Improving Health
and Wellbeing for Walsall

REGISTRATION AUTHORITY
POLICY

NHS

Walsall Clinical Commissioning Group

Registration Authority (RA) Policy
For
Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 17 September 2018
Signed: Chair of the committee
Signed: Designated Senior Officer

Version:	3.0
Status	Review
CCG Lead	Simon Brake, Chief Officer
Senior Officer responsible	Informatics Manager
Ratified by:	Audit & Governance Committee
Date ratified:	17 September 2018
Date Policy is Effective From:	Date of ratification
Review date:	February 2019
Expiry date:	March 2019
Date of Inequalities Impact Assessment	
Target audience:	GPs, GP Practice Staff, Pharmacy Leads and Pharmacy Staff
National Documents	
CCG linked documents	IG policy IMT policy
Distribution of the document	Email and team meetings
Implementation of the document	Immediate
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	

CONTRIBUTION LIST
Key individuals involved in developing the document

Designation
Primary Care Informatics Manager
Risk and Assurance Manager
Head of Primary Care & Medicines Management

Circulated to the following for consultation

Name/Committee/Group/	Designation
SQP Committee	
Head of Primary Care & Medicines Management	

Comments received from consultation

Name/Committee/Group	Comments
Audit & Governance	

Committee (A&G)	

Version Control Summary

Significant or Substantive Changes from Previous Version
This Patient Experience Strategy has been ratified by SQP for Walsall CCG. It was written by.

Version	Date	Comments on Changes	Author
1.0	01/11/2013	Drafted policy for General Practice staff and Pharmacy Staff working in Walsall CCG	Barbara Yates
2.1	August 2018	Reflect Data Protection Act 2018 and General Data Protection Regulation	Serena Ellis

Contents

1. Introduction

The process of gaining access to National Programme applications like Choose and Book, Summary Care Record and EPS is called National Programme Registration. This function is operated within NHS Walsall CCG by a locally configured Registration Authority (RA) which is set up according to nationally defined guidelines and policy (National Registration Policy and Procedures). This is to ensure that they

comply with the 'NHS Care Record Guarantee' and 'NHS Confidentiality Code of Practice' and that any individual providing healthcare services to the NHS directly, or indirectly, has appropriate access to NHS Care Record Systems (NHS CRS) information in accordance with their role.

From April 2008, NHS Employment Check Standards became a requirement in the NHS as part of the annual health check. Similarly, robust identity checks were also enforced using the same identity management standards carried out by an NHS organisation's Registration Authority (RA) to verify an individual's identity before allowing access to NHS Care Records Service (NHS CRS) applications. Combining these two parallel activities into a single **Integrated Identity Management** (IIM) process has proven to deliver significant benefits through HR/RA Process Integration and the move to Position Based Access Control (PBAC), both supported by the following new software applications.

Integrated Identity Management significantly improves access control to NHS CRS systems containing person identifiable information through revised business processes and the introduction of two new software applications:

- **User Identity Manager (UIM)** is the new registration software to manage NHS CRS access control across General Practices and Pharmacies.

Significant benefits and improved Information Governance has been achieved in implementing the UIM Interface which was activated on the 1st April 2011.

See Appendix 1 for outlines of the key processes requirements.

2. Scope
This document defines the RA operating models for:
1. The RA arrangements for Primary Care e.g. General Practice staff
2. The RA arrangements for local Pharmacy staff
3. The RA arrangements for those organisations which currently receive RA services for PCT's e.g. Badger OOH, Social enterprises (CSU staff based locally, NHS England staff based locally.

3. Statement of Intent
This Policy ensures a consistent process when determining an employee's NHS CRS access and acts as an enabler for the implementation of any future applications. It also protects data security in relation to patient and staff records.

4. Registration Authority
NHS Walsall CCG needs a Registration Authority to manage the registration, creation, distribution and use of Smartcards.

The Registration Authority is an official or committee within the CCG with appropriate organisational authority who is responsible for ensuring that all aspects of registration services and operations are performed in accordance with National Policies and procedures. http://systems.hscic.gov.uk/rasmartcards/planning/uimop/index_html

They are responsible for providing arrangements that will ensure tight control over the issue and maintenance of electronic Smartcards, whilst providing an efficient and responsive service that meets the needs of the users.

