University Hospitals Birmingham
NHS Foundation Trust

CONTROLLED DOCUMENT

Registration Authority Policy

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE	This policy details the operation of the Registration Authority
Controlled Document Number:	1083
Version Number:	001
Controlled Document Sponsor:	Medical Director
Controlled Document Lead:	Head of Service Delivery, IT Services
Approved By:	Chief Executive
On:	March 2018
Review Date:	March 2021
Distribution: • **Essential Reading for:** • **Information for:**	All Registration Authority Staff Staff with, or requiring a Smartcard, their line managers, sponsors and Divisional/Group managers All Staff

Contents

1. Policy Statement

1.1 The purpose of this policy is to highlight the roles and responsibilities for University Hospitals Birmingham NHS Foundation Trust (the Trust) in relation to the operation of the Registration Authority (RA).

1.2 The RA enables users access to relevant systems based on their position, this is known as Positions Based Access Control. All organisations which run a local RA do so on a delegated authority basis from NHS Digital.

1.3 The following systems require access via a Smartcard and are referred to as relevant systems within the policy:

1.3.1 Summary Care Records (SCR, including Pharmacy, Child Care Protection and Birth Notification Application Midwives);

1.3.2 Oceano

1.3.3 Choose and Book (Advice and Guidance);

1.3.4 Electronic Staff Record (ESR);

1.3.5 SystmOne

2. Scope

This policy applies to those Trust employees requiring a Smartcard to fulfil their role, as defined either through position based access control, or via a designated Sponsor. This includes 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 a relevant system.

3. Framework

3.1 This section describes the broad framework for the Registration Authority Policy.

3.2 The Medical Director shall approve all procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

3.3 Definitions

Choose and Book	Choose and Book gives patients the opportunity to choose the date, time and location of where they would like to go for their treatment. Patients will be offered a choice of four to five care providers for their first new outpatient appointment, which enables patients to be more involved in choosing their healthcare.
CIS	Care Identity Service
e-GIF Level 3	Is a previous inter-governmental standard known as eGIF Level 3. This is a standard of identity assurance determined by the government. 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
NHS Digital	The single Registration Authority under which Trusts have delegated authority to run RA activity locally.
PBAC	Positions Based Access Control.
RA	Registration Authority
SCR	Summary Care Records including Pharmacy, Child Care Protection and SCR Birth Notification Application
SystmOne	SystmOne provides patient information across the community setting.
Oceano	Patient administration system

3.4 Where a new starter or existing employee requires access to one or more of the above systems to fulfil their role, they will require clearance to access that system by issue of a Smartcard. All employees must be registered to obtain this card, which has a chip and a personal identification number (PIN). The Smartcard will be issued following the least privileged principle. Varying levels of access to patient records or workforce information will be assigned, dependent on the job role undertaken and the need to view only details, change details or enter clinical / workforce information.

3.5 Smartcards contain a digital certificate that enables authentication to take place.

3.6 Confidentiality

3.6.1 All users issued with a Smartcard must adhere to the Terms and Conditions of Smartcard Usage, NHS Confidentiality Code of Practice (November 2003) and the Data Protection Act (1998) and any Trust policies on Confidentiality, Information Governance and Security. 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.

3.6.2 Any user trying to access patient information outside of the access rules will trigger an alert report, which will be sent to a nominated Privacy Officer for the Trust. The Privacy Officer will take the appropriate action in line with Trust policies.

3.6.3 Under normal Information governance rules, every community pharmacy has an obligation to ensure its staff access patient information appropriately. The way this is handled with SCR is by using the alert viewer tool (ie. audit reports) to see accesses made and auditing some/all of these accesses. To access tool/reports you need a smartcard with the role 'Privacy Officer' assigned to it. This person is then known as a Privacy Officer (PO).

3.7 Registration Process

The registration process will be managed by the Trust's RA Offices. The RA Offices will maintain local procedures.

3.8 Suspension of Smartcards

During a disciplinary investigation it may be necessary to suspend a user's Smartcard.

3.9 Incident Reporting

3.9.1 Incidents must be reported in line with the Trust's Incident Reporting process or Raising Concerns in the Public Interest (Whistleblowing) Policy and then notified immediately to the RA Manager. The RA Manager will identify any external reporting required, such as to NHS Digital.

3.9.2 Incidents must be reported by any employee who suspects there is a risk to the health of a patient(s), a member of staff, confidentiality or the Trust's reputation.

3.9.3 Examples of incidents include, but are not limited to:

- Smartcard or application misuse, including unauthorised access;
- Theft of a Smartcard;
- Non-compliance with local or national RA policy;
- Any unauthorised alteration of patient or staff data.

3.10 Leavers

3.10.1 It is the responsibility of the Sponsor/Line Manager to ensure that users who leave or take an agreed period of leave from the Trust have their status recorded by the RA Office. The RA Office will process leavers/absentees in line with locally developed procedures by either suspending or revoking the Smartcard. It is the Sponsor's responsibility to notify the RA office of any users who require their Smartcard and User ID to be re-activated.

