Essex Partnership University
NHS Foundation Trust

Registration Authority Procedure

(Issue and Use of Smart Cards)

PROCEDURE REFERENCE NUMBER:	CPG29
VERSION NUMBER:	2
REPLACES SEPT DOCUMENT	CPG29
REPLACES NEP DOCUMENT	N/A
KEY CHANGES FROM PREVIOUS VERSION	
AUTHOR:	Head of Service – System Delivery
CONSULTATION GROUPS:	Information Governance Steering Sub Committee
IMPLEMENTATION DATE:	October 2017
AMENDMENT DATE(S):	04/09/2018
LAST REVIEW DATE:	15 Nov 18
NEXT REVIEW DATE:	15 Nov 2021
APPROVAL BY INFORMATION GOVERNANCE SUB COMMITTEE:	24th September 2018
RATIFICATION BY QUALITY COMMITTEE:	15th November 2018
COPYRIGHT	2018
PROCEDURE SUMMARY	
The Trust monitors the implementation of and compliance with this procedure in the following ways:	

Services	Applicable	Comments
Trust-wide	✓	

The Director responsible for monitoring and reviewing this policy is

The Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Registration Authority Procedure (Issue and Use of Smart Cards)

APPENDICES

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Registration Authority Procedure
(Issue and Use of Smart Cards)

Assurance Statement

These procedures set out clear guidelines to ensure that there is a system in place to ensure that all risks associated with registration practices for electronic access to care records and other national applications are minimised. It will ensure that practices are carried out in line with national guidance and apply to all staff (permanent, agency and/or contracted) within any service within the organisation. It will ensure that the risk of authorising staff to access electronic care records / national applications is kept to a minimum.

1. INTRODUCTION

1.1. Essex Partnership University NHS Foundation Trust (the Trust) aims to provide an environment that is safe and secure for its staff and the people who use our services.

1.2. These procedural guidelines and the related policy document outline the Trust's undertaking to ensure that information is held and accessed securely.

1.3. This document describes procedures for the operation of the Registration Authority (RA) within the Trust.

1.4. The Trust will comply fully with the latest published national policies and procedures identified in the following documents:

1.5. NHS Digital Registration Authority Policy and related guidance can be found within the following link: https://digital.nhs.uk/Registration-Authorities-and-Smartcards

1.6. Essex University Partnership Trust is the result of the merger of South Essex University Partnership Trust and North Essex University Partnership Trust. It is not currently possible to implement a standardised procedure across the whole of the Essex University Partnership Trust as