Avon and Wiltshire
Mental Health Partnership
NHS Trust

Registration Authority Policy

Board library reference	Document author	Assured by	Review cycle
P111	RA Manager	Director of HR	3 years

This document is version controlled. The master copy is on Ourspace.

Once printed, this document could become out of date.

Check Ourspace for the latest version.

Contents

1. Introduction

The National Registration Authority run by NHS Digital (formerly the Health & Social Care Information Centre (HSCIC)) is the overall controlling body for the issue and management of Smartcards enabling staff to access the National Health Service (NHS) Care Records System and other associated Information Technology (IT) Systems such as RiO, Choose and Book, Electronic Prescriptions Service, Secondary Users Service, Electronic Staff Record and Summary Care Record.

All organisations that run a local Registration Authority do so on a delegated authority basis from NHS Digital. Avon & Wiltshire Mental Health Partnership NHS Trust (AWP) has a legal obligation to comply with the National Policy as well as the Data Protection Act 2018.

It is the responsibility of each local Registration Authority to clearly define how they will set up and manage their Smartcard operations ensuring that the National Policy is followed and no deviations occur. This document details how such a Registration Authority is operated within AWP.

1.1 Why do we use Smartcards?

Smartcards are currently considered the most secure and cost-effective solution to provide the necessary identity requirements and authentication for access, when issued in accordance to a recognised and accredited PKI model using digital certificates, which meets the relevant legislation* for legal admissibility for medical records."

- Electronic Communication Act 2000
- Electronic Signatures Regulations 2002

The Smartcard also ensures that 2 factor authentication (i.e. something you have and something you know) is used which meets the requirements of the NHS Care Record Guarantee and ensures compliance with the IG Toolkit.

2. Purpose or aim

The Registration process is required to allow authorised and 'adequately identified' users, access to the services of the NHS Care Record Service (NHS CRS) and other national applications.

'Adequately identified' is determined by the United Kingdom (UK) Government E-GIF level 3 requirement that the person is identified 'beyond reasonable doubt'. The 'Verification of Identity' standard has been developed as part of the NHS Employment Check Standards. This requires the production (in a face to face meeting) of proof of identity documents such as a current passport or photo card driving licence together with 2 proofs of address documents such as a utility bill, bank statement or council tax document dated within the last 3 months in order to meet RA requirements. The ID check requirements are set at National level and as such there can be no local deviation.

A Smartcard (Personal or Temporary Access Card) cannot be issued to anyone who has not met the ID requirements to e-Gif level 3.

The NHS Employment Check Standards includes all pre-appointment checks that are required by law, those that are mandated by Department of Health (DH) policy, and those that are required for access to the NHS Care Record Service. These standards apply to permanent staff, staff on fixed-term contracts, temporary staff, students, trainees, and contractors employed through an agency. Trusts appointing locums and agency staff or providing authorisation for external researchers will need to ensure that their providers comply with these standards.

Failure to comply with these standards could potentially put the safety, and even the lives, of patients, staff and public at risk. It would also put AWP in breach of various Policies, legislation etc.

The Registration Authority (RA) role is a hierarchical structure cascaded to a network of Agents who have access to specific equipment for the production of the photographed Smartcards.

Once registered, the signing on process can only take place when the computer being accessed has the appropriate hardware and application running on it. The Passcode and Smartcard are authorised across the network to an Identity Service which establishes the credential of the card in the form of a digital certificate. This allows an authorised session to take place and grants access as required to appropriate medical records of a patient, associated with their particular role.

A Smartcard and its passcode can only be used by the owner of the card. Smartcard sharing is not permitted under any circumstances.

Misuse of the Smartcard can lead to disciplinary action.

3. Scope

This document applies to all those wishing to access National Programme for IT applications using Smartcards and all those involved in the process of such applications. It should be used in conjunction with the RA Procedures document.

This document covers the following areas:

- Definition of National policies which must be incorporated into local operations
- Description of key roles and responsibilities required for the Registration Authority and Smartcard operation
- Key policies and procedures for the following areas:
  - User Registration
  - Role Profile maintenance
  - Revocation and cancelling of Smartcards
  - User Suspension
  - Pass-code resetting
  - Smartcard renewal and exchange
  - Certificate renewals
  - Temporary Access Cards
  - Identification of Unlockers/Sponsors

4. Definitions

4.1 Agent (RA)

Registers and issues Smartcards to authenticated Smartcard applicants.