Smartcards are the responsibility of the user and should be treated with care and protected to prevent loss or damage.

The NHS Walsall CCG Registration Authority is made up of the following personnel:

- Registration Authority (RA) Manager
- Registration Sponsor (Caldicott Guardian)
- Registration Authority (RA) Agents

4.1 Registration of RA Manager
To register a RA Manager to the organisation the Chief Executive is required to put a request in writing to the RA Lead at the Strategic Health Authority.
All other roles are assigned at a local level.

4.2 Position Based Access Control (PBAC)

The CCG's RA team and IT Business Change team has reviewed all of the NHS CRS access used within the organisation and established the Access Control Positions required. These Access Control Positions have been identified and now form the basis of templates that will identify activity codes for every role.

4.3 Access Control Position (ACP) Management
Access Control Positions could periodically be reviewed and may need to be amended, removed or new positions created due to:
- Identification of amendment through the audit review process
- Notification from a system supplier that an amendment is required
- A new NHS CRS system being implemented in the CCG
- A new NHS CRS ACP
- A brand new role being created in the CCG
- Trust Acquisitions or Mergers

Whatever method is used for requesting the change, the process for change will follow the authorisation process established within the Trust. Change will need to be approved by the Registration Authority Manager before the amendment is made to the Access Control Position

5. Registration and Access for General Practice
A nominated 'Sponsor' will need to be identified within both the GP Practice and Pharmacies to undertake a number of Registration Authority activities within UIM such as creating a new user, modifying a user, closing a user and management of smartcards i.e. unblocking and renewing certificates. The Sponsor is bound by the roles and responsibilities aligned to this role and approve an individual's request for a particular set of position based access roles within their practice/pharmacy. They should work with RA agents to maintain access to NHS CRS compliant applications within their area of responsibility that is consistent with the Confidentiality: NHS Code of Practice, Department of Health, Gateway reference: 2003.

5.1 New Starters
The Practice Manager or Lead Pharmacist (as the Sponsors) will determine whether a new staff member requires a NHS Smartcard and activate this request in UIM

This policy is subject to further revision and will be reviewed on a six monthly basis

under the section 'Create User'. They will verify and validate the new starters identification documents, create the request in UIM, then contact the RA Office via an electronic request using the # SmartcardsPrimaryCare@walsall.nhs.uk email address to arrange a meeting with the RA Agents for the new starter to have their photograph taken, produce their ID documents for verification, and to be given a Smartcard. The photograph is saved in a secure shared drive (INFCBO\Staff Photographs\GPs\Pharmacy) to ensure it is accessible to the RA team.   This enables the Smartcard to be produced and access to become active and the user's record will be associated to the relevant NHS CRS systems via the UIM interface ensuring access via the Smartcard without delay.

5.2 Personal Information - Change Management
Any amendment to the following personal information will be completed by the   RA Sponsor using the Modify User section of UIM. Changes to be modified are:
- Title
- Surname
- First name
- Middle name

The Sponsor will verify and validate the modification identification documents, create the request in UIM, then contact the RA Office via an electronic request using the # SmartcardsPrimaryCare@walsall.nhs.uk to arrange a meeting with the RA Agents for the user to produce their ID documents for verification, and to be given a Smartcard. Once a message is received for requesting and approving, it can be granted in UIM and a smart card produced by the RA Agent

5.3 Leavers
If the User is permanently leaving the NHS
The Sponsor will be responsible for deactivating staff that are leaving the NHS organisation altogether within UIM under the 'Close User' section.
Reasons for leaving are:
- Retirement
- Death

Once the message is received for requesting and approving, it can be granted in UIM by the RA Agent and the inactive Smartcard can be destroyed by the Sponsor.

If the User is transferring to another NHS organisation they are required to retain the Smartcard and contact the RA Agents via an electronic request using the # SmartcardsPrimaryCare@walsall.nhs.uk immediately to ensure that their NHS Walsall CCG profile is removed automatically.

