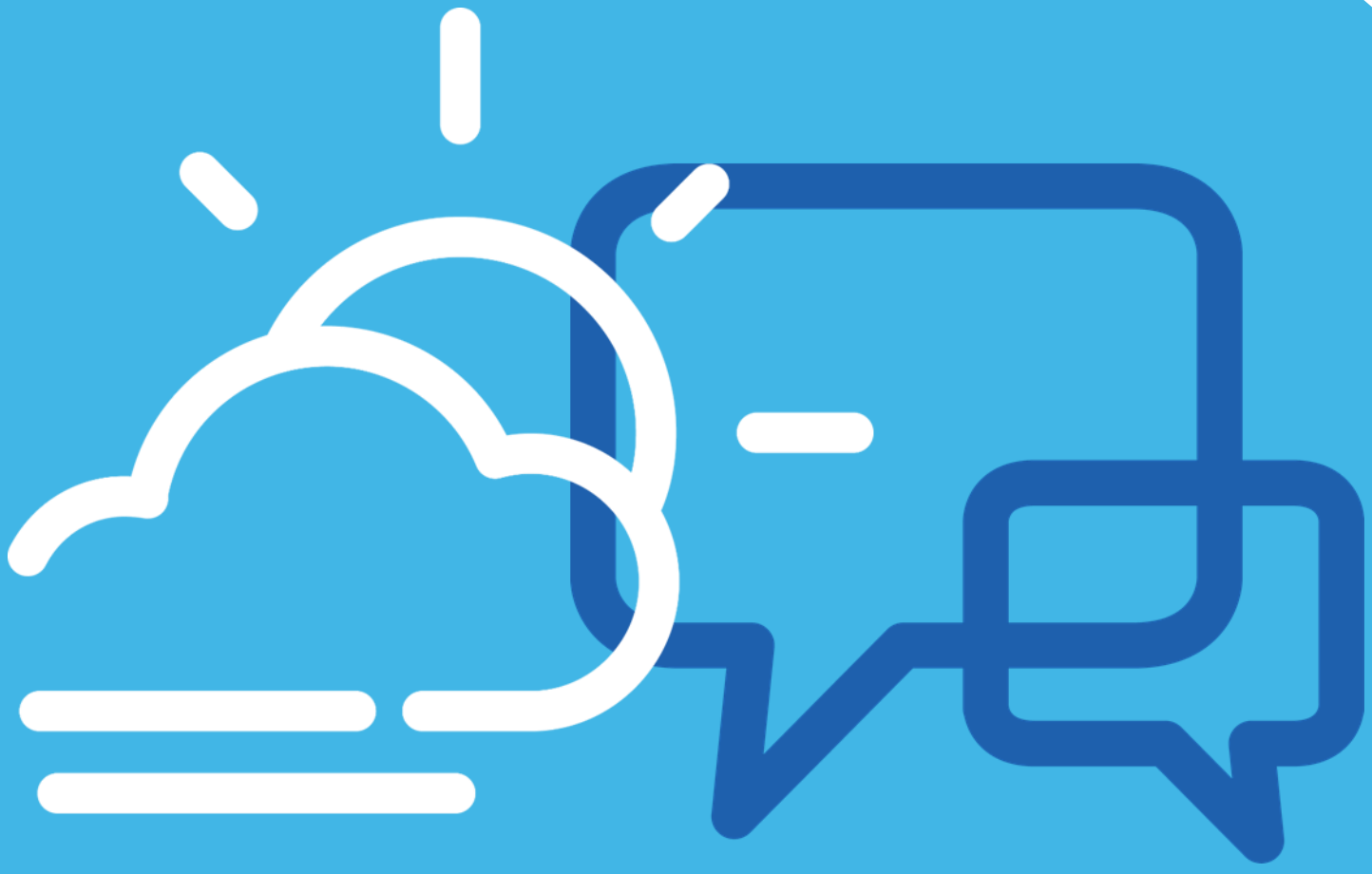
NHS
Greater Manchester Mental Health
NHS Foundation Trust

