that, for example, someone working in an administrative role rather than a clinical one might only be able to see the demographic information needed to process an appointment, not the full clinical record.

CPFT have identified staff care groups and roles and have allocated a national PBAC position to the corresponding employee role.

Access will be granted following the National guidelines by using either the electronic Care Identity Service, Care Identity Service forms or through the Trust Straight On process. The HR and RA departments work in partnership to identify and allocate Smartcards to new employees who require access to patient and staff information systems

The removal of access positions should be requested using the Straight On requests, Care Identity forms or linked to the Trust leavers policy & monthly leavers reports, to ensure access is removed in a timely manner.

6.5 Incident Reporting

Any member of staff can report incidents where they feel there is any risk to service users' or others' health or safety, confidentiality or the Trust's reputation. Incidents in the context of this policy should be reported through the Trust's Incident Reporting System

In the context of this policy, examples of incidents can include:

- Smartcard or system misuse
- Smartcard theft or loss

- Any non-compliance with local or national RA Policy
- Any unauthorised access of smartcard enabled IT systems
- Any unauthorised alteration of service user's data.

Where incidents demonstrate that an individual member of staff has breached the conditions associated with the use of their smartcard, an investigation may be undertaken and, where appropriate, may lead to the Trust's Disciplinary procedure being invoked. If it suspected that a Smartcard is being misused the certificate associated with the Smartcard should be suspended or revoked as appropriate. In these circumstances the RA Manager will authorise the appropriate action and inform the relevant Sponsor(s) and the RA User.

6.6 Temporary and Contract Staff

CPFT will ensure all temporary staff or contractors who need to use the NHS CRS applications are bound by the General Data Protection Regulations and The NHS Confidentiality Code of Practice. This will include the process to be taken in cases of a breach and liability issues. Where relevant, CPFT will ensure any contracting procedure meets this requirement.

Temporary or contract staff, (locums, agency staff, students, bank staff etc) who require access to NHS CRS applications need to fulfil the same starting and leaving requirements as permanent staff for registration purposes. They will for example need to provide appropriate level of personal identification.

Line Managers/Sponsors should specify starting and leaving dates. If no leaving date is specified, RA staff will apply open ended position access and this will then be managed by revoking position access from those who have not used their cards in the previous three months.

Line Managers/Sponsors are responsible for notifying RA staff in advance if registration or changes to an individual's profile is required and when they leave the Trust.

The policy permits the issue of smartcards/smartcard access profiles or positions to individuals from organisations which support NHS CRS applications such as those responsible for system deployment/testing. The same policy requirements apply and such access should only be provided for the required period and then revoked. For example, access being provided only for the period of system deployment/testing

6.7 RA Processes & Procedures

The following standard operating procedures (SOP's) detail the end to end process followed the RA department that link into other Trust departments to ensure access to any EPR system is assigned appropriately and in a timely manner.(See RA SOP Section 6.16)

7. Training

All staff will comply with the mandatory training requirements of the Trust and this includes Information Governance Training:

The RA Manager has responsibility for maintaining training and awareness of RA procedures for all staff with who undertake RA roles.

Training for all staff with RA roles can be completed using NHS Digital online training tool or by direct training sessions with a member of the RA team. Nationally there is currently no mandatory requirement to complete the training but the Trust will only apply access to RA roles to those who have successfully completed the training.

8. Partnership Arrangements with other Agencies

CPFT works closely with other agencies - both statutory and those from the voluntary sector in order to promote more effective joint working. This may involve the requirement to share information with staff who are employed outside the NHS and would include any arrangements made within section 75 of the 2006 NHS Act which enables formal partnerships to be created between, for example, NHS Trusts and relevant social services

Social Services staff formally seconded to the Trust can be issued with smartcards to permit an appropriate level of access to NHS CRS applications dependent upon their role.

Smartcards may be issued to NHS/non NHS staff who have a legitimate reason for access. Examples include staff employed within other NHS Trusts who may provide local services to CPFT via a Service Level Agreement, those working within Local Authority Emergency Duty or Child Protection Teams, or those responsible for health related data input on social services systems.

It is a requirement that staff from other organisations undertake appropriate training in the application they are using before access is assigned. It is also necessary at the outset to agree the appropriate role of staff which will determine their level of access within the system. Access for external users will only be granted where there is a lawful and fair processing condition under the General Data Protection Regulations to allow (i.e. SLA's/honorary contracts are in place).

9. Monitoring compliance with this policy

"The table below outlines the Trusts' monitoring arrangements for this policy/document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs".