3.10.2 Suspension of a Smartcard is appropriate for users who will not be in a position to use their Smartcard due to period of absence such as sickness or maternity leave, for a period of longer than 4 weeks duration.

3.10.3 The RA office must keep records to show that access has been revoked. Any Smartcards returned to the RA office must be securely destroyed.

3.10.4 A list of leavers will be supplied to the RA team by the Workforce Information team on a monthly basis.

3.11 Changes to Role

Line managers are responsible for reviewing a member of staff's access to relevant systems when they change role. This includes completing the appropriate paperwork in order to remove/add access.

3.12 Certificate Renewal

3.12.1 RA Managers, RA Agents, and Sponsors can renew users' certificates.

3.12.2 Certificates must only be renewed if they are within three months of expiry or there is the belief that they may have been compromised (i.e. transactions have been found that may not have been performed by the user and the Smartcard has been entirely in the care of the user).

3.12.3 Users can renew their certificates (provided they have not yet expired) via the Self Service Portal without having to visit their local RA Office.

4. Duties

4.1 Group Managers/Clinical Directors

Group Managers/Clinical Directors and Medical Directors will:

4.1.1 Identify and agree all roles within their area of responsibility which require access to a relevant system;

4.1.2 Identify Sponsors and ensure that on an ongoing basis that there are sufficient Sponsors in place within their area of responsibility in order to support the registration process;

4.1.3 Ensure that Sponsors are correctly registered with the RA office using the full authentication process; and

4.1.4 Ensure that the RA office is notified immediately if any Sponsor ceases to fulfil this role and advise of the nominated replacement, and if this individual is not already a Sponsor, ensure that they are correctly registered using the full authentication process.

4.2 Medical Director

4.2.1 Has overall accountability for Registration Authority activity within the organisation;

4.2.2 Reports annually to the Information Governance Group regarding the operation of the Registration Authority;

4.2.3 Signs off the annual RA Information Governance Toolkit Submission; and

4.2.4 Confirms the appointment of RA Managers and Sponsors in writing.

4.3 Sponsors

Sponsors will be responsible for:

4.3.1 Approving user's access to relevant systems and will clarify and agree access in cases of dispute with the Group Manager or equivalent, and/or Clinical Director;

4.3.2 Unlocking Smartcards and renew Smartcard certificates for non RA staff;

4.3.3 Immediately reporting to the RA office any lost, stolen or misplaced cards;

4.3.4 Informing the RA office of any Smartcards that need to be suspended or revoked;

4.3.5 Informing the RA office of any 'suspended' users whose Smartcard and User ID needs to be re-activated;

4.3.6 Ensuring that users within their area are aware of the RA policy and local procedure and their responsibilities in relation to use of and access to the system;

4.3.7 Ensuring that any confidential RA information is held securely in line with Trust policies;

4.3.8 Ensure that users within their area who require registration contact the RA office in order to agree a date and time to attend registration; and

4.3.9 Provide appropriate support to users within their area of responsibility e.g. with the resetting of passwords. Appropriate guidance and training will be provided by the RA office.

4.4 Registration Authority Manager

The Registration Authority Manager will:

4.4.1 Develop the RA Policy and local processes that meet the policy and guidance for the creation of digital identities, production of Smartcards, assignment of access rights, modifications to access and people and certificate renewal and card unlocking;

4.4.2 Implement the RA Policy and RA Processes locally adhering to national guidance;

4.4.3 Assign Sponsors and register RA Agents and Sponsors;

4.4.4 Train RA Agents and Sponsors, ensuring they are competent to carry out their roles and adhere to policy and process;

4.4.5 Facilitate the process for agreeing the Trust's access control positions via Position Based Access Control;

4.4.6 Conduct audits and ensure any actions arising from the outcomes of these audits are undertaken;

4.4.7 Request audits from information asset owners demonstrating users are compliant with the terms and conditions of Smartcard usage;

4.4.8 Verify users' ID to the previous inter-governmental standard known as eGIF Level 3. This provides assurance that the identity is valid across any organisation an individual works within;

4.4.9 Ensure leavers from the Trust have their access rights removed in a timely way;

4.4.10 Ensure that any confidential information is stored securely in line with Trust policies;

4.4.11 Ensure all service issues are raised appropriately locally and/or nationally;

4.4.12 Keep up to date with national policy requirements, initiatives and changes, ensuring that their email address is entered as part of their personal details held within the database of Smartcard users. They are also required to subscribe to the national email address; and

4.4.13 Have a line of professional accountability to uphold good RA practice to NHS Digital, and report relevant incidents.