Registration Authority Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Registration Authority Policy**
Executive Summary:	This policy provides the standards and procedures to be used for the issuing and the subsequent using of 'smartcards', that provide access to the NHS central data base for patient demographics, commonly referred to as the 'NHS Spine'.
Executive Lead:	Director of Finance and IM&T
Document Author:	Sarah McDonald, Head of IM&T Service Delivery
Document Purpose:	Policy
Target Audience:	All employees of Greater Manchester Mental Health NHS Foundation Trust
Additional Circulation List:	All employees via Trust intranet
Date Ratified:	15/01/19
Ratified by:	Information Governance Steering Group
Consultation:	Representatives from all directorates via membership of the IGSG.
Cross Reference:	Related trust policies including the Information Governance Policy (IG006) and the Incident, Accident and Near Miss Policy and Procedure (RM004) Information Security Management Code of Practice for NHS organisations and the Data Security and Protection Toolkit.
Superseded Docs	GMMH Registration Authority Policy (IG11) V1
Date of Equality Impact Assessment:	14/08/2017
Board Objective Reference:	Objective 3 – To engage in effective partnership working Objective 6 – To achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	NHS Digital, the NHS Registration Authority (RA) regulatory body
Risk Register Reference:	N/A
Contact Details for further information	Sarah McDonald, Head of IM&T Service Delivery Tel: 0161 358 1751 Sarah.McDonald@gmmh.nhs.uk
Document Status	This is a controlled document. Whilst this document may be printed, the electronic version posted on the Trust intranet is the controlled copy.

Contents

1. Introduction

1.1. Purpose

The purpose of this policy is to provide clear, robust procedural guidance to Greater Manchester Mental Health (GMMH) staff, that ensures that 'Smartcards' are issued to and subsequently used by staff in line with the regulations provided by NHS Digital, the NHS Registration Authority (RA) regulatory body.

Suspected deliberate misuse of the smart card, and any information derived from this will result in a comprehensive investigation and may result in disciplinary action.

1.2. Scope

This policy applies to all employees of Greater Manchester Mental Health NHS Foundation Trust.

2. Definitions

CIS	Care Identity Service
DPA	Data Protection Act 2018
GDPR	General Data Protection Regulation
IT	Information Technology
PBAC	Position Based Access Control
RA	Registration Authority
RBAC	Role Based Position Access Control
SCR	Summary Care Record
SIRO	Senior Information Risk Owner
SUD	Spine User Directory

2.1. Relevant Legislation – GDPR/DPA 2018

The General Data Protection Regulation sits within the Data Protection Act 2018. It is the legislation that provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers all staff records.

There are six principles identified under GDPR that set out standards for information

handling and sets the foundation for personal data to be:

1. Lawful, fair and transparent
2. Limited for its purpose
3. Adequate and necessary
4. Accurate
5. Not kept longer than needed
6. Integrity and confidentiality (security).

GDPR also details a separate accountability principle which details organisations' responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate compliance and accountability.

2.2. Data Protection Officer

The GDPR introduces a legal duty to appoint a Data Protection Officer (DPO) for all public authorities and on organisations that carry out certain types of processing activities.

DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (ICO).

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The Trust's DPO will help demonstrate compliance and is part of the enhanced focus on accountability within the Trust.

3. Duties

3.1. Board/Lead Committee

The Information Governance Steering Group is responsible for the approval and monitoring of this Policy.

3.2. Chief Executive

The Chief Executive has ultimate responsibility for ensuring that the Trust develops and implements a robust Registration Authority (RA) framework which is compliant with the principles and policies of NHS Digital, this key function is delegated to the Trust Senior Information Risk Owner (SIRO).

3.3. Senior Information Risk Owner

The SIRO is responsible for the development and implementation of the Registration Authority framework as mentioned above.

3.4. Deputy Senior Information Risk Owner

The Trust's Deputy SIRO is responsible for supporting the SIRO in ensuring that robust processes are in place that support the issuing and using of smartcards in line with the principles and policies of NHS Digital.

