North West London
Collaboration of
Clinical Commissioning Groups

North West London Collaboration of Clinical Commissioning Groups Registration Authority Policy

Version 2.0

DOCUMENT STATUS:	Final
DOCUMENT OWNER:	Craig Thomas (Registration Authority Manager) Raphael Danladi (Registration Authority Manager Christine Dunne (Deputy Director, Primary care systems)
DATE ISSUED:	2nd July 2020
DOCUMENT RATIFIED BY:	NWL CCGs Governing Bodies
DATE RATIFIED:	September 2020
DATE TO BE REVIEWED:	Annually

CONTENTS

Introduction

The Registration Authority is the governance framework within which NHS organisations can register individuals as users of the NHS Care Records Services (CRS) and other IT services. The North West London Collaboration of Clinical Commissioning Groups (NW London CCGs) Registration Authority (RA) function is a pre-requisite for access to NHS Spine based applications controlled by NHS Digital ensuring maintenance of confidentiality and security of patient information. Having a common and rigorous approach to how users are registered and given access to the NHS Spine Services and other services is an integral part of the organisations governance requirements.

The smartcard is the card issued to the user by the Registration Authority and contains an electronic chip that is used to access the NHS Digital and NHS spine services and applications, along with a PIN. The chip itself does not contain any personal information, providing only a secure link between these services and the database holding the users information and access rights. The combination of Smartcard and PIN helps protect the security and confidentiality of patient information.

As more national applications and clinical systems are released in line with NHS Digital programmes, the RA function and the NHS smartcard plays an increasingly vital role in the continued development of information security and patient care, both of which constitute core aspects of the CCGs stated vision and values.

The process of gaining access to these National Applications, for example ERS, EPS, SystmOne, EMIS Web, Secondary User Services (SUS) and Summary Care Records is carried out by the Registration Authority.

Access to local systems and applications are managed through a single sign-on process *(Smartcard access)* and use the security aspects of the national database to manage smartcards. All staff that require access to either national or local electronic information systems must be processed through the RA procedures.

Unauthorised access, modification, transfer, disclosure, or deletion of computer held records are criminal offences under the Computer Misuse Act 1990. An offender is liable to a fine, a five years imprisonment or both. Such offences will constitute gross misconduct and may result in summary dismissal. Unauthorised access, modification, transfer, disclosure, or deletion of manual records may be subject to disciplinary action as may misuse of the Trusts' E-mail and Internet services.

This policy describes procedures for the operation of the Registration Authority (RA) within the organisation.

Scope

It is intended that this document is used by the following people:

- All users of NWL CCGs RA Service: NWL CCG staff, GP practices, Pharmacists, Independent Sector Healthcare Providers, temporary locum and Bank staff and NHS Digital Application Leads.
- NWL CCG Human Resources personnel NWL CCG ICT Services personnel

- NWL CCG Information Governance Specialists including Caldicott Guardian
- NWL CCG CYBER SECURITY
- NWL CCG Board Members

Registration Authority

The Registration Authority (RA) is an official department within NWL CCGs with appropriate organisational authority who are responsible for ensuring that all aspects of registration services and operations are performed in accordance with National Policies and procedures. 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.

The CCGs Registration Authority is made up of the following personnel:

- Registration Authority Managers
- Registration Sponsors
- Registration Agents

RA Manager		
	• Setup Registration Authority • Manages roll out of smartcard access • Performs RA Managerial function	• Can perform Agent role • Has higher permissions on system than Agent • Has access to Reporting Tool in CIS (Care Identity Service).
RA Sponsors		
	• Checks user credentials • Decides system access based on role • Ensures access to patient record security on system	• Has fewer permissions than Agent • Can reset PIN numbers
RA Agents		
	• Confirms photo ID matches applicant • Enters users onto the Spine User Directory (SUD) • Creates smartcards • Administers SUD and smartcard access	• Can view, create, amend, delete users in Care Identity Service (CIS) • Can create smartcards • Can manage certificates in CIS (Care Identity Service).

The RA services available to NWL CCG users will be:

- User Registration
- Role Profile maintenance
    - o adding Role Profiles

    - changing Role Profiles
    - deactivating Role Profiles
- Revocation and cancelling of Smartcards
- User Suspension
- PIN/Pass-code resetting
- Smartcard renewal and exchange
- Management of fall-back smartcards
- Auditing user access

The above services will be available during the NWL CCG core hours, 9am – 5pm, Monday to Friday. Registration Services outside of core hours can be arranged for project support or pre-arranged support services. .

Compliance to Recommended Guidelines

NWL CCG will comply fully with the latest published National Policies and Procedures identified in the following documents:

- Registration Authorities Operational Process and Guidance (available from https://digital.nhs.uk/services/registration-authorities-and-smartcards).
- Registration Policy and Practices for Level 3 Authentications (available from https://digital.nhs.uk/services/registration-authorities-and-smartcards)
- The NHS Confidentiality Code of Practice (available from https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/confidentiality).
- CIS Acceptable Use Policy, Terms and Conditions (available from https://uim.national.ncrs.nhs.uk/urswebapp/viewTermsAndConditionsDashboard

Roles and Responsibilities

NWL CCGs Shared Services Senior Management Team (SMT)

The SMT have identified and confirmed the selection and appointment of an RA Manager for the NWL CCGs.

RA Manager

The RA Manager is selected by the NWL CCGs and is responsible for the set up and day to day running of the organisations RA service. The RA Manager must ensure that all RA procedures are carried out in accordance with local and national policy.

RA Managers will report significant incidents to the IG Manager and Cyber Security Lead adhering to the Incident Reporting Policy.

RA Agents activities will be audited by the RA manager and IT security on a quarterly basis using the Care Identity Service to check the correct process and methods are being adhered to

RA Sponsors

Sponsors are appointed and entrusted to act on behalf of the RA Team determining who should have what access and maintaining the appropriateness of that access. They have the following responsibilities:

- Ensure that they are familiar with the extent of the functionality and information access a role profile may give a user on CIS
- Ensure that they are familiar with the users need for access to functionality and information
- Ensure that the role profile associated with a user is appropriate
- Escalate any role profile problems to the RA Manager
- Work with RA to maintain appropriate access to NHS Spine Service compliant applications for users within their area of responsibility which is consistent with the NHS Confidentiality Code of Practice (as available on the NHS Digital site). This will include access to profile change and removal, instigating the revocation of Smartcards and Smartcard certificates where required.
- Complete the appropriate parts of the RA forms and any other material which supports the issue/revocation of a Smartcard and the role profiles associated with the card
- Report any security breaches to the RA Manager via the organisation's Incident Reporting process. This includes smartcard sharing, smartcard misuse, inappropriate access and leaving the card unattended.
- If a user is leaving the NHS this will need to be reported to the RA team their smartcard will need to be returned to the RA team or destroyed securely. .

Sponsors will be held accountable by NWL CCGs for their actions. Sponsors are responsible to the organisation to ensure only appropriate access to NHS Spine Applications is granted.

Sponsors will be identified by the RA Manager as being suitable persons by virtue of their status and role. Sponsors will be registered by an RA Team. Sponsors will be staff with sufficient seniority to understand and accept the responsibility required. Registration Sponsors are responsible to the RA Manager for the accuracy of the information on the national smartcard forms found on the NHS Digital website https://digital.nhs.uk/services/registration-authorities-and-smartcards/care-identity-service/forms The list of sponsors are available to all RA staff is found on the CIS System . This report will be available via the reporting tool on CIS.

It is the Sponsor's responsibility to inform the RA Agent/Manager of any required changes to access positions and profiles. NWLCCGs leavers' details will be forwarded to the RA Team by Human Resources and / or Managers. Sponsors are required to ensure their staff lists are kept up-to-date on the Care Identity Service.

Appointment of Registration Sponsors

The NWL CCGs has approved the following process for appointing the Registration Sponsors:

Currently NWL CCG sponsors are:

- Heads of Services and departments
- Lead General Practitioners
- Practice Managers

The appointing of a new sponsor is tied into the RA registration process. All Sponsors are required to provide documentary evidence to prove their identity.