4.2 Applicant

A potential user that is applying for a Smartcard.

4.3 Business Function

Access to functionality within the Choose & Book application. Sponsor defines appropriate function and is assigned during the registration process. Now known as ‘Activity’.

4.4 Cardholder

A User that has been issued with a valid Smartcard.

4.5 Care Identity Service

New Smartcard System that replaces the current systems - Calendra, User Identity Management (UIM), Card Management System (CMS) and reporting tool (ERS) from 1st November 2014.

4.6 Caldicott Guardian

The person responsible for safeguarding the confidentiality of patient information.

4.7 CIS

Care Identity Service (replaced CMS, UIM, Calendra in Feb 2015).

4.8 CMS

Card Management System

4.9 Certificate Expiry

The Certificates on the Smartcard expire every 2 years and need to be renewed. It is possible for the card holder to Self-renew these certificates.

4.10 Certificate Renewals

Process for re-issuing certificates to smartcards. Certificates expire every two years.

4.11 NHS Digital

All organisations that run a local Registration Authority do so on a delegated authority basis from HSC NHS Digital

4.12 Job Role

NHS RBAC Role profile of user.

4.13 NCRS

NHS Care Record Service

4.14 Passcode

A smartcard Passcode is used to log on to NCRS applications. It is comprised of letters and numbers and is a minimum of 4 characters and maximum of 8 characters in length.

4.15 PBAC

Position Based Access Control. The ability to assign access rights with RBAC codes per post within an organisation.

PBAC Positions have been set up within AWP to control access to Systems such as RiO.

4.16 Roles Based Access Control (RBAC)

Defines a national standard set of Job Roles and related Activities. (See PBAC).

4.17 Registration Authority (RA)

An individual or team that is responsible for the identification and authentication of Smartcard applicants; which registers applicants and issues them with Smartcards; manages the validity of information embedded on Smartcards, and the Cardholder's continued entitlement to their Smartcard.

4.18 Registration Authority Manager

Person responsible for RA team and all aspects of registration services and operations performed in accordance with Policy Management Authority requirements.

4.19 Registration Authority User

Anyone that has been granted access National Programme applications as a user.

4.20 RiO

RiO is the Trust's main electronic patient record system.

The system will give clinical staff access to accurate, up to date and secure information around the clock.

4.21 Smartcards

The credit card sized, electronic card issued by an RA that, together with a personal Passcode, enables the Cardholder to access National Programme applications, according to their User Profile/PBAC Position.

4.22 Sponsor

Assists the Registration Authority by identifying and approving Smartcard applicants for which they have direct management responsibility. They can also unlock Smartcards.

4.23 TAC (Temporary Access Card)

(if in use) TAC's are pre-populated Smartcards with a particular level of access that can be issued in an emergency to someone already registered to egif level 3 in instances when they may have lost their card or it has been damaged.

4.24 Terms and Conditions

Everyone who applies for a Smartcard needs to read and accept a set of Terms and Conditions. These may be presented via a paper form or online at point of registration.

4.25 Unlocker

This role/access allows a nominated person (set up by RA) to unlock the Smartcards for staff/students.

4.26 User

(see 4.2)

5. Policy statement

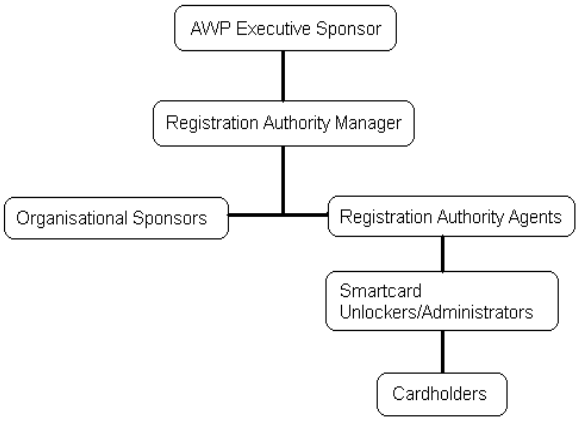
Accountability for the Registration Authority in the NHS sits with NHS England, which commissions NHS Digital to deliver the National RA service. The Registration Authority is the overall controlling body for the issue and management of the Smartcards which enable NHS employees to access the Care Records Service (CRS). The CRS is an interactive patient record service being phased in across England which will be accessible by healthcare professionals twenty-four hours a day, seven days a week. It will also provide access for patients to key information in their medical record.