3.5. RA Manager

The RA Manager appointment is approved by the SIRO on behalf of the Trust Board. The RA Manager is the named contact for NHS Digital and will act as a focal point for all communications between GMMH and NHS Digital.

The RA Manager is responsible for ensuring that any staff member allocated to an RA role has received the necessary training and is competent to perform the role on behalf of the Trust.

The following functions are available to the RA Manager in the CIS (Care Identity Service) application:

- Register RA Manager in child hosting organisation
- Register Advanced RA Agent, RA Agent, RA Agent ID Checker, Sponsors and Local Smartcard Administrators in own organisation and child organisations
- Register Smartcard users
- Search and view closed users
- Reopen closed users
- Create positions and workgroups
- Modify positions
- Assign individuals to positions
- Review positions definitions including assigned users
- Assign individuals to workgroups
- Manage request lists
- Access reporting and run reports
- Assign users to positions
- Use batch functionality
- Create Temporary Access Cards
- Cancel Smartcards
- Close users

- Unlock Smartcards & renew certificates
- View all requests

3.6. Advanced RA Agent

The Advanced RA Agent is responsible for the practical functionality of the CIS, ensuring that staff access is restricted in line with the NHS Digital agreed positions for GMMH.

The following functions are available to the RA Agent in the CIS application:

- Register Smartcard users
- Search and view closed users
- Reopen closed users
- Create positions and workgroups
- Modify positions
- Assign individuals to positions
- Review positions definitions including assigned users
- Assign individuals to workgroups
- Manage request lists
- Access reporting and run reports
- Assign users to positions
- Use batch functionality
- Create Temporary Access Cards
- Cancel Smartcards
- Close user
- Unlock Smartcards & renew certificates
- View all requests.

3.7. RA Agent

The main function of the RA Agent is to grant requests made by users.

The following functions are available to the RA Agent in the CIS application:

- Register Smartcard users
- Search and view closed users

- Reopen closed users
- Assign individuals to positions (only grant the assignment)
- Review positions definitions including assigned users
- Assign individuals to workgroups
- Access reporting and run reports
- Create Temporary Access Cards
- Cancel Smartcard
- Close user
- Unlock Smartcards & renew certificates
- View all requests.

3.8. RA Agent ID Checker

The RA Agent ID Checker is able to perform the identity checks to register users in CIS.

The following functions are available to RA Agent ID Checkers in the CIS application:

- Raise and approve request to assign a user to a position
- Directly assign user to any assignable position
- Raise request to register a new user (completed by RA)
- Review positions definitions including assigned users
- View my requests and requests pending approval
- Unlock Smartcards & Renew Certificates
- Assign users to Workgroups.

3.9. RA Sponsors

The RA Sponsor is able to approve requests for smart cards.

The following functions are available to RA Sponsors in the CIS application:

- Raise and approve request to assign a user to a position
- Directly assign user to any assignable position
- Raise request to register a new user (completed by RA)
- Review positions definitions including assigned users
- View my requests and requests pending approval

- Unlock Smartcards & Renew Certificates
- Assign users to Workgroups.