RA01 forms must be completed to the point of identity documents being noted in the presence of the user being registered. The form will then be hand delivered or emailed to the designated sponsor for his/her signature. RA02 forms may be hand delivered or emailed to RA Agents for processing. Registration Sponsors are responsible for making sure that National Programme application users are given the appropriate level of access needed to perform their job.

The areas of responsibility with respect to NHS Spine Application user access should be clearly defined for each Sponsor.

Sponsor Reporting

Registration Sponsors and Agents will report any RA related incidents, using the organisations incident reporting procedure to the RA Manager. Additionally Sponsors and RA Agents will report any operational difficulties especially where these have patient healthcare implications to the RA Manager.

Sponsor Training

All Sponsor guidance and instruction material is available on the NHS digital website https://digital.nhs.uk/services/registration-authorities-and-smartcards/spine-2-care-identity-service-if-not-own-section/care-identity-service-guidance-leaflets. The material covers the following:

- Understanding their responsibilities as sponsors
- Resetting of PINS
- Care of the Smartcard
- Incident reporting procedures
- Identifying security breaches

RA Agents

RA Agents are responsible to the RA Manager for ensuring that the National and local processes are followed and for the accurate input of information on RA forms onto CIS.

RA Agents will ensure that all NWL CCG policies and procedure pertaining to NHS Spine Services access are followed and adhered to. All incidents, misuses, anomalies and problems will be reported to the RA Manager.

RA Agents activities will be audited by the RA manager and IT security on a quarterly basis using CIS.

RA Agents responsibilities include:

Being familiar with this document and the Registration Policy and Practices for Level 3 Authentications or latest version, Registration Authorities: Governance Arrangements for NHS Organisations and the NHS Care Records Service Operational Procedure Manual on https://digital.nhs.uk/services/registration-authorities-and-smartcards ensuring that they are adhered to in full;

Ensure that all users are registered and issued with a Smartcard containing a UUID and their photograph and are aware of their responsibilities relating to information governance and Smartcard use;

Adhere to the Audit policy and ensure that all RA forms and associated information are maintained and securely stored according to National and Local Policy;

Promptly report all incidents of misuse, anomalies or problems to the RA Manager and initiate local Risk Management procedures;

Apply common sense checks and challenge the content of the RA forms they action, e.g checking that:

The registration request is from a recognised Sponsor or the Executive Management Team from their own organisation;

Appropriate sponsorship has been applied e.g. a Practice Manager has not sponsored the registration of a GP (unless they have been requested to do so) or that clinical activities have not been requested for Administration and Clerical staff.

RA Agent Training

All agents must have undertaken the NHS Digital online training on https://digital.nhs.uk/services/registration-authorities-and-smartcards/spine-2-care-identity-service-if-not-own-section/registration-authority-training which covers the following:

- Understanding all support procedures as documented in the operational manual
- Management of user profiles using the Spine User Directory
- Management of smartcards using the CIS System
- Using and troubleshooting RA hardware
- Identifying breaches in security
- Incident reporting procedure

Processes

We will ensure that processes supporting the identification, registration and management of staff will be integrated with other NWL CCG processes as appropriate.
All of our RA policies and procedures will be auditable by internal auditors as well as external auditors. Audits will also be conducted by the RA on a quarterly basis. Audits would typically cover:

- the issuing of Smartcards
- the management of Smartcards
- the profiles associated with users in relation to what they do
- activities of Sponsors and RA staff
- the use of Smartcards
- the use of NHS Spine applications
- identity management
- security of supplies and equipment

Incident Reporting

Incidents may be reported by any member of staff where they feel that there is a risk to patient health, confidentiality or NWL CCG reputation. Incidents should be reported, using the NWL CCG Incident procedure to the RA Manager.

Examples of incidents are:

- Smartcard or application misuse.
- Smartcard theft.
- Non-compliance of local or national RA policy.
- Any unauthorised access of NHS Spine applications.
- Any unauthorised alteration of patient data.

The RA manager will consider all incidents reported to RA. Any incidents considered significant will be escalated to the IG Manager and Caldicott Guardian depending on the nature of the incident. A major breach of security will also be reported by the RA manager to the NWL CCGs IT Shared Services SMT LSP (Local Service Provider) and NHS Digital to ensure any risks resulting from the event can be taken into account and mitigated against.

A significant incident is an isolated incident or a series of less significant incidents that could lead to a serious degradation of healthcare or information security. The NWL CCG IT Shared Services SMT and Caldicott Guardian will consider incidents reported to them and decide whether NWL CCG systems or working practices should be reviewed as a result.

Incidents involving breaches of security or demonstrate that a user may not be considered trustworthy should also be reported to RA Manager and Caldicott Guardian by the so that any disciplinary measures required may be taken.

Registration of Users

CARE IDENTITY SERVICE (CIS)

The CIS is the current Smartcard application already in use in North West London for issuing Smartcards and this can now be done without the submission of an RA form. Increasingly the CIS is being used for granting access levels to users on request of the practice/pharmacy Sponsor.

The CIS uses Position Based Access Control (PBAC) as opposed to Role Based Access Control (RBAC) to ensure that users have the right access to systems at a more granular level than RBAC allows. PBACs also help to ensure that each role in the organisation can be issued to a group of users to ensure uniformity.

Using the CIS, Smartcard Sponsors are able to request access to applications for new staff member who has a Smartcard without the use of RA02 forms. In North West London all PBAC positions have been created by the RA teams and were approved by the Information Governance team and Sponsors and are available for Smartcard Sponsors to request via the CIS for their staff members.

PLEASE NOTE FOR REGISTRATIONS USERS

The following flowchart shows users who have no acceptable photographic documentation and whose identity is confirmed by a sponsor.

Registration Flowchart

Notes	Description
A	The sponsor must complete the appropriate parts of the Registration RA01 form and sign to confirm the applicants' identity. Sponsors are personnel that have been assigned this responsibility by the by the Local Management of the Department or RA Manager and registered by the RA with the sponsor activity.
B	The sponsor is required to fill in the correct paperwork for the applicant to give to the RA Team . **Note**: All applicants who are applying for RA roles, that is RA managers, RA agents, and sponsors are required to provide photographic documentary evidence of their identity.
C	The RA agent should confirm that the acceptable non-photographic documents have been seen and checked two forms of non-photographic personal identification, and two documents confirming their address. All active in the community documents must be originals, and less than six months old (and must prove the applicant's address). The RA must be confident that all documents are bona fide. **Note***:* If an applicant is in the process of moving, their old address details can be offered as proof if the documents are not more than three months old. In the case of overseas applicants their home address does not have to be in the UK.
D	The RA agent or RA manager must be entirely satisfied that an applicant has been known to the sponsor and the applicant isin employment with the organisation. If in doubt they should refer this to the RA manager.

E	When the RA agent or RA manager is satisfied with the following, an applicant can be registered and issued with a Smartcard: • an applicant's identity has been established • an applicant has been sponsored for registration within the sponsor's area of responsibility • an applicant has signed the RA01 and understands their responsibilities regarding the RA01 Short Form Conditions

Identity Documents

The NWL CCG RA Service will accept the following identity documents for the completion of a user's application for a smartcard:

All staff will need to produce **ONE** of the following **COMBINATIONS** of identity documents in order to complete registration and receive a Smartcard:

- 2 photo ids + 1 active in community document
- 1 photo id + 2 active in community documents
- 2 non photo ids + 2 active in community documents

The Department of Health has noted that the following identity documents will be accepted for registration:

Photo ids:

- Passport - Passports of non-EU nationals should contain UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK
- EU or non-EU drivers' license
- National identity documents issued to citizen of an EU country

Non-photo ids:

- UK Birth Certificate;
- Current Full Driving Licence (old version); (Provisional Driving Licences are not acceptable);
- Residence permit issued by Home Office to EU Nationals on inspection of own-country passport;
- Adoption certificate;
- Marriage/Civil Partnership certificate;
- Divorce or annulment papers;

- Police registration document;
- Certificate of employment in HM Forces;
- Current benefit book or card or original notification letter from the Department of Work and Pensions (DWP) confirming legal right to benefit;
- Recent Inland Revenue tax notification;
- Firearms certificate;
- Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms);
- GV3 form issued to people who want to travel in the UK without valid travel documents;

Active in community documents:

Recent (i.e. not more than three months old) utility bill or a certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms

NOTE: Mobile telephone bills are not accepted as they can be sent to different addresses.