All healthcare professionals will have their access profile approved by a Sponsor (usually the persons Manager/Supervisor). A robust authentication system has been developed to ensure that users gain access only to the information they are entitled to use, and that everyone having access to patient information has been through the same rigorous identity checks before access is granted.

5.1 RA Management Process Structure

The chart below shows the management process structure for the Registration Authority.

The RA Manager is responsible for the Registration Authority Agents, Sponsors and Smartcard Unlockers/Administrators within AWP.



Each organisation that runs local RA activity must name the Board/EMT accountable person for the RA function and the RA Manager.

At AWP these are:

- Dean Bridges (Registration Authority Manager)
- Trust SIRO

5.2 Related Procedural Documents

The RA manager will ensure that processes supporting the identification, registration and management of staff will be integrated with other AWP processes as and when appropriate.

6. Roles and responsibilities

6.1 Chief Executive

The Chief Executive is ultimate responsibility for ensuring that the Trust develops and implements a robust Registration Authority (RA) framework, this key function is delegated to the Trust Senior Information Risk Owner (SIRO).

- Trust Senior Information Risk Owner (SIRO)

The Trust SIRO is responsible for ensuring that a robust registration authority framework is operational within the organisation.

- Head of HR

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

- Caldicott Guardian

The Caldicott Guardian is responsible for the integrity of information.

6.2 Registration Authority (RA) Manager

The RA Manager is responsible for providing a comprehensive RA service to healthcare staff (and students) within AWP. This includes establishing and training the RA team, developing robust processes around them and producing and developing the RA policy for the Trust.

This will include the following:

- The day to day operation of the local Registration Authority function ensuring that the RA Policy and Processes achieve their overall aims and are followed by all.
- Ensuring that the RA Agents, RA Sponsors and RA Administrators/Unlockers are sufficiently responsible and trained to operate the National RA processes, equipment and applications and abide by National and Local Policy.
- Ensuring Sponsors, Smartcard Unlockers/Administrators are trained in their role and responsibilities and maintain an active list of these key staff.
- Ensuring that the National RA Policy/Processes for Smartcard issue/revocation, Profile modification, Position/Templates, Short Term Access Smartcards (if used) are adhered to within the Trust.
- Escalating any process, hardware and application problems to NHS Digital where necessary. Providing support to Trust RA Agents and Sponsors on process, hardware and application problems
- Ensuring that all forms and any other material which supports the issue/revocation of a Smartcard and the role profiles associated with the card are retained in accordance with the National RA processes.
- Ensuring that all 'Leavers' access is removed from the Smartcard system and their Smartcards are returned for destruction (if they are leaving the NHS, retiring etc).
- Responsible for maintaining and managing an audit trail of all cards and fallback cards issued and access granted and revocations.
- Ensuring that the HR starters and leavers policies accommodate the current requirements for RA and review where changes are made.
- Maintaining an inventory of all RA kits, including cards, card printer supplies etc and ensure that all is in good working order.

6.3 RA Sponsors/Managers

A Sponsor/Manager has a responsibility when appropriate to approve access issuance/modifications and may be able to reset Smartcards passcodes and renew certificates on a smartcard (if the relevant access has been assigned to them).

The Sponsor/Manager is responsible for:

- Ensuring they are aware of all RA functionality and access profiles required by the user to deliver the correct role based access to applications (via the appropriate online or paper based form).
- Ensuring that they are familiar with the users need to access to functionality and information
- Ensuring that the role profile associated with a user is appropriate
- Escalating any role profile problems to the AWP RA Manager
- Completing the appropriate parts of the RA form (be that paper based RA Forms or an Electronic form where appropriate) and Temporary Access Smartcard Usage Forms if in use and any other material which supports the issue/revocation of a Smartcard and the role profiles associated with the card
- Ensuring that the RA Manager is notified in a timely manner of all members of staff that are leaving by the completion of the relevant form (be that paper based RA Forms or an Electronic form).

As part of the leaving process, the sponsor/manager should only retrieve the leavers smartcard if the user is leaving the NHS completely with no plans to return (i.e. if they are retiring, moving abroad etc).

If the leaver is joining another NHS Organisation (or plans to in the future) then they should keep their Smartcard as it is totally transferable between NHS Organisations.

Authorisation is achieved by identification verification to e-gif level 3 and assignment of the activities and Role that the user carries out. This determines the Position Based Access Control (PBAC) that is associated with a token which is in the form of a Smartcard with the user's photograph that has been issued by the Registration Authority.