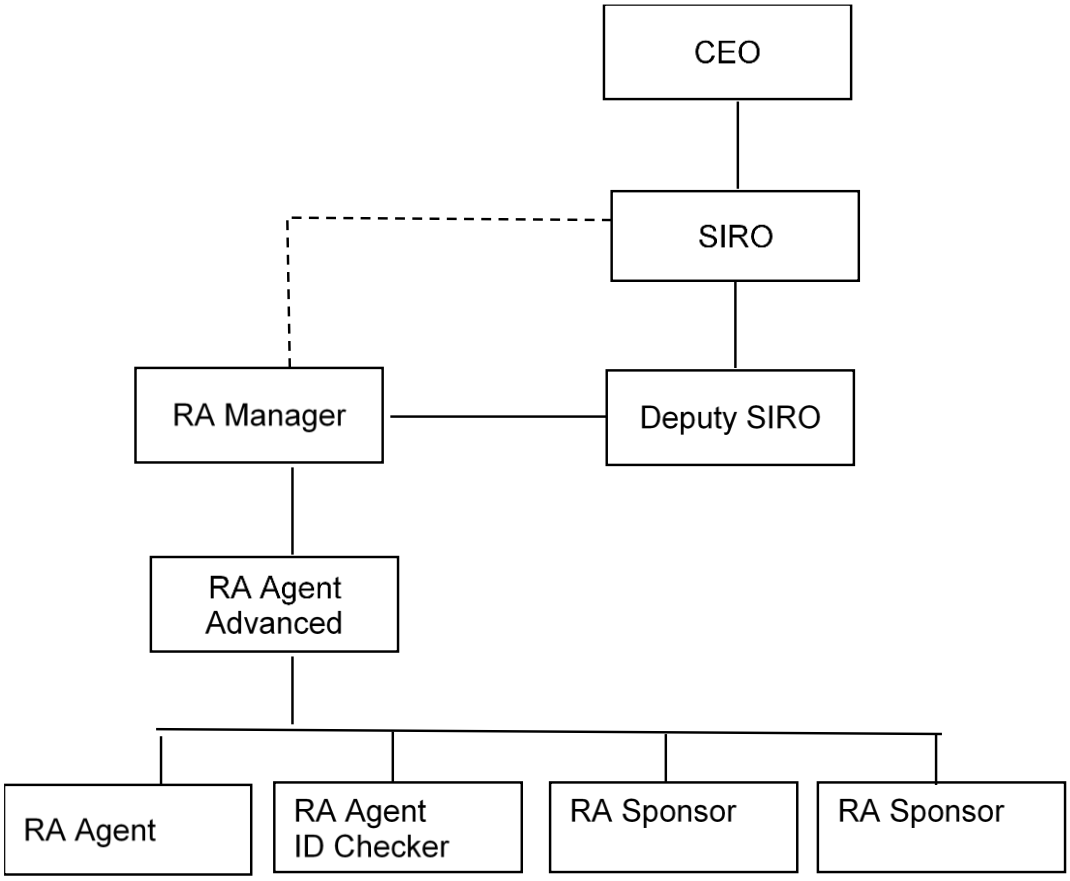
3.10. Application end-users

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

- To keep their pass-codes secret and not share them with anyone, including colleagues.
- To always have their Smartcard available when required and to take reasonable steps to protect it from misuse.
- To never share login sessions with other users. In practice this will require logging in and out at the start and end of each session.

4. Processes and Procedures

4.1. Process overview diagram



4.2. Function of Registration Authority

A Registration Authority (RA) manages the registration and access control processes to the NHS Care Records Service. In essence, the RA ensures that individuals needing to access the NHS Care Records Service, have had their identity rigorously

checked and are assigned appropriate access.

The national policy requires everyone accessing NHS Digital applications to be registered with an individual identity on the National NHS database and to have their access authorised by a Registration Sponsor appointed by the Trust executive. The individual can then be issued with a personal “chip-and-PIN” smartcard that gives them access to the authorised position associated with their role in the NHS.

GMMH will ensure that all Independent Service Providers and contractors who need to use the NHS Digital applications are bound to the Data Protection Act (DPA) 2018, General Data Protection Regulation (GDPR) and the NHS Confidentiality Code of Practice. This will include the process to be followed in cases of a breach and liability issues. GMMH will ensure that its contracting procedures are updated to meet this requirement. The Contracting team will ensure that third party providers have a Confidentiality Policy, DS&P Toolkit and are IG training compliant.

Staff are required to have their smartcard and PIN number available for use at all times at work. Support will be available where a smartcard or PIN have been forgotten or mislaid, but because replacement will unavoidably incur some delay, with some risk to productivity and patient care, staff who persistently fail to produce them when required will be subject to supervisory, and if necessary, disciplinary action. IM&T will monitor this through the Manage Engine portal where requests are generated for replacement RA Smartcards. Reports will be generated monthly and actions taken as follows:

- For a first replacement card, the staff member will receive an email from the RA Manager reminding them of the importance of retaining their card safely.
- A second request will result in an email to the staff member’s Line Manager.
- A third request will result in an email to the Line Manager prompting performance management.