- Utility bills in joint names are permissible;
- Local authority tax bill (valid for current year);
- Current UK photocard driving licence (if not already presented as a personal ID document);
- Current Full UK driving licence (old version) (if not already presented as a personal ID document);
- Bank, building society or credit union statement or passbook containing current address;
- Most recent mortgage statement from a recognised lender;

- Current local council rent card or tenancy agreement;
- Confirmation from an electoral register search that a person of that name lives at the claimed address;
- Court Order.

Starters

As part of normal induction processes new staff required to use NHS Spine Applications will be:

- Introduced to the relevant Sponsor who will identify the appropriate role profile for the user and take them through the NWLCCG RA processes required. This is how a new user will be registered or, if the user already holds a Smartcard issued by another organisation, adding the necessary role profile/s to associate them with the NWLCCG.
- Trained on the aspects of NHS Spine applications use relevant to their role/s. (This guidance must be written as well as verbal)
- Trained on the National and NWLCCG RA processes.

Where full registration is required; the Applicant must bring suitable forms of identification with them as noted in the Identity documents section.

Where staff are recruited to a role which requires access to National NHS Spine Applications it is important that the following points are considered:

- checks on an applicant's ID are made during CRB check to ensure that RA Level 3 identification requirements can be met

- staff must sign to acknowledge that they have read and understood the policies and procedures governing the use of Smartcards and NHS Spine Applications (RA01 form)

GP Practice Staff Starters

Practice managers will notify the RA of any new starters. They will check with the user if they have ever applied for a smart card. The RA will also conduct its own check to verify the accuracy of this response. The present process is that new starters will present to the RA after having their RA01 and RA02 signed off by their practice manager or senior partner. They will be required to present with photographic ID and activity in the community documents.

All the above processes will be integrated into the standard employment processes of the Trust, as much as possible to prevent duplication.

Leavers

It is recommended that there are strong links between the HR function and the Registration Authority so that the HR function advises the RA where practicable, prior to a user leaving.

The Human Resources department is responsible for the following in regards to CCG employed staff:

- The production of the leavers list on a regular basis to an agreed format and frequency.
- The leavers list is the primary trigger for the RA team to initiate the process of account deletion for a user. It is essential, therefore, that the list must be timely and above all accurate. Incorrect inclusion of a current staff member in the leavers list could result in significant loss of data

The User must:

- Return their smartcard if they intend to leave the NHS or no longer require a smartcard in their next role.

The RA Team:

- Must, on receipt of the leavers list and/or leavers form and any notification from the Sponsor, initiate access revocation from the smartcard(s).

Leavers – with no intention to return to a health organisation. They are defined as; users who are leaving the organisation and who are not known to be commencing work within another health organisation in the near future where they would require a Smartcard to access NHS Spine Services Service compliant applications e.g. users having a change of career or those retiring. These leavers should have their Smartcard and its certificates revoked using an RA03 form.

Leavers – transferring to another health organisation e.g. GP practice, Acute Trust etc., (and the user can give details/proof e.g. letter of appointment) then they will be allowed to retain their Smartcard but their current organisational profile(s) must be removed via a RA02 form at a time close to their departure. The new organisation may request copies of the user's RA01 and any RA05 forms (if

applicable) to complete the records of their 'new employee'. It is the responsibility of the RA Manager to ensure that any requested RA forms are sent securely and in a timely manner. The NHS Smartcard will be retained by the RA in a secure safe, should the employee decide to later return to the NHS and request their NHS Smartcard for use in the new organisation.

Short term leave - up to 6 months with an intention to return. In cases where leave is expected to be up to 6 months and the user intends to return after this period, it is recommended that user's organisational profile(s) are removed the day after they leave. An RA02 form should be used to identify the profile(s) to be removed and to reinstate their profile when they return. If prior to the leave period expiring the RA have been advised by HR that the user has ceased to provide healthcare related services then the user Smartcard should be revoked using the RA03 form. If, after the leave period, the user has not returned to the organisation then the RA will check to see if another organisational profile, since the leave period commenced, has been created, if this isn't the case then their Smartcard should be revoked using a RA03 form. It is the responsibility of the RA Manager to request that all such Smartcards are returned and appropriately destroyed within a reasonable timescale.

Contractors

The Trust will ensure all contractors who need to use the NHS Spine applications are bound to the Data Protection Act and The NHS Confidentiality Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice). This will include the process to be taken in cases of a breach and liability issues.

Locum and Agency Personnel

Temporary staff filling roles may need access to NHS Spine records as part of their role. The following points should be considered:

- staff working as part of a team may not need a Smartcard to fill the role
- some temporary staff could already be registered and will only require a role profile added
- Temporary staffs who are Smartcard holders may not have sufficient training in the use of the particular NHS Spine Application needed to be accessed.

All locum and agency staff must follow the registration process as detailed in section 4.2. If they do already have a smartcard, however, an RA02 form must be completed by the relevant sponsor to add their appropriate role for the organisation to their profile.

Management and use of RA Equipment

The RA Manager, on behalf of NWL CCGs will be responsible for ensuring that adequate numbers of Smartcards are available and maintaining the Smartcards throughout their useful life. The Head of IT Operations will ensure that there is sufficient computer equipment to support all users of NHS Spine applications (including those for registration). All RA equipment will be subject to policies and procedures governing the management and control of NWL CCG Assets.

Note the following:

- All RA Equipment (e.g. cameras, laptops, card printers) will be recorded on an Assets register spreadsheet

RA Forms

The forms are:

- **RA01** to register a user
- **RA02** to change a user role profile
- **RA03** to revoke a user's Smartcard or their certificates and issue, where necessary, a replacement Smartcard
- **RA05** for when a user changes their name

In all the cases only printed forms are acceptable, not photocopied or faxed.

Transportation of RA forms

As the NWL CCG, General Practice and Pharmacy employees are located on multiple locations across the borough, it will be necessary for them to attend face to face meetings or email forms securely to the RA.

The RA will ensure the latest version of the RA forms is used as published on the NHS Digital website.

Training

All RA Team members will receive training on the RA forms and their use. Special training will be arranged whenever RA forms are changed significantly.

Contingencies

It is expected that many users may turn up with either incomplete forms, or may not be able to meet the requirements for proving their identity. In this scenario several work-around are suggested.

Incomplete forms

If staff present to the RA Agent with incomplete, or incorrect forms on registration day their smart card will not be able to be issued. In this scenario it is hoped that their sponsor will be present to assist with completing a new form. If not, the user will need to return to the RA Agent with the completed form at a later date.

Unable to Prove Identity

If staff present with the RA Agent with a completed form but their identity cannot be verified by a sponsor, or supporting documentation then the RA Agent will not complete the registration process with the user. This will prevent the user from accessing the system until they have proved their identity A list

of users needing to return to prove their identity will be forwarded to the RA Manager and users not returning will be followed up accordingly.

RA01

The RA01 form is used to record the registration of new NHS Spine Application Users

The RA01 is divided into 2 parts:

Part 1 – to be completed by applicant who requires access to NHS Spine Services applications

Part 2 – to be completed by RA sponsor and RA Agent who registers applicant.

NI number is mandatory and without it registration cannot be complete

The RA01 form is held by the RA Team once the user completes Section 1. Once registration is completed the user is registered on the Care Identity Service and the RA01 form is filed away securely, to be available for RA Manager, Agents, Sponsors, or auditors as necessary.

RA02

The RA02 form is used to record changes made to an existing NHS Spine Applicants User Role Profile(s). If any change is made to a user's profile a RA02 form must be filled out to reflect those changes. This will be necessary whenever employee NHS Spine Application related roles start or end in the NWL CCG or any of the constituent General Practices or Pharmacies.