6.4 RA Agents (RAA)

The RA Agent is responsible for ensuring all applicants have read and accepted the terms and conditions and receive the completed application form (or the relevant process within the Smartcard system) approved by the Sponsor. The user will then be linked to a Position/Role that is appropriate, which has been indicated by the Sponsor on the relevant Form (be that on a paper form or electronic process).

The Trust RA Agent is responsible for:

- The day to day support of the local Registration Authority function
- Issuing Smartcards to users who have been sponsored (via a paper form or relevant electronic process) and who have proven identities to e-gif level 3.
- Updating user Smartcard profiles in accordance with the sponsor's requirements/approval (via a paper form or relevant electronic process)
- Ensuring that the National RA Policy/Processes are adhered to
- Escalating any process, hardware and application problems to the RA Manager
- Ensuring that all forms and any other material which supports the issue/revocation of a Smartcard and the role profiles associated with the card are retained in accordance with the National RA processes.

6.5 Smartcard Unlocker/Administrator

The Smartcard Unlocker/Administrator role offers a subset of RA Agent functionality. This role only allows limited Smartcard maintenance i.e. the ability to reset a user's passcode.

This role comes under the responsibility of the RA Manager and can be supported by the RA Agent.

A List of all Smartcard Unlockers will be published on the RA pages of Ourspace.

It is the responsibility of the Unlocker to tell the Registration Authority if they move locations within AWP, change Role or are leaving the Trust so that the Unlocker List can be updated and the unlocking access removed.

6.6 RA ID Checker

The RA ID Checker role offers a subset of RA Agent functionality. This role allows the checking of ID documents for the purpose of Registration or changes in details etc.

The RA ID Checker can start the process for Registration and pass details to the central RA Team so that a Smartcard can be produced.

6.7 Smartcard Applicants

Each applicant is required to provide relevant details for registration purposes (including their National Insurance Number), have their registration approved by a Sponsor/Manager and then submit their identity documents in person to the RA Agent / RA Manager. They must also read, understand and accept Terms and Conditions for the use of the Smartcard.

The RA Agent/RA Manager will arrange the registration process and issuance of the Smartcard.

All Staff/Students should attend appropriate training to ensure they know how to access and use the relevant system/s operated by the Trust. Training is provided by designated trainers within AWP from the Learning and Development Team.

Only when Staff/Students have been sufficiently trained (and this training recorded) will they be granted access to the relevant system.

Cardholders must never share their Smartcard (or passcode) or allow it to be used by anyone other than themselves. This would be an infringement of the Data Protection Act and breach the Terms and Conditions for the Smartcard. Smartcard misuse of any kind can lead to disciplinary action and in certain cases could lead to dismissal.

Any cardholder that is leaving the NHS completely must ensure that they have returned their Smartcard to their Sponsor/Manager or RA prior to leaving. As part of the leaving process, the cardholder's Sponsor/Manager will send the card back to RA and ensure that the relevant forms are completed and returned to the RA Team (or the relevant process is completed in the Smartcard System).

Any cardholder that is leaving the organisation but remaining in the NHS (or planning on re-joining the NHS in the future) should take their Smartcard with them. As part of the leaving process, the cardholders Sponsor/Manager will complete the relevant form/process and send it to RA to remove the profile for their organisation on the card. The new organisation will then arrange for the Smartcard to be set up for their system.

If in use, any Temporary Access Smartcard requests will need to be logged onto the appropriate Usage Form and approved by an appointed Custodian who will be responsible for the card and who uses it.

Temporary Access Smartcards (if in use) should only be used in an emergency.

7. Implementation

7.1 New Staff

New staff will need to be informed in advance of starting that they will be required to meet with an RA Agent/RA Manager in a face to face meeting to provide relevant ID (which satisfies e-Gif Level 3) and have their photo taken.

Staff will be assigned to an access position relevant to their role once the processes for approval (i.e. relevant system access form and Training) have been completed.

Notice will have to be given of legal responsibilities and potential disciplinary actions for inappropriate disclosure etc.

7.2 Registration and Issue

Smartcards will be issued to new staff on a 'needs must' basis, in a timely fashion and all staff (permanent, temporary, agency etc.) will go through the same ID checks in accordance to National Policy.

Existing staff will be registered under the same rules and conditions as and when access is required.

The issue of Smartcards will be controlled by the RA Manager in compliance with strict National rules and regulations which cannot be deviated from at local level.