5.4 Temporary Suspension of NHS CRS Access
There are times within the employee life cycle when access to NHS CRS applications need to be temporarily suspended. This includes the following but is not exhaustive:

- Maternity Leave
- Long Term Sick Leave
- Adoption Leave
- Suspension from Duty
- Career Break

The Sponsor MUST contact the RA Agents Office to notify the RA Agents if any of the above criteria applies to a staff member. This MUST be submitted via an electronic request using the # SmartcardsPrimaryCare@walsall.nhs.uk email address. Once the request has been completed the email communication will be archived to provide an audit trail.

The RA Agents will then temporarily suspend the Smartcard however once the staff member has returned to work, a further electronic request, MUST be submitted confirming the return to work date. UIM will be updated and all access to NHS CRS systems will be re-instated.

6. Temporary Workforces

6.1 Indirectly Deployed External Temporary Workforce (Agency and Locum)

All agency and locum workers will be created and managed via UIM. Actions through UIM require the 'approval' and 'granting' stages, managed by the RA Agents team to become active.

6.2. Registrations and Access

NHS CRS systems access for agency and locum workers will be requested by the Sponsor; the application required and the role being undertaken MUST be identified.

The individual will register for a Smartcard with the RA Agents team. If the user has not been previously registered on UIM a manual registration is required; in addition to the standard RA ID checks National Insurance number and date of birth have to be provided.

RA staff will determine and assign the NHS CRS Access Control Position most appropriate for the user.

Once the request has been completed the email communication will be archived to provide an audit trail.

If the agency or locum worker stops working the Sponsor responsible **MUST** inform the RA team so that access can be revoked immediately.

7. Smartcard Management

7.1 Blocked cards

Users will need to have their Smartcard pass-code re-set if:
- the pass-code has been forgotten
- they suspect that it may be known by another
- it has been locked out because of three failed login attempts

Sponsors and identified Smartcard/RA Administrators within each practice/pharmacy are responsible for pass-code re-sets and certificate renewals.

This task can only be carried out by the Sponsors, or Smartcard/RA Administrators and the smartcard holder MUST be present throughout this process.

7.2 Smartcard expired

When a smartcard expires, the Sponsor will notify the RA Agents office via the # SmartcardsPrimaryCare@walsall.nhs.uk to alert the RA Agents that a new card will need to be printed and issued to the user.

The smartcard will need to be collected from the RA Agents office and this will be the sole responsibility of the User – RA Staff are not able to deliver smartcards to staff however a nominated person within the practice/pharmacy is able to collect the smartcard on the users behalf when the need arises.

7.3 Smartcard certificate expired

Sponsors and identified Smartcard/RA Administrators within each practice/pharmacy are responsible for certificate renewals.

This task can only be carried out by the Sponsors, or Smartcard/RA Administrators and the smartcard holder MUST be present throughout this process.

8. Lost, stolen and damaged cards

Lost, stolen and damaged Smartcards must be reported to the RA Team as soon as is practicable via an electronic request using the
SmartcardsPrimaryCare@walsall.nhs.uk. The RA Agent will arrange to have the smartcard revoked and replaced as soon as possible.
The RA Team will then:
1. Meet the User face-to-face to verify their identity and issue a replacement NHS Smartcard. The User's identity should be confirmed by the photograph in UIM. If the identity still cannot be verified the User will be required to produce documentary evidence of their identity.
2. The RA Team will cancel the old lost/stolen/misplaced/damaged NHS Smartcard.
3. The RA Team will issue a replacement NHS Smartcard.

8.1 Smartcard Misuse

All General Practice and Pharmacy staff members are required to have general responsibility for the security of information that they create or use in the performance of their duties. All staff members are required to comply with information security procedures, as detailed in the Information Management & Technology policy including the maintenance of data confidentiality and data integrity.

8.1.1 Each staff member is responsible for the operational security of the information systems, including records management, smartcards and pass-codes they use and should be aware of the local security policies for their area of work. It is the responsibility of all staff members to report any suspected or known breaches of security within information systems to the RA Agents or Information Governance department for consideration. Suspected smartcard misuse may be reported directly to the RA Manager; this will be reported to the Information Governance department via the CCG's incident reporting system.