Whenever a change to a User's Role Profile is identified the relevant Sponsor must be requested to authorise the changes required. The following are examples of when Role Profile changes would be needed:

- A Medical Admissions Secretary changes departments
- A Senior Nurse covers a colleague's role as a Nursing Manager during a period of sick leave.
- An Administrator takes on an extra job in a different department.
- A therapist's assignment in a department comes to end.

As the assignment of a user's role profile is quite complex, the local RA will make use of Role Based Access Control (RBAC) templates. The amount of RBAC templates will be kept to a minimum.

Once the relevant Sponsor has authorised the change(s) by signing, the RA02 form shall be processed by the RA. Should there be any problems with the form these will be referred to the signing Sponsor.

RA03

The RA03 is used to record revocations. Whenever it is necessary to revoke a certificate associated with a Smartcard a RA03 form must be completed and signed by the Sponsor. Sponsors should only do this when it has been confirmed the user has left the organisation or in the case of disciplinary action, on the express request by HR. Once complete the RA03 should be sent to the RA team for action.

Once RA has completed the changes on the RA03 form it will be delivered securely to the organisations RA where the RA forms are logged and filed, to be available for RA Managers/Agents/Sponsors/auditors as necessary.

RA05

The RA05 form is filled out when a user's personal details change. This form must be forwarded to the RA as soon as it is practical by the Sponsor.

Once RA has completed the changes on the RA05 form it will be filed securely at the organisations RA offices where the RA forms are stored, to be available for RA Managers/Agents/Sponsors/auditors as necessary.

Smartcards

Smartcards should be treated with care and protected to prevent loss, damage or theft.

Smartcard **do's and don'ts.**

Do's

- Ensure you keep your smartcard with you at all times
- Ensure your password is amended if you feel someone might know it
- Access only the information that you are authorised to see
- Ensure that any identified security weakness, suspected or actual breach of security is reported to the RA via the Service Desk in a timely manner
- Ensure that printouts or other outputs from the NHS Spine Services are appropriately protected and disposed of when no longer needed

Don'ts

- Leave NHS Spine Services logged-in workstations unattended
- Leave smartcards unattended
- Share smartcards, passcodes or shared secrets with other users
- Write down passwords in places where they may be misused or programming passwords into 'function-keys'
- Hold local copies of important data that is not backed-up for contingency
- Not locating NCRS workstations in places where they may be easily damaged or where the content of their screens is easily read by non-authorised people
- Copy or remove printouts from the workplace or share with others without the proper authorisation

Generic/ Locum Smartcards

NWLCCG will issue GP Practices with a short term access (SAS) cards for use with the SystmOne Clinical System in an emergency. It is considered an **emergency** when the RA team cannot be contacted to update individual smartcards.

The short term access card is only valid for a period of 12 hours and **MUST** only be used by individuals who have been registered with their own smartcard.

If a locum is going to continue with further sessions at the GP practice then a sponsor will need to email/send a signed RA02 to the RA agent to add them to your practice.

Sponsors will ensure:

- When the smartcard is not in use it is kept in a secure location
- The smart card is locked when not in use. (by entering the wrong password 3 times)
- An RA04 form is completed for each usage of the SAS smartcard and a simple log is kept of all users of the card
- If a card is not returned to the sponsor immediately after use*, then the sponsor needs to contact the RA agent immediately for them to cancel the card to log as an incident. An RA03 will need to be sent to the RA agent for the card to be replaced)

*A suggestion is to ask the locum using the card that day to part with their car/house keys until the card is returned to the sponsor. This ensures the return of the card.

Pharmacy smartcards and 5 “F” code

The NWLCCG RA team will issue smartcards to pharmacy staff working at sites within the North West geographical area which currently covers Brent, Central London, Ealing, Hammersmith & Fulham, Harrow, Hillingdon, Hounslow and West London CCGs. Locum Pharmacists\Dispensers may be issued with the locum five “F”s code only if their locum status can be verified by a Pharmacy Sponsor via CIS or CIS user modification form or Locum agency using an official email address. Please note if a pharmacist works as a regular locum at up to 10 sites, then they will have all sites added to their smartcard rather than be given the locum code. The five “F”s code will only be issued in exceptional circumstances and at the discretion of the NWLCCG RA Managers. As stated in the National RA Policy, locum access will only be granted for a 2 year period after which access will need to be reviewed if it is still required. Locums are encouraged to save the date when the 5 F access terminates so they can contact the RA team and have their access extended to avoid clinical risk.

Organisation name on Smartcards

As the smartcards will be used throughout an employee’s career with the NHS, cards will not be printed with the organisations name, only the UUID, preferred full name of the user and the user’s picture.

Lost, Stolen and Broken Smartcards

Lost and damaged Smartcards should be reported to the RA Team as soon as is practicable by email on NWLCCGs.Registration.Authority@nhs.net. The sponsor of the user must send a RA03 or CIS cancel smartcard form to the Local RA via email and arrange a suitable face-to-face meeting where the RA can verify their identity and issue a replacement card. If the identity cannot be verified then the applicant’s Sponsor will need to be contacted (and their identity established) to vouch for the user. This will be recorded as a near miss incident.

Once notified that a Smartcard has been lost or damaged. RA Agents will arrange to have the lost/damaged Smartcard revoked and replaced (see below) as soon as possible. In the case of loss or theft, the RA Lead or RA Manager must be informed so that checks may be made to ensure that the Smartcard has not been misused.

When an issued Smartcard becomes unusable or it is lost or stolen the Smartcard certificate must be revoked. Revocation renders the Smartcard useless.

As long as the Smartcard holder's identity can be verified at a face to face meeting a new Smartcard may be issued.

PIN/Pass-code Unlocking/Changing

GP Users

Practice Managers have been set up as Sponsors with additional functionality on the Care Identity Service which will enable them to unlock pass codes. A dedicated PC (usually their own) will be set up with a 2nd card reader which is necessary to enable the process.

NWL CCG Staff

Arrange a suitable face-to-face meeting where the RA can verify the identity and reset the password on the card. Users will need to contact members of the RA via the IT Service Desk.

Certificate Renewal

In release 2008A there is a new version of the Identity Agent that advises the user how to renew their certificates. Users may renew their certificates twice without an RA manager or agent. For every third renewal they must verify their identity with either an RA manager or RA agent. Users with the new Identity Agent (v11) will be advised once per day when they initially log on that their certificates are nearing their renewal date (30 days prior to their expiry). When they receive this message they are given the choice of renewing the certificates or deferring renewal until later. If certificates are within 20 days of the expiration date users are forced to renew their certificates.

To renew user certificates: The system will check that the appropriate Identity Agent components are available on the PC, if not they will be copied to the PC. Note: This does not require local admin access to the PC or any application to be installed on the PC. The user is asked to enter their Passcode again, prior to the old certificates being removed and the new certificates being copied to the Smartcard. Note: This new functionality uses the current certificate expiry to trigger this process so there should be no adverse load on the RA in six years time. After the user has self-renewed their certificates twice and when the latest certificates get closer to expiry, the user will be advised to visit their RA to get the certificates renewed. The RA at a face-to-face meeting will then re verify the users' identity by checking the user's photograph against that on the Smartcard. If the likeness is satisfactory the RA will renew the user's certificates. Whenever an RA renews certificates post 2008A, users can self-renew their certificates twice before having to visit the RA.

If users are unsuccessful in renewing their certificates, they will be asked to attend a face to face meeting at the RA office (or any other location as advised by the RA Manager).

Unacceptable use of smartcards (Misuse)

Types of Misuse can include (but are not limited to):

- Smartcard or application misuse
- Theft of a smartcard
- Non-compliance of a local or national RA policy e.g. card sharing, password sharing
- Any unauthorized access of national applications
- Any unauthorized alteration of patient data
- Smartcard left unattended in the reader. The card should be removed and handed to the person's manager
- Inappropriate issuing of cards by the RA Manager/RA Agents
- False registrations – this will be escalated to the NHS Counter Fraud Team immediately
- Excessive card losses i.e. more than 2 Smartcards reported lost within any 12 month period

Breach of Confidentiality will be reported to the NHSE for onward investigation and could result in disciplinary action being taken against the user.