The applicant must have completed the relevant Registration process, met certain conditions and supplied identification to the satisfaction of RA before a Smartcard can be issued. Smartcards will NOT be issued until all conditions have been satisfied. Each Smartcard user will also need to read and agree to certain Terms and Conditions prior to using the Smartcard to access any system.

7.3 Assigning Access to Systems

Access to systems will be managed via the Smartcard System Access Form (formerly the RiO Registration Form).

This form will be completed by the users Manager/Supervisor and will provide all of the information required to set an individual up with a Smartcard profile and a RiO profile (or SCR, Choose & Book or ESR access).

The Manager will approve the relevant Access Position required based on the persons Job Role and confirm electronically that they need a Smartcard as part of their Role.

This electronic form is, in effect a Sponsor declaration that this person needs a Smartcard and Access to the system/s specified.

7.4 Removing Access to Systems

The Registration Authority will remove access to systems from electronic Leavers Notifications or from specific requests from HR (i.e. immediate termination, long term absence, disciplinary matters etc.)

See 7.7 Cancellation of Smartcards

Leavers will be closed in a timely fashion and access removed to AWP systems. Smartcards will only need to be retained if the Leaver has no plans to return to the NHS (i.e. retiring, moving abroad etc.)

The Smartcard should be retained by the Leaver if they are joining another NHS Organisation or could possibly return to the NHS in the future.

Smartcards may also be cancelled and retained by RA if they receive confirmation from HR or a Manager that there has been misuse of the Smartcard or if the member of staff is undergoing an investigation, been suspended, employment terminated or on long term leave etc.

7.5 Bank/Agency/Locum Staff

Temporary staff, (locums, agency staff, students, bank staff etc.) who require access to Rio and other NHS CRS applications need to fulfil the exact same requirements as permanent staff for registration purposes.

They must be ID checked (to e-gif level 3) and registered before they can be issued with a Smartcard and access to systems. This is set at National level and there can be no local deviation under any circumstances.

Line Managers/Sponsors will identify if Smartcard access is required for Bank and Agency staff and the Starters process will be followed in the normal way.

7.6 Updating of Smartcards

This activity will take place whenever a user changes role, has additional responsibilities added to their existing role requiring them to have access to additional data from the Care Records System or other Spine compliant system, or has left the organisation. Equally, this will apply to staff that no longer require access to a dataset and therefore must have that access revoked.

The sponsor will complete and sign the relevant form on behalf of the member of staff. This sponsor may or may not be the original sponsor. The RA Team will then make the necessary changes.

The signed and completed forms will be passed to the RA Team for safe and secure storage or the appropriate electronic process followed.

The RA team will run regular reports to show what access has been granted or revoked

7.7 Cancellation of Smartcards

Smartcards may be cancelled for a number of reasons:

- They are compromised - any inappropriate access or inappropriate disclosure with the use of Smartcards should be reported to the cardholder's line manager. The Line Manager will need to complete an incident form and also alert the RA Manager, access to the Smartcard will then be suspended pending investigation and following appropriate internal HR policies and procedures.
- Lost, Stolen, Damaged, Name Change or Photo Update

Cancellation/person removal must happen in a timely fashion and will be also linked with the Leavers Procedure within the Registration Authority Procedures where the person is leaving AWP or HR disciplinary policy due to inappropriate disclosure and the Smartcard is to be cancelled. The user or their sponsor will complete the relevant form and/or process.

The RA Team can run a report on all card cancellations if/when required for audit purposes.

7.8 Lost/Stolen/Damaged Smartcards

Cardholders who have either lost or damaged their Smartcard or had it stolen must report the fact at the earliest possible opportunity to the RA Manager or Agent via the IT Service Desk. The RA Manager/Agent will then cancel the card with immediate effect and the process for a replacement will be put in motion. An incident form should also be produced for Lost/Stolen cards.

They will not be required to produce any further documentation as the RA Agent/RA Manager re-issuing the smartcard will be able to examine the digitally held identity/photo of the applicant when re-issuing the card to guarantee that the applicant is the person who the original card was registered to.

It is a National Policy requirement for a lost or stolen Smartcard to be replaced in a face to face meeting with an RA Agent/RA Manager. This is needed in order to confirm the identity of the card holder by comparing them to the photo held on the National System. They will also need to be present to set their own passcode to a new Smartcard.

If the identity cannot be proven in the face to face meeting then ID may be required.