8.1.2 A breach of these policies and procedures whether accidental or intentional will be considered a disciplinary offence; and bought to the attention of the responsible GP within the practice or the lead Pharmacist within the pharmacy.

8.1.3 Classifications for misuse of a Smartcard include but are not exhaustive to:

- Smartcard and pass-code being shared with another user
- Using another's Smartcard and pass-code

- Leaving Smartcard unattended
- Pass-code being stored with Smartcard
- Leaving access to NHS CRS applications unguarded
- Accessing data outside of the remit required to carry out role

Employees who have Smartcard access should ensure they understand and comply with information security policies and are fully aware of their responsibilities.

8.1.4 Smartcard misuse by a temporary worker will result in a full investigation and may result cessation of agency or locum workers.

9. Equipment, Consumables, Maintenance and Security of Smartcards

9.1 All RA equipment will be documented on a local asset register as detailed in the Information Management and Technology Policy; this will include maintenance contact details.

9.2 To ensure that national and local policies are being followed RA documents will be used and stored appropriately. Old paper based documentation (RA forms) will be scanned and stored securely.

9.3 Unused Smartcards will be stored safely.

9.4 Printed Smartcards will be stored securely prior to distribution.

10. Roles and responsibilities

10.1 Accountable Officer – overall Organisational accountabiliy and is required to delegate authority for Registration Authority within the CCG

10.2 Caldicott Guardian – a senior clinician who has ultimate responsibility for the confidentiality of patient information throughout the CCG. Recorded as Registration Sponsor for UIM interface purposes and is required to authorise any changes for the RA Manager to the Strategic Health Authority.

10.3 RA Manager – selected by the Chief Executive and is responsible for the set up and day to day running of the CCG Registration Authority service. They must ensure that all RA procedures are carried out in accordance with local and national policy. The RA Manager is also responsible for:
- Taking appropriate action where misuse of a Smartcard is identified or suspected.
- Amendments or additions to Position Based Access Control (PBAC)
- RA audits

10.4 RA Agents – are responsible to the RA Manager for ensuring that local and national processes are followed. All incidents, misuses, anomalies and problems will

be reported to the RA Manager. Day to day responsibility for RA card management and for the accurate management of information on UIM sits with this role.

A full llist of Roles and Responsibilities can be founds under Appendix B

11. Audit / monitoring arrangements

e.g. Smartcards, Access Control Positions, terms and conditions

11.1 Access Control Positions

The RA Manager will review all Access Control Positions and amend access rights as appropriate. This will carried out on an annual basis; there will also be a requirement for review on an ad-hoc basis when a request for additional access is made.

11.2 Smartcard Management

The RA team ensure electronic terms and conditions are read and accepted as part of the card issuing process. Evidence of electronic acceptance of Smartcard terms and conditions will be provided by a report from the Card Management System.

11.3 Work lists

These will be checked daily to ensure actions in UIM are managed and maintained in real time. This ensures that requests for access are granted, amended and revoked in a timely manner.

12. Training

12.1 RA Staff - Training on Registration Authority systems is a mandatory element of training for the CCG's RA staff. This will maximise the staff's knowledge of the system to ensure that they have the ability to use the system as per the requirements specified by the CCG and Health & Social Care Information Centre.

12.2 UIM Stand Alone Training

Walsall NHS CCG Registration Authority staff will also be required to complete the relevant additional stand-alone UIM e-learning material. This is available on the Health & Social Care Information Centre Registration Authority web pages http://systems.hscic.gov.uk/rasmartcards

Following the completion of the relevant e-learning material the trainee must notify the RA Manager or an RA Agent so that this can be documented by the RA Manager in accordance with the latest version of the IG Toolkit.