Monitoring of smartcard use

Spot checks may be undertaken by any organisational sponsor or user to ensure that card sharing is not occurring. NWLCCGs in agreement with supported organisations may monitor smartcard use at any time without prior notification. Such monitoring would occur for reasons including, but not limited, to the following:

- Technical maintenance or problem resolution.
- During an investigation into alleged misconduct, including unauthorised or excessive use of the smartcard applications, or in connection with the prevention or detection of criminal or illegal actions.
- During an enquiry concerning compliance with this Policy.

Major misuse will be reported to the NHSE by the RA Manager

Please note when possible that if the RA Sponsor is experiencing problems in unlocking a smartcard, the Ra/IT Team will attempt to resolve issues remotely. If the issue cannot be resolved, users will be asked to attend a face-to-face meeting at the RA Office or arrange for the smartcard to be delivered securely to the RA Team where applicable any other location as advised by the RA Manager.

Smartcard Misuse

A staff member must report suspected Smartcard misuse in line with NWL CCGs incident reporting policy and procedure. Depending on the severity of the allegation an investigation may be required. If it suspected that a Smartcard is being misused then it should be reported to RA Manager who may request that the certificate associated with the Smartcard should be suspended or revoked as appropriate.

If Smartcard misuse by a NWL CCG staff member is discovered the appropriate disciplinary measures must be taken.

User Profiles

What a user is able to access is based on the information in their profile. Whenever there is a temporary and permanent change in the way a person works, a review of the person's NHS SpineApplication access must be carried out. If there are significant changes to the staff member's role the relevant Role Profile on the NHS Spine User Database must be requested via a suitable Sponsor. Examples of changes that would necessitate such changes are changes to a person's:

- Job Title
- Access requirements
- Department
- Site(s)
- Work Group

Where new roles are being added or roles are being changed the Registration sponsor of the relevant department or service will complete an RA02 form which is used to update the user's profile. If the user's personal details change, the sponsor must fill out an RA05 form.

When a particular role comes to an end the profile must be updated by deactivating the role as soon as is practical after the role has ceased.

Revocation

There are occasions when it is necessary to deactivate a Smartcard by revoking the Smartcard certificate. Reasons for this include:

- The Smartcard is lost or stolen
- There has been some other security breach associated with the Smartcard or Smartcard certificate.
- The user is no longer employed by an NHS organisation

Revocation tasks on the Care Identity Service can only be carried out by the RA agent or manager.

Where the revocation is needed due to a staff member leaving the NHS, the Sponsor will inform the RA Manager accordingly so that the correct actions can be taken.

Where the revocation has been requested by the Sponsor because of security related events, the RA Manager will authorise the appropriate action and inform the following staff as appropriate:

- The HR Manager
- The relevant Sponsor(s)
- The Information Governance Manager
- The IT Security and Cyber Security Lead

Revocation renders the Smartcard useless. Revocation can only be carried out by RA Managers and Agents.

Local Support Process for NHS Spine Application Users

NHS Application Users who need support should contact the NWL CCGS IT Shared Services Service Desk on 0203 350 4050.

Support provided by the Service Desk is limited to the following:

- Connectivity e.g. no connection to the Spine due to network fault
- Hardware e.g. card reader not working
- Software e.g. Gemplus does not authenticate

Local Audit

The management and use of Smartcards will be subject to internal and external audit to ensure that national and local policies are being followed.

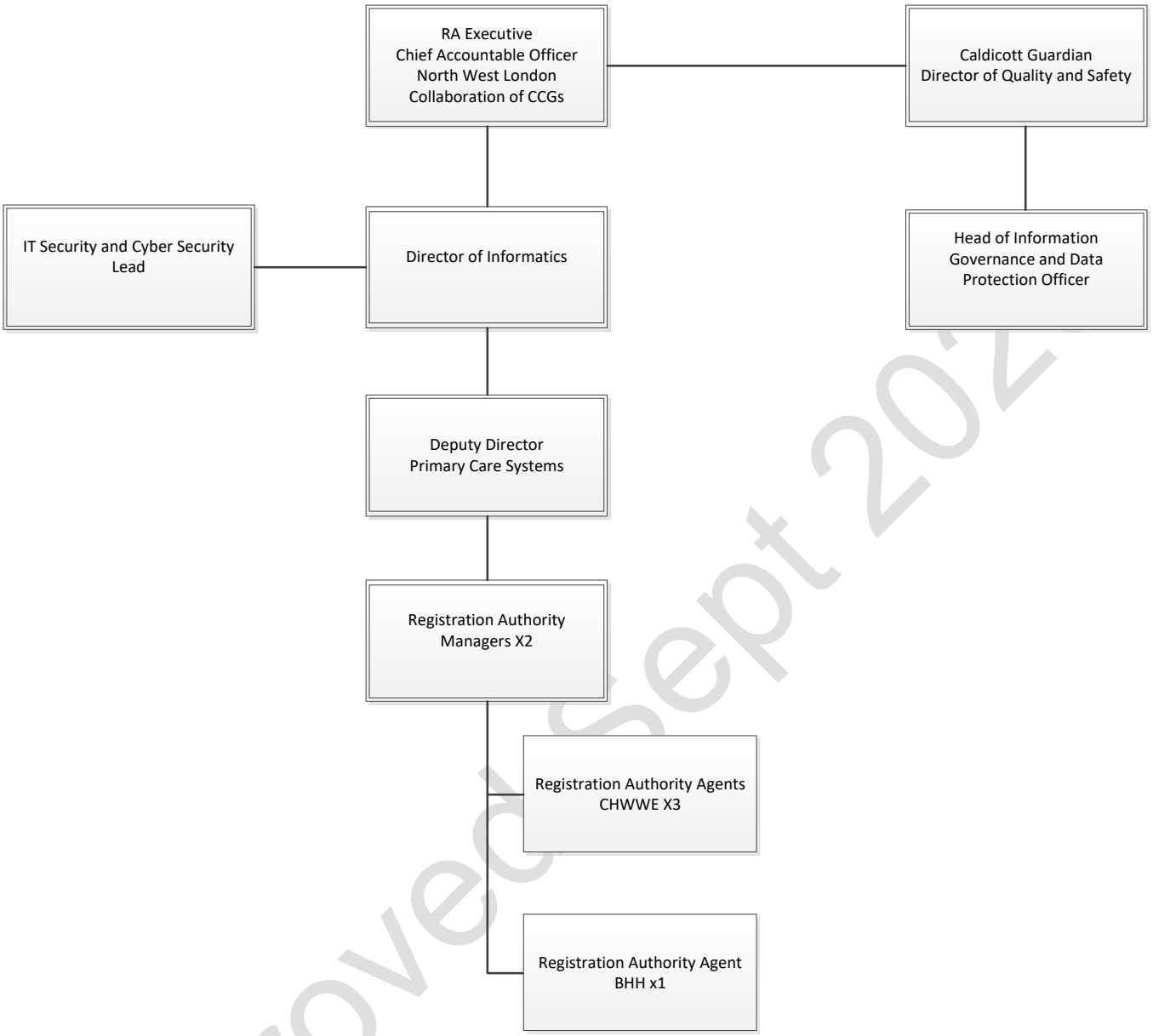
All activities performed by RA agents and sponsors will be randomly audited by the RA Manager and the Head of IT Security.