7.9 Temporary Access Cards

Temporary Access Cards (TAC), if in use, allow for continuity in the provision of healthcare due to lost, stolen, misplaced or damaged Smartcards. TAC cards may only be used to permit continuity of access in cases where the user does not have access to their own Smartcard (or the Smartcard System is not in use) and the normal process for re-issue is thought by the RA Sponsor not to be appropriate because:

- they are satisfied a user is unable to obtain their Smartcard
- there is a risk to healthcare provision (identified by the Issuer)
- there is significant business impact (as defined by the Executive)

TAC cards could have a pre-populated Access profile added for a particular Position – so there may be a ‘Nurse’ TAC Card, a ‘Health Professional’ TAC Card, an ‘Administration’ TAC card etc and they will be kept securely locked by a named senior person who will act as the responsible Custodian.

This responsible Custodian will sign out and record the use of the TAC Card on the appropriate form and unlock it for use. They will also be responsible for ensuring the card is returned.

TAC Cards may not under any circumstances be used to permit access to NHS Care Records Service compliant applications for newly appointed staff/students, temporary/agency staff or Locums etc unless they have been previously registered with their own digital identity and therefore checked to e-gif level 3 and issued with their own Smartcard in the past or pass an on the spot ID check to the same standard (e-gif level 3).

This regulation is set at National level and there can be no local deviation.

Custodians/Sponsors/RA personnel will ensure that these TAC cards are locked and kept physically secure when not in use and are only distributed following the process identified in the local policy and an audit log is maintained by the Custodian and sent to the RA Manager on a regular basis.

The Custodian should understand that any misuse of the TAC card will be their responsibility and as such they are accountable for its use. The Custodian should put their own steps in place to ensure the member of staff that they assign the card to understand their responsibilities in its temporary use.

TAC cards should only be used in the case of emergency. Staff should therefore be reminded at all times to have their Smartcards with them in order to carry out their duties in the provision of healthcare.

It is the duty of the name Custodian to ensure the TAC Card Usage Form is complete and available to the RA Team. It is essential this action is carried out. Failure to do so may result in the RA Team revoking the use of TAC Cards.

7.10 Incident Reporting

Any member of staff can report RA related incidents where they feel there is any risk to service users' or others' health or safety, confidentiality or the Trust's reputation.

All security incidents shall be reported via the Trust’s Incident Procedure, to the RA Manager and the Information Governance Officer for investigation. All security incidents shall be investigated to establish their cause, operational impact, and business outcome.

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

- Smartcard or Rio misuse
- Smartcard theft or loss
- Any non-compliance with local or national RA policy
- Any unauthorised access of Rio or other Smartcard applications
- Any unauthorised alteration of service user's data.
- Deliberate defacing or damage of the Smartcard

The RA Manager or Information Governance Manager will consider all reported incidents and any which are considered “significant" will be escalated to the Caldecott Guardian/Information Governance Management Group and the Trust Board if then considered necessary. A significant incident could for example be a single incident or a series of more minor incidents that could lead to a serious degradation of healthcare or information security and may require a review of working practices to avoid repetition.

Where incidents demonstrate that an individual member of staff may not be trustworthy by for example, breaching the security of information/confidentiality, then the RA Manager should initially consult with Human Resources/IG and Line Managers as appropriate who may determine whether disciplinary action is appropriate. It may also be necessary to revoke the smartcard associated with the member of staff.

8. Standards

This policy shall be assessed against the Information Governance Toolkit standards.

9. Monitoring or audit

The RA Manager will be responsible for ensuring an audit trail of all RA activity is maintained. This will include the RA forms and use the appropriate RA system to record information electronically. The RA Manager and RA Agents will be able to produce reports to show staff and students registered and card usage etc.

9.1 Reporting and Monitoring Procedures

An audit trail covering all cards issued, updated and cancelled, all roles and activities granted or revoked will be available.

Access will be reviewed regularly and reports generated monthly to quarterly to make sure staff (and Students) are given the most appropriate access to the relevant system/s.

10. References

- National RA Policy v1 Sept 14

  This is the NHS Digital National RA Policy that all local Policies need to adhere to.

- Registration Authority Process Guidance

  This document (available on the NHS Digital website) gives guidance to organisations relating to a Registration Authority’s processes and operation.

11. Appendices

11.1 CIS – Create New User (RA only)

The information in this form must be entered in Care Identity Service (CIS) in the event CIS is not being used to register a new Smartcard User. All mandatory fields must be completed to complete this process.

Applicants must present proof of identity as per the Identity Checks at NHS Employer Standards at the face to face meeting with the RA Manager, Advanced RA Agent, RA Agent or RA ID Checker (RA). RA must capture a photograph of the individual.

Applicant Personal Details	**(Please complete all fields as fully as possible in BLOCK CAPITALS)**		
Title: (e.g. Dr, Mr, Mrs, Miss etc.)		Date of Birth: (Mandatory)	
Given Name: (Mandatory)			
Middle Names:		Preferred name:	
Family Name: (Mandatory)		Previous Family names:	

Applicant Identifiers (Mandatory)	**(At least one Identifier must be completed)**
NI number:	
Passport number:	
Driving licence number:	

Applicant Contact Details	**(Please complete all fields as fully as possible)**
Telephone number:	
Mobile number:	
Email:	

Identity Verification (Mandatory) (3 Forms of ID: 1 Photo ID + 2 Address ID OR 2 Photo ID + 1 Address ID)		
Photo Identification	Passport	Driving Licence
Passport Country:		N/A
Passport/Driving Licence Number:		
Date of Issue:		
Address Identification:	Address 1	Address 2
Address ID Type: (Utility Bill, Electoral Register, etc.)		
Name of Company:		
Date of Issue:		

RA declaration (To be entered in the Notes field in CIS when entered by another RA)

I confirm that the Applicant specified above can be issued a Smartcard. I verify the original document was seen and confirmed to be genuine in a face to face meeting with the applicant.

RA Name:		RA Role:	
RA UUID:		Date:	

11.2 CIS – Modify User Personal Details

The information in this form must be entered in the Care Identity Service (CIS) in the event CIS is not being used to modify the personal details of an existing Smartcard User.

All mandatory fields must be completed to complete this process.

Smartcard Users must present proof of identity as per the Identity Checks at NHS Employer Standards at the face to face meeting with the RA Manager, Advanced RA Agent, RA Agent or RA ID Checker (RA).

Current Smartcard Details	**(Please complete all fields as fully as possible in BLOCK CAPITALS)**	
UUID: (Mandatory)		
Personal Details	**(Complete only fields requiring change/update)**	
Title (e.g. Dr, Mr, Mrs etc.):		
Given Name (Forename):		
Middle Names:		
Family Name:		
Preferred name:		
Previous family names:		
Date of Birth:		
NI number:		
Reason for change: (Mandatory – circle the appropriate reason and add corresponding ID information)	Marriage / Change of Name by deed poll / User name incorrect in CIS	
Identity Verification (Mandatory) (3 Forms of ID: 1 Photo ID + 2 Address ID OR 2 Photo ID + 1 Address ID)		
Photo Identification	Passport	Driving Licence
Passport Country:		N/A
Passport/Driving Licence Number:		
Expiry Date:		
Address Identification:	Address 1	Address 2
Address ID Type: (Utility Bill, Electoral Register, etc.)		
Name of Issuing Organisation:		
Date of Issue:		

RA declaration (To be entered in the Notes field in CIS when entered by another RA)

I confirm that the Amendment details specified above should be modified. I verify the original documentation was seen and confirmed to be genuine in a face to face meeting with the applicant.

RA Name		RA Role	
RA UUID		Date	

11.3 CIS – Position Assignment Modification

The information in this form must be entered in the Care Identity Service (CIS) in the event CIS is not being used to request the modification of a position assignment.

All mandatory fields must be completed to complete this process.

Reason for position assignment modification must be completed and inputted in the Notes field in Care Identity Service.

Please use additional forms when needing to amend positions belonging to multiple organisations.

Please complete the following mandatory fields in BLOCK CAPITALS:

User Name	User Smartcard UUID number
Organisation Name	Organisation Code

Position Name	Add/ Remove	Reason for position assignment modification	Position Assignment Start Date*	Position Assignment End Date*

* If the dates are left blank the profile starts now and ends at the CIS default end date (10 years).

RA / Sponsor declaration (To be entered in the Notes field in CIS when entered by another RA)

I confirm the Position amendment(s) detailed in this form are correct and can be made to the user above.

RA / Sponsor Name:	
RA / Sponsor UUID:	
Date completed:	

11.4 Identification Criteria

Employees/Students will need to provide either of these two combinations:

2 forms of photographic personal identification **and** 1 document confirming their address

or

1 form of photographic personal identification **and** 2 documents confirming their address

or if they do not have any photo ID then the following is required:

2 forms of non-photographic personal identification **and** 2 documents confirming their address **and** A passport sized photograph and signed statement endorsed by someone of legal standing within their community (magistrate, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager, or civil servant)

All documents must be originals, or copies of originals certified by a solicitor.