All officers and agents of GMMH Registration Authority will have sufficient training to carry out their tasks in accordance with National Policies and Procedures. GMMH will ensure sufficient Registration Sponsor, Officers and Agents of the Registration Authority are available to support the continual availability of smartcards required for effective healthcare.

GMMH regards loss, theft, misappropriation or misuse of a smartcard as a reportable security incident. Staff will report incidents using the GMMH Trust procedures and will notify Registration Authority of incidents requiring urgent action to protect patients, data or staff.

Information Governance

In order to monitor that the level of security associated with the use of smart cards is both appropriate and compliant with national requirements, the RA manager will engage the Information Governance team to complete annual audits and spot checks as part of the information governance schedules.

4.3. Registration Process

The Registration process consists of three distinct activities:

1. Registration of identity – a user is sponsored to be issued with a Smartcard; has their identity checked to eGif level 3 and a personal details record is created in the Spine User Directory (SUD); this part need only be performed once by a Registration Authority Agent or Manager.
2. Choosing appropriate access to NHS CRS functionality/information (via their profile) and linking it to the SUD record; this may be changed as necessary (by each organisation); a profile requires a sponsor's approval and they are granted by a Registration Authority Agent or Manager.
3. Creating a card to link the user (Smartcard Holder) to their SUD record and access profile(s) and hence allow access to NHS CRS.

4.4. Leavers Process

The Support Central team receive notification of staff leaving the Trust via email notification from HR to the Support Central Outlook inbox. On occasion, notification is also received via a request to ManageEngine.

The Support Central team will ensure that Leavers with active Smartcards have any GMMH Trust Positions set to end on the leave date provided. If the team are subsequently notified that the Leaver has remained within the Trust but moved to a different role, their Smartcard will be updated accordingly with their required Positions, on receipt of a request to the Manage Engine portal. Such requests will require line manager approval to proceed. Where a Smartcard is returned to Support Central being no longer required or damaged, these are destroyed on site via a shredding process.

5. Training Requirements

The Registration Authority will ensure that all RA members and registered users are provided with appropriate training via the RA Manager. Information Governance training is mandatory training for all staff and is completed annually. This training includes awareness and understanding of Caldicott principles and confidentiality, information security, data protection and Freedom of Information. A training needs analysis will be completed via the IG Steering Group to identify the training requirements of those with additional IG responsibilities. This will link into the Trust's overall Training Needs Analysis.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
Monitoring against the policy will be carried by undertaking an audit of compliance.	This will be carried out on an annual basis	audit	reports	Registration Authority Manager	Information Governance Steering Group (IGSG)

7. Resource/Implementation Issues

N/A

8. Risk Issues

Registration Authority Risks are part of overall Information Governance Risks and as such are incorporated into the IM&T Risk Register, which is to be monitored via the IM&T Risk Group, on a monthly basis. Any identified risk can be escalated to the IGSG as appropriate, and all risks of twelve or above will be reported to both the IGSG and the Trust's corporate Risk Group.

9. Requirements, Supporting Documents and References

9.1. Supporting Documents

The key supporting documents are the Trust's Information Management and Technology Strategy and Information Governance Policy.

9.2. References

- Registration Authority Policy V1.0, Spine 2 – IAM Replacement Project, 02 September 2014
- Registration Authorities Setup and Operational Phase 1 release 1, NPFIT-FNT-IMF-IME-0182.02, Version 0.9d, 10 Dec 2004
- User Registration – Sponsor Briefing, NPFIT-FNT-IMD-IME-0184.01RA01 Form – Registration for use of National Programme applications, version 5

10. Subject Expert and Feedback

Advice and support queries in relation to this document should be sent to the author.

11. Review

Trust policy for review is every five years, however this policy will be reviewed annually in line with the Data Security and Protection Toolkit, or sooner in the light of organisational, legislative or other changes.