Specifically, Auditors will look to confirm that:

- Smartcards are handled securely by Users
- RA documents are used and stored appropriately
- Access to NHS Spine Applications and Records is controlled appropriately
- Unused Smartcards are stored safely and appropriate records are kept
- Revoked Smartcards are destroyed securely
- RBAC role allocation and de-allocation is performed appropriately
- Random checking of RBAC roles with those requested by the sponsor

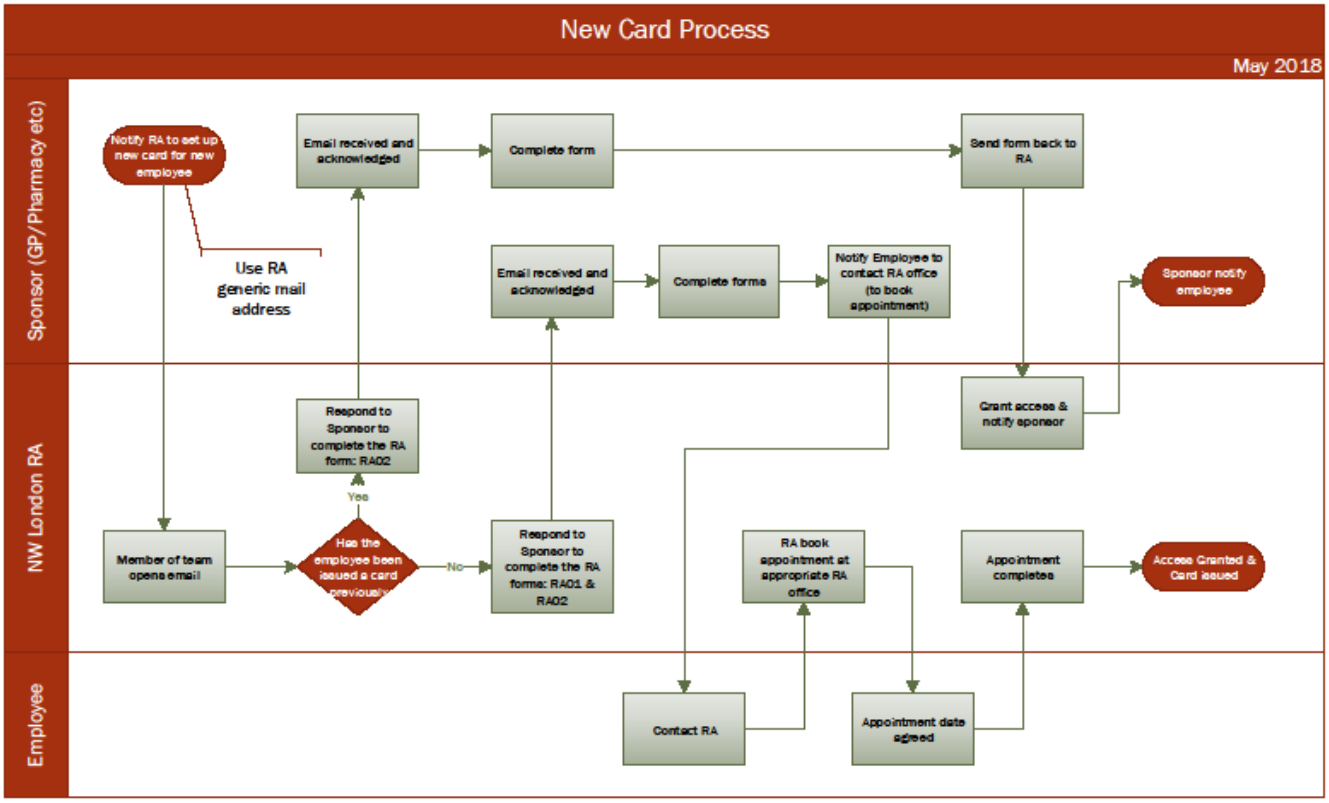
Appendices

Appendix 1: CCG RA Organisational Structure

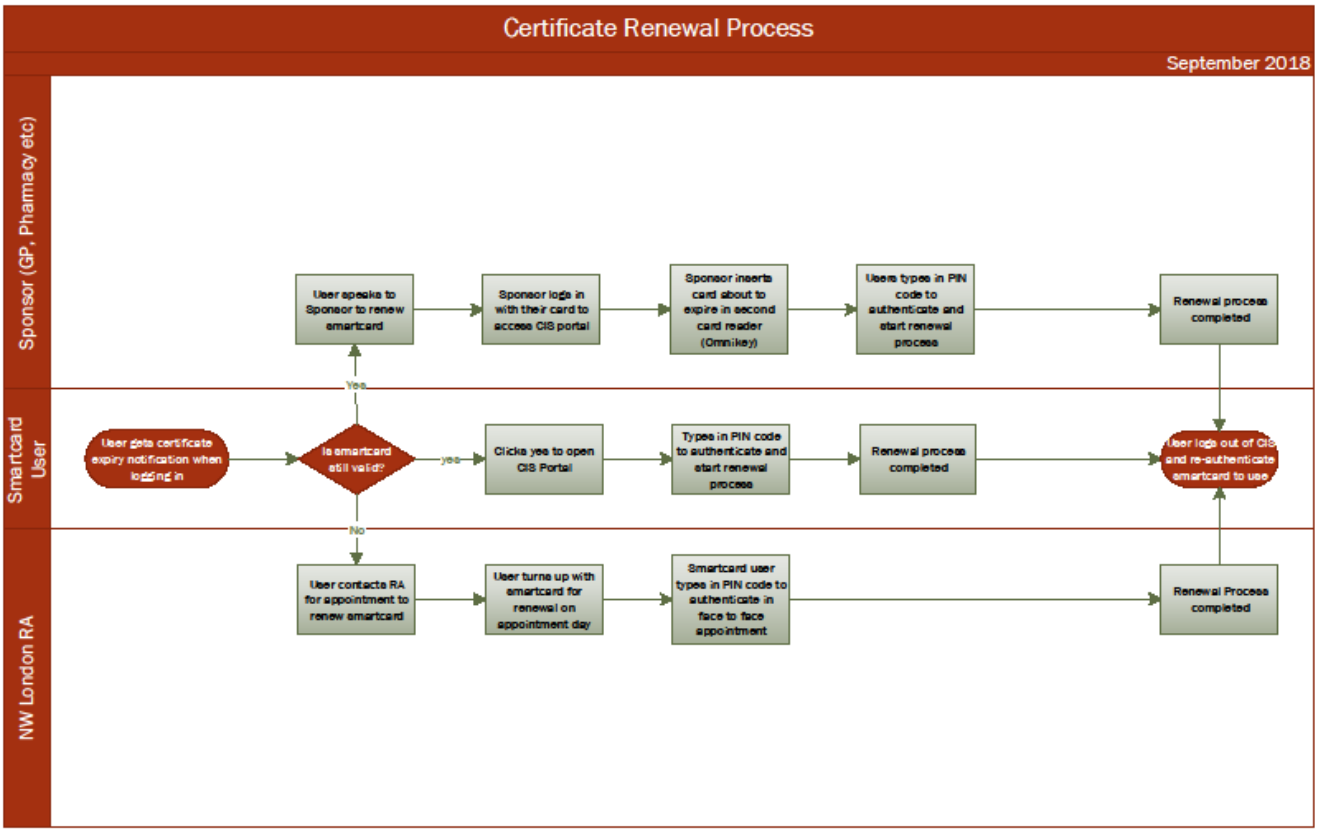


Appendix 2: Processes

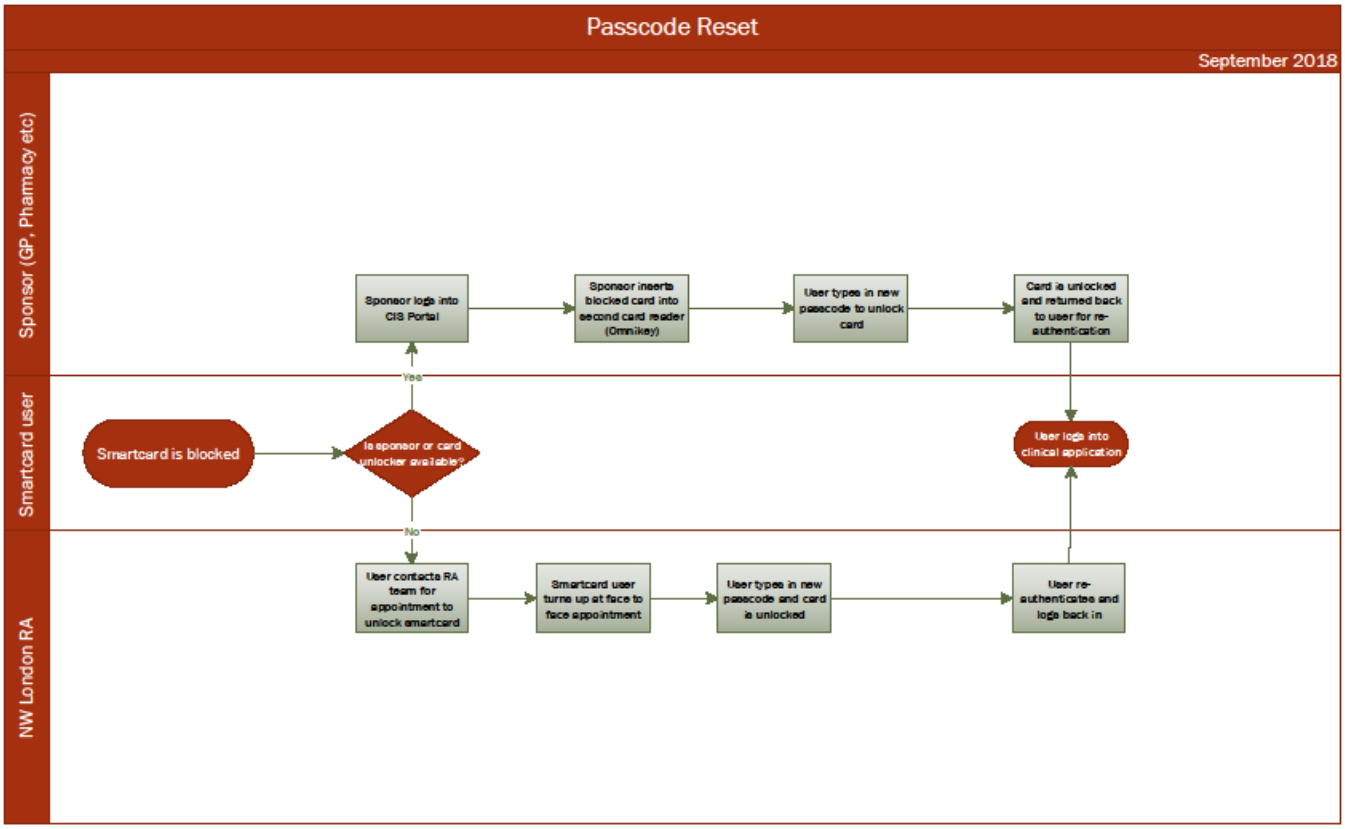
Get a smartcard process



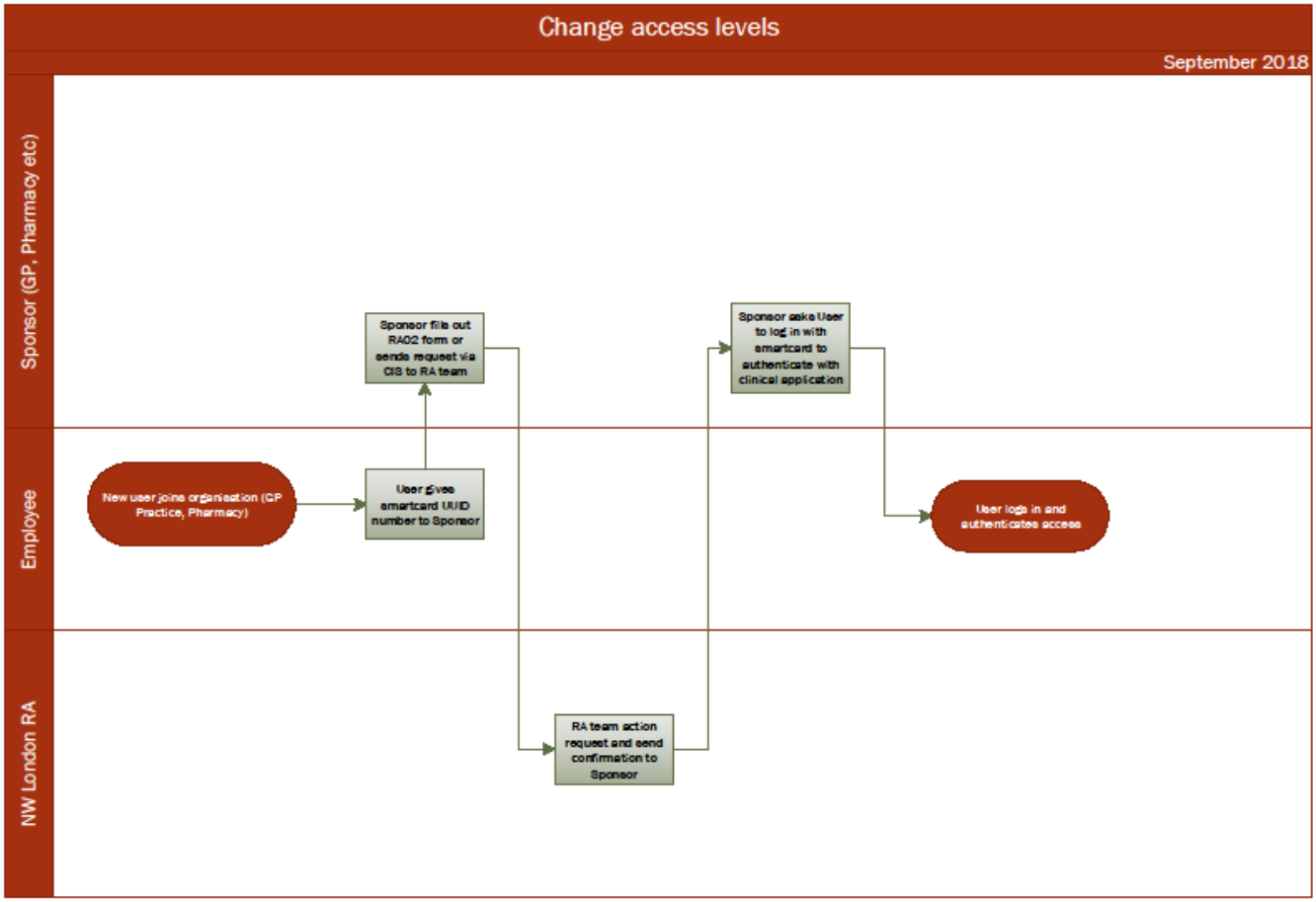
Certificate Renewal Process



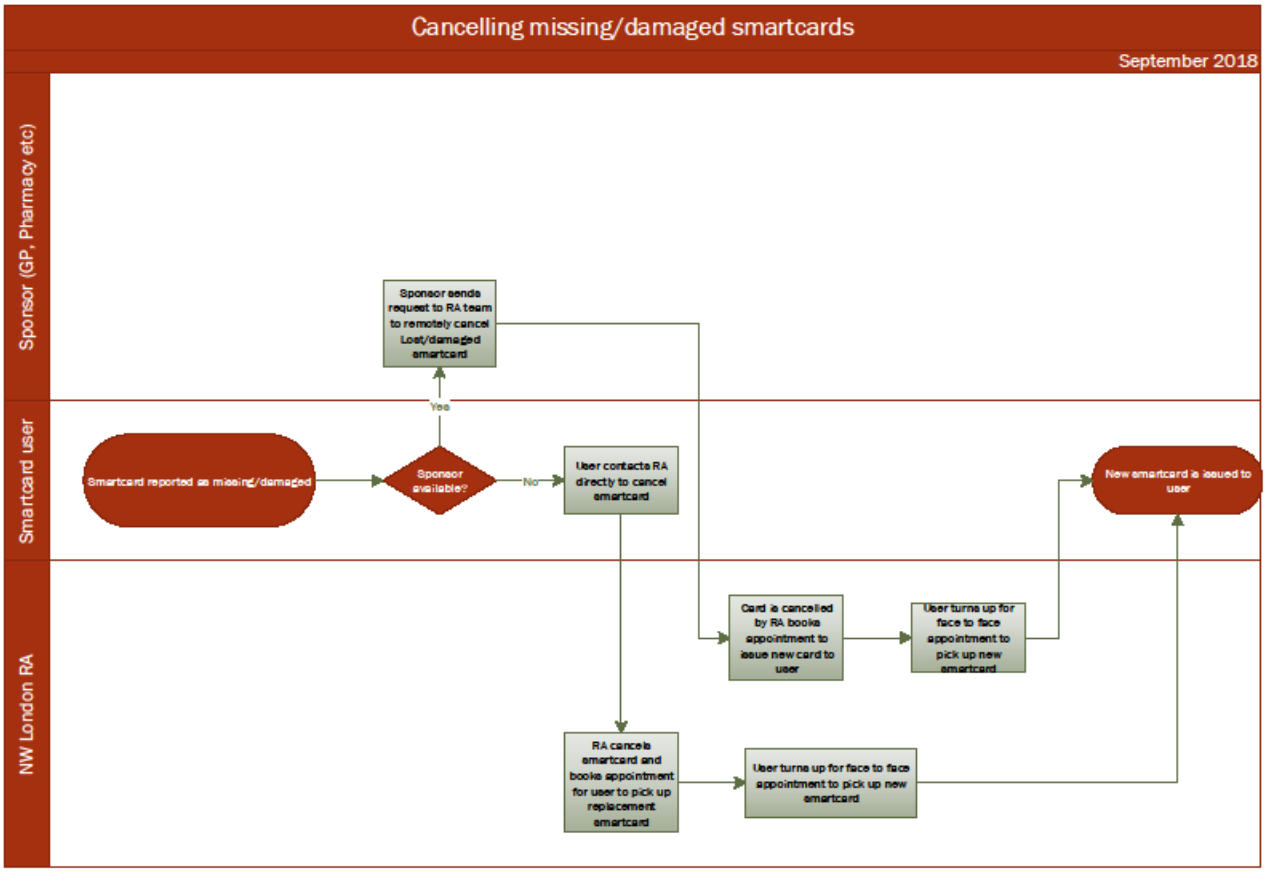
Passcode Reset Process



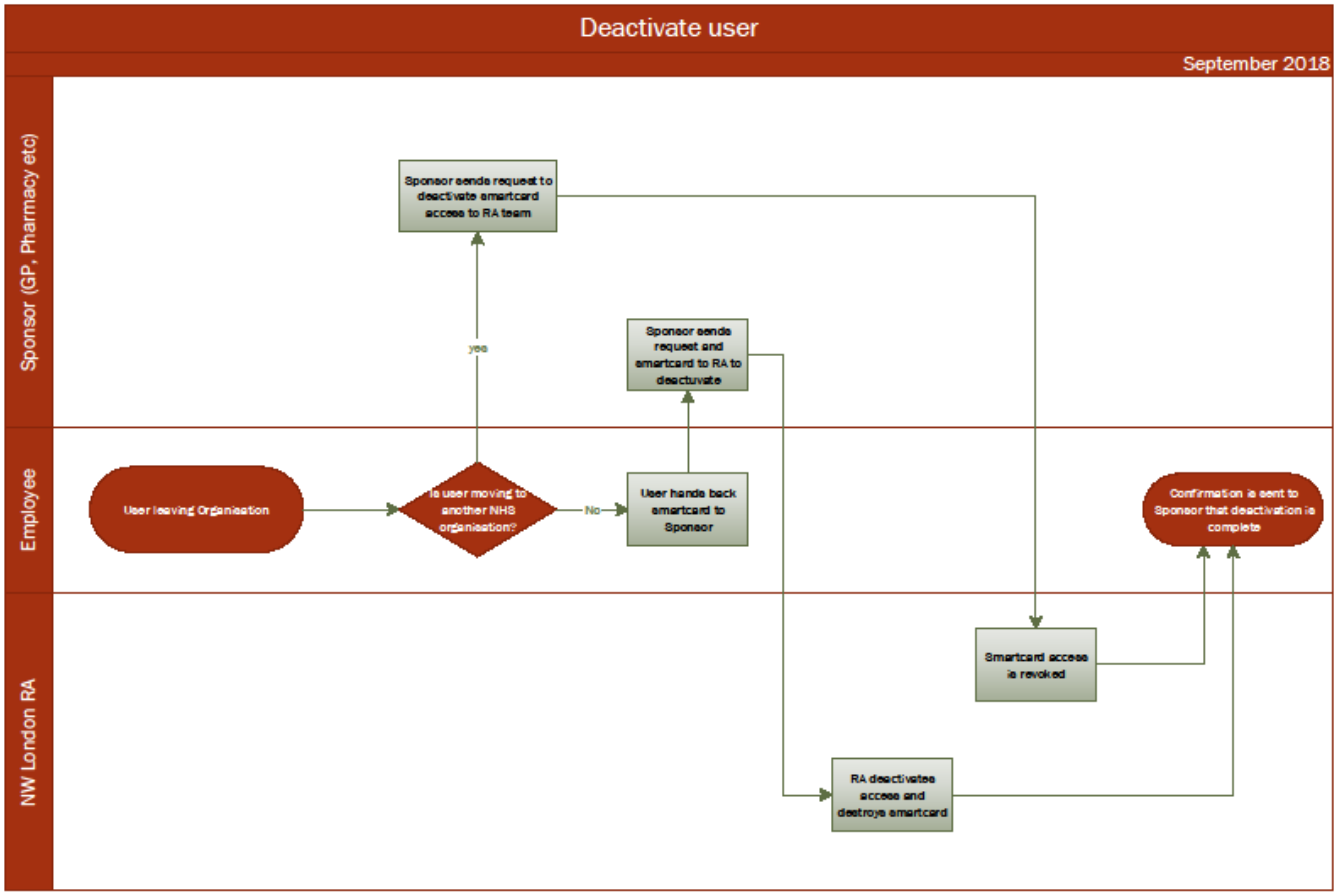
Updating or Changing Access Levels Process



Cancel Missing or Damaged Smartcard Process



Deactivate User Process


Deactivate user
September 2018
Sponsor (GP, Pharmacy etc)
Employee
NW London RA
Sponsor sends request to deactivate smartcard access to RA team
yes
Sponsor sends request and smartcard to RA to deactuvate
User leaving Organisation