Appendix 1

13. RA Manager Responsibilities

The responsibilities an RA Manager has for their organisation are:

- to be familiar with and adhere to this document and Registration Authorities: Governance Arrangements for NHS Organisations;
- to assign, sponsor, and register RA Agents (where permitted under governance arrangements); ensuring there are sufficient resources to operate the registration processes in a timely and efficient manner;
- to ensure users have only one NHS CRS Smartcard issued to them showing their User's Unique Identifier (UUID) and photograph, and that users are aware of their responsibilities relating to Information Governance and Smartcard use. The issue of more than one NHS CRS Smartcard to a user is not permitted.
- to ensure that the National Registration policy and processes identified in this document and in the online guidance are adhered to and that any local processes support the National policy and processes. The guidance may be found at http://nww.hscic.nhs.uk/iim;
- to identify areas where the organisation's business processes need integrating to minimise risk and duplication of effort. Examples of these include HR processes for starters, leavers, suspensions, terminations, and approved leave;
- to implement an audit policy and identify a secure locked area for the storage of all registration and associated information in accordance with the Data Protection Act 2018 and the General Data Protection Regulation. This includes RA Manager, RA Agent, and Sponsor assignment documents; RA forms; RA reports; and inter-organisation agreements. All RA forms must be clearly marked with the user's UUID number and filed in a designated area (typically in HR/Personnel) that the RA have access to.

  Note: RA records need to be retained in accordance with Department of Health Gateway document reference 5130 or its successor:

- to report all RA related security incidents and breaches to the organisation's Risk Management Team, Information (Caldicott) Guardian, and Executive Management Team or as indicated by the local Information Governance policy;
- to escalate all queries that cannot be resolved locally to the next level in the RA hierarchy;
- to disseminate National RA information to interested parties. For example, communicate PBAC and access control information to sponsors;
- to ensure there is a sufficient supply of Smartcards and RA hardware, including access to the Card Management System (CMS) for sponsors

(Smartcard unlocking and certificate renewal), and communicate technical requirements to the Information Technology team;
- to register RA Managers who have letters of assignment from organisations in the cascade;
- to ensure there is a process for the renewal of Smartcard certificates;
- when performing RA Agent duties, observe the same responsibilities as the RA Agent;
- to ensure your (RA Manager) contact details including email address and telephone number are recorded in the Spine User Directory.

13.1 RA Agents Responsibilities

The responsibilities an RA Agent has for their organisation are:

- Complete the e-learning modules available via the NHS NSCIC website
- Complete the required Information Governance training
- Complete any local training requirements
- Be familiar with and adhere to this document and Registration Authorities: Governance Arrangements for NHS Organisations;
- check the users identity according to the NHS Employers Identity guidance to e-GIF level 3;
- Ensure users have only one NHS CRS Smartcard issued to them showing their User's Unique Identifier (UUID) and photograph, and that users are aware of their responsibilities relating to Information Governance and Smartcard use. The issue of more than one NHS CRS Smartcard to a user is not permitted. grant previously approved and granted positions to users who have been approved by a sponsor to be assigned to that position;
- Implement the process identified in the local policy for enabling locum, agency, and bank staff access to NHS CRS compliant applications;
- 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;
- Renew a user's Smartcard certificates if confident of the user's identity.
- Unlock a user's Smartcard and reset logon Passcodes;
- Ensure your (RA Agent) contact details including email address and telephone number are recorded in the Spine User Directory.

13.2 Sponsor Responsibilities

Sponsors may have different responsibilities depending on their function within the organisation.

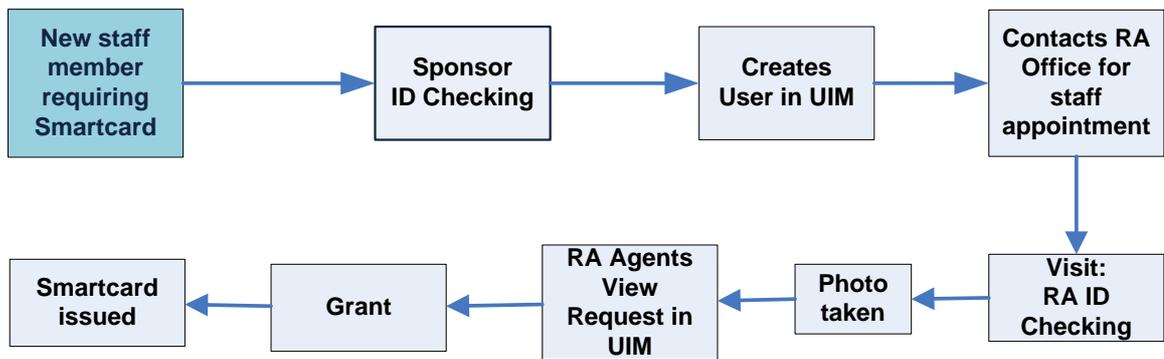The responsibilities a sponsor has for their organisation are:

- Complete the required Information Governance training
- Complete Walsall CCG local training requirements
- Approve user registration requests as defined by the Executive Management Team and the organisation, or if one is in place, as defined by the inter-organisational agreement approved by the Executive Management Team
- Ensure users have only one NHS CRS Smartcard issued to them showing their User's Unique Identifier (UUID) and photograph, and that users are aware of their responsibilities relating to Information Governance and Smartcard use. The issue of more than one NHS CRS Smartcard to a user is not permitted. grant previously approved and granted positions to users who have been approved by a sponsor to be assigned to that position;
- 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.
- Work with RA agents to maintain access to NHS CRS compliant applications within their area of responsibility that is consistent with the Confidentiality: NHS Code of Practice, Department of Health, Gateway reference: 2003. This includes access profile change and removal, and the revocation of Smartcards and Smartcard certificates.
- Be familiar with the applications they sponsor users for via briefing material from the application providers.
- to report all RA related security incidents and breaches to the organisation's RA Manager immediately
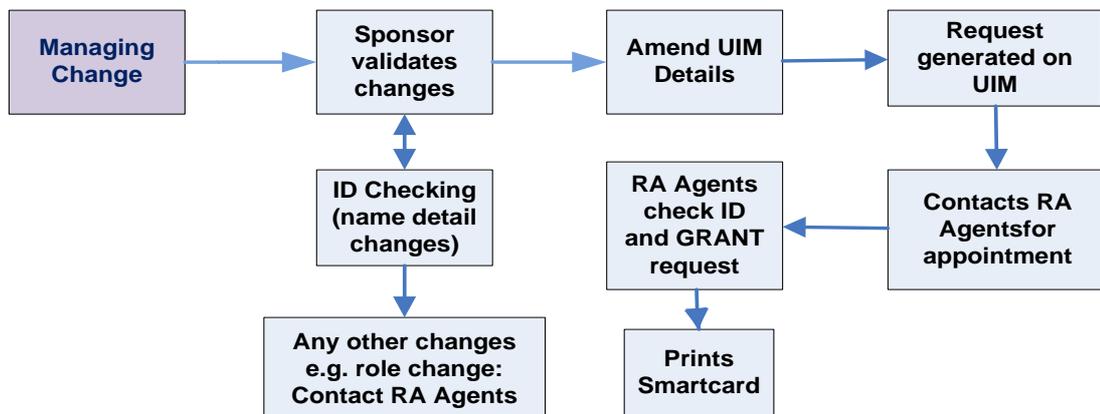
Sponsors may

- Renew a user's Smartcard certificates if confident of the user's identity.
- Unlock a user's Smartcard and reset Passcodes.
- Create a new request for a user via the UIM application
- Modify a user within the UIM application
- Close a user if leaving the NHS entirely

This policy is subject to further revision and will be reviewed on a six monthly basis

Sponsor Flow Chart

New Starter Process:

New staff member requiring Smartcard → Sponsor ID Checking → Creates User in UIM → Contacts RA Office for staff appointment → Visit: RA ID Checking → Photo taken → RA Agents View Request in UIM → Grant → Smartcard issued

Modify User: Personal Detail Changes:

Managing Change → Sponsor validates changes → Amend UIM Details → Request generated on UIM → Contacts RA Agents for appointment → RA Agents check ID and GRANT request → Prints Smartcard

Sponsor validates changes ↕ ID Checking (name detail changes) → Any other changes e.g. role change: Contact RA Agents

Staff Leaving Process:

Leavers → NHS Exit Retiring Deceased → Sponsor Closes User in UIM → RA receives request and closes user → Sponsor destroys smartcard

Leavers → NHS Organisation change → Sponsor Contacts RA Agents

This policy is subject to further revision and will be reviewed on a six monthly basis

This policy is subject to further revision and will be reviewed on a six monthly basis