4.5 Advanced Registration Authority Agent

The Advanced Registration Authority Agent will be responsible for:

4.5.1 Registering Smartcard users;

4.5.2 Verifying users' ID to e-GIF level 3 when they register users;

4.5.3 Searching and viewing closed users;

4.5.4 Re-opening closed users;

4.5.5 Creating positions and workgroups;

4.5.6 Modifying positions;

4.5.7 Assigning individuals to positions;

4.5.8 Reviewing positions definitions including assigned users;

4.5.9 Assigning individuals to workgroups;

4.5.10 Managing request lists;

4.5.11 Accessing reporting and run reports;

4.5.12 Cancelling Smartcards;

4.5.13 Closing user accounts for staff members that leave the NHS;

4.5.14 Unlocking Smartcards and renew certificates;

4.5.15 Viewing all requests; and

4.5.16 Print Smartcards and grant access assignment requests.

4.6 **Line Managers**

Line Managers will be responsible for:

4.6.1 Identifying all roles within their area of responsibility which require access to the system and ensure that all employees, are provided with appropriate access;

4.6.2 Ensuring that all roles that involve access to the system 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;

4.6.3 Ensuring that current/future users attend the appropriate meetings with a member of the RA office to enable the Smartcard to be issued, providing users with authorised time away from the department where applicable;

4.6.4 Ensuring that all new starters within their area of responsibility receive training in order to be able to access the relevant system;

4.6.5 Ensuring that all Smartcard users are aware of the contents of this policy and any accompanying procedure and their responsibilities in relation to use of and access to the relevant system;

4.6.6 Informing the Sponsor/RA office of any leavers, starters and staff changes;

4.6.7 Informing the RA office of any Smartcards that need to be suspended or revoked;

Informing the RA office of any 'suspended' users whose Smartcard and User ID needs to be re-activated; and

4.6.8 Informing the RA office of any employee who is expected to be absent from work for a period of 4 weeks or longer.

4.7 Registration Authority Agent ID Checker

The Registration Authority Agent ID Checker is responsible for checking users' identification and granting the digital identity;

4.8 Local Smartcard Administrator – Functions in CIS

Users assigned to the local Smartcard Administrator role in CIS only have the ability to renew certificates and unlock Smartcards for users that have been assigned to a CIS RA Role.

4.9 Employees

All Employees are responsible for ensuring:

4.9.1 They use their Smartcard responsibly and in line with their access rights and terms and conditions of smartcard usage;

4.9.2 They inform the Sponsor (who in turn must inform the RA office) immediately if their Smartcard is lost, stolen or misplaced;

4.9.3 They report any misuse of the system in line with this policy;

That their Smartcard and log-in details remain confidential. In particular PCs must not be left logged in and unattended; Smartcards must not be left unattended and must not be shared with other users. Any breach of the above could lead to action being taken in line with the Trust's Disciplinary Policy;

4.9.4 That they accurately complete the necessary paperwork, provide suitable identification and attend any appropriate appointments in order to register on the system or have their Smartcard updated or re-issued; and

4.9.5 That upon issue they sign the electronic Terms and Conditions of Smartcard Usage.

5. Implementation and Monitoring

5.1 Implementation

5.1.1 This policy will be available on the Trust's Intranet and external internet site. The policy will also be disseminated through the management structure within the Trust;

5.1.2 All users must undertake training before being allowed access to the relevant system.

5.1.3 The RA Agent is responsible for ensuring that the electronic terms and conditions of Smartcard Usage are read and signed, prior to user being issued their smartcard

5.1.4 The Sponsor/Line Manager 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 must be undertaken as part of the local induction process.

5.2 Monitoring

Appendix A provides full details on how the policy will be monitored by the Trust.

6. References

Data Protection Act 1998

Information Governance Toolkit

National Registration Authority Policy (NHS Digital)

Registration Authorities Operational and Process Guidance (NHS Digital)

Terms and Conditions of Smartcard Usage

7. Associated Policy and Procedural Documentation

Data Protection and Confidentiality Policy

Disciplinary Policy

ICT Acceptable Use Policy

IT Security and Access Control Policy

Information Governance Policy

Policy for Raising Concern in the Public Interest (Whistleblowing)

Policy for the Reporting and Management of Incidents including Serious Incidents

RA Procedure

Appendix A **Monitoring Matrix**

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO	MONITORING PROCESS	MONITORING FREQUENCY
Annual Audit of Registration Authority activity	RA Manager	Information Governance Group	Audit to include as a minimum: -The issue of Smartcards -The management of changes to Smartcards including leavers -Signing of Smartcard Terms and Conditions. -The profiles associated with users in relation to what they do -Identity management -Security of supplies and equipment	Annual
Information Governance Toolkit	RA Manager	Information Governance Group	Completion of IG Toolkit sections 303 and 304 via attendance at IG Toolkit Group. This includes seeking assurance from relevant systems managers in relation to Smartcard users accessing information in line with Smartcard terms and conditions of usage. Annual Submission in March.	Annual