Acceptable photographic personal identification includes:

- current UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities passport
- passports of non-EU nationals, containing UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK
- a current UK (or EU/other nationalities) photo-card driving licence (providing that the person checking is confident that non-UK photo-card driving licences are bona fide)
- a national ID card and/or other valid documentation relating to immigration status and permission to work.

Any document that is not listed above (ie an organisational ID card) is not acceptable.

Acceptable confirmation of address documents include:

- recent utility bill (gas, electricity or phone) or a certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms (note: mobile telephone bills should not be accepted as they can be sent to different addresses). Utility bills in joint names are permissible
- local authority tax bill valid for the current year
- current UK photo-card or old-style driving licence (if not already presented as a personal ID document)
- bank, building society or credit union statement or passbook containing current address 2
- most recent mortgage statement from a recognised lender

- current local council rent card or tenancy agreement
- current benefit book or card or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit
- confirmation from an electoral register search that a person of that name lives at the claimed address
- court order

The date on these documents should be within the last six months (unless there is a good reason for it not to be, eg, clear evidence that the person was not living in the UK for six months or more) and they must contain the name and address of the applicant.

Acceptable non-photographic proof of personal identification documents include:

- full UK birth certificate – issued within six weeks of birth
- current full driving licence (old version) – provisional driving licences are not acceptable
- residence permit issued by the 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
- most recent tax notification from HM Revenue and Customs (formerly Inland Revenue)
- current 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
- Home Office letter IS KOS EX or KOS EX2
- Building industry sub-contractors certificate issued by HM Revenue and Customs (formerly Inland Revenue)

11.5 Care Identity Service and Position Based Access Control (PBAC)

The Care Identity Service (CIS) was rolled out nationally in February 2015.

The new service has replaced a number of the existing Spine systems used for the creation of Smartcards and a national digital identity including User Identity Manager (UIM), Card Management System (CMS), RA Reporting via Enhanced Reporting Service (ERS), End Point Registration, Organisation Migration systems and all necessary functionality contained within the existing Spine User Directory (Calendra), with a unified application. This new Identity and Access Management system provides a single location for all RA activities.

It serves as a system to print and manage Smartcards and allows Access Positions to be created and assigned to allow staff to access systems such as RiO, ESR, Summary Care Record, Choose & Book and SUS.

CIS uses Position Based Access Control (PBAC) to provide access to these systems.

Position Based Access Control (PBAC)

Strict control of access to patient care records is fundamental to the operation of the NHS Care Records Service (NHS CRS). Position Based Access Control (PBAC) provides a simple and effective mechanism for providing users with the access they need in the course of their work, whilst also ensuring that these access rights are properly managed and appropriate for the job they are doing.

Instead of requiring case-by-case scrutiny for every person who requires access to care records, PBAC grants these rights according to the access control position to which their job is assigned. Once the rights attached to each access control position have been approved - along with the jobs included in these different positions - the process of granting access rights for staff becomes much simpler.

The PBAC Access Positions (set up for use in RiO) that have been approved and set up within AWP are shown in the AWP RBAC Mapping Overview document that can be requested from the RA Team

Version History

Version	Date	Revision description	Editor	Status
0.1	0.1	20/11/2009	Initial draft	RA Analyst
1.0	02/03/2010	Amendment from Quality & Healthcare Governance Committee	Sys Dev Mgr	Approved
1.1	23/09/2010	Minor Amendments	RA Manager	Approved
1.2	15/6/2011	Minor Amendments & addition	RA Manager	Approved
2.0	4/9/2014	Re-written due to new Smartcard System (UIM)	RA Manager	Approved
2.1	9/6/2015	Re-written due to new Smartcard System (Care Identity Service – CIS)	RA Manager	Draft
3.0	22 January 2016	Approved by Finance and Planning Committee	HD	Approved
3.1	26/06/2017	Updated due to process / form changes	RA Manager	Approved
4.00	18/09/2017	Administrative review Removal of HSCIC and replaced with NHS Digital Removal of all references to National Programme for IT	RA Manager	Draft
4.1	9/10/2018	Minor amendment to update mention of Data Protection act to 2018 version	RA Manager	Approved
5.0	9/1/2019	Reviewed with minor updates	RA Manager	Approved