Aspect of compliance or effectiveness being monitored	Monitoring method	Individual responsible for the monitoring	Frequency of the monitoring activity	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed
KPI's results via InPhase	RA activities monitored via InPhase	RA Manager	Monthly	IG Board	IG Board
Compliance with HSCIC	Conclusion Reports	RA Manager	Annual	IG Board	IG Board

RA toolkit					
RA Training	Training is monitored on a monthly basis through Inphase				

10. References/ Bibliography

NHS Digital – IG Toolkit
IG Toolkit - Requirements

NHS Applications – NHS Spine Authentication Portal
https://portal.national.ncrs.nhs.uk/

NHS Digital - National Registration Authority Policy
https://digital.nhs.uk/article/311/Registration-Authorities-and-Smartcards/

NHS Digital - Registration Authorities Operational and Process Guidance
https://digital.nhs.uk/article/311/Registration-Authorities-and-Smartcards/

11. Related Trust Policy/Procedures

Link to:
Access Controls Policy

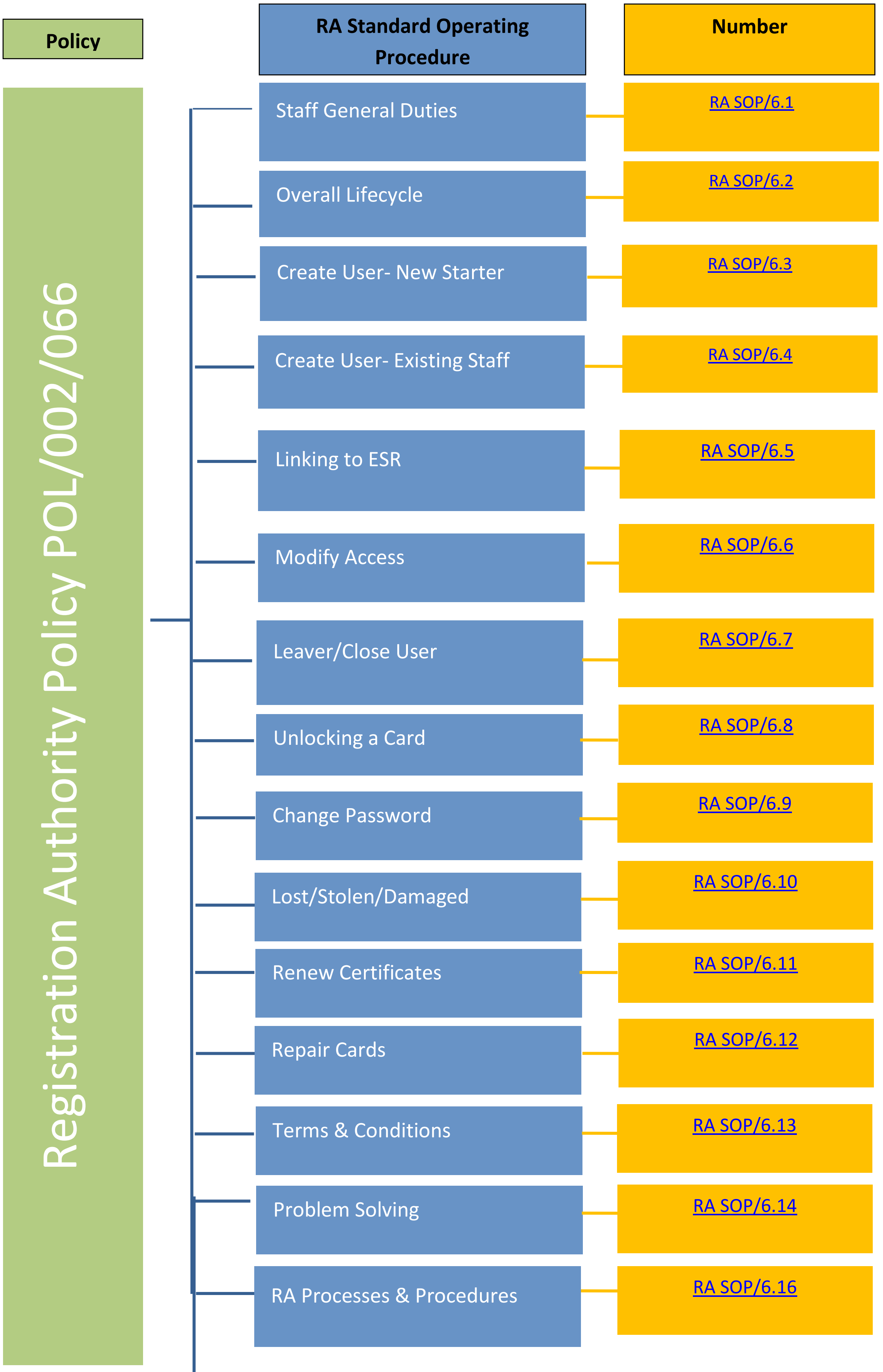
Local SLSP ID Checking Process

RA Standard Operating Procedures

RA Process Maps

APPENDIX 1

Registration Authority Policy and Standard Operating Procedure Framework.



Policy	RA Standard Operating Procedure	Number
Registration Authority Policy POL/002/066	Staff General Duties	RA SOP/6.1
	Overall Lifecycle	RA SOP/6.2
	Create User- New Starter	RA SOP/6.3
	Create User- Existing Staff	RA SOP/6.4
	Linking to ESR	RA SOP/6.5
	Modify Access	RA SOP/6.6
	Leaver/Close User	RA SOP/6.7
	Unlocking a Card	RA SOP/6.8
	Change Password	RA SOP/6.9
	Lost/Stolen/Damaged	RA SOP/6.10
	Renew Certificates	RA SOP/6.11
	Repair Cards	RA SOP/6.12
	Terms & Conditions	RA SOP/6.13
	Problem Solving	RA SOP/6.14
	RA Processes & Procedures	RA SOP/6.16