Is user moving to another NHS organisation?
No
User hands back smartcard to Sponsor
Confirmation is sent to Sponsor that deactivation is complete
Smartcard access is revoked
RA deactivates access and destroys smartcard

Appendix 3: Policy Audit Tool

The following are four questions to assess your understanding and implementation of this policy.

Score yourself – Yes / No

Do you understand who this RA policy applies to?	Yes / No
Do you understand your responsibilities as members of staff?	Yes / No
Do you understand your responsibilities as a sponsor?	Yes / No
Do you know where to find more information?	Yes / No

If you score yourself No for any of the questions, please re-read the relevant section of the policy. If you are still unclear, please contact the RA Agent for clarification.

A copy of this should be kept in your personal file and may be used as part of a continuous professional development folder.

Signed …… Role ……

Date ……

Appendix 4: Equality Impact Assessment Tool

Document Authors: Craig Thomas, Raphael Danladi	Directorate: Informatics
Name of Policy: Registration Authority Policy	New: Existing: X
Date:	

Aim/Status

a) What is the aim/purpose of the policy/strategy/procedure? To ensure all users know how to obtain and use RA applications and smartcards
b) Who is intended to benefit from this policy/strategy/procedure and in what way? All users
c) How have they been involved in the development of this policy/strategy/procedure?
d) How does it fit into the broader corporate aims? Ensuring the CCGs sensitive information is managed, accessed and process safely and appropriately
e) What outcomes are intended from this policy/strategy/procedure? Reduce breaches of information security
f) What resource implications are linked to this policy/strategy/procedure? RA team and hardware

Impacts

(a) what is the likely impact [whether intended or unintended, positive or negative] of the initiative on individual users or on the public at large? None
(b) Is there likely to be differential impact on any group? If yes, please state if this impact may be adverse and give further details [e.g. which specific groups are affected, in what way, and why you believe this to be the case] No
If the policy is unlawfully discriminatory it must go to a full impact assessment (please Contact the Equality, Diversity & Human Rights Advisor – Human Resources Directorate) N/A

Persons conducting EqIA	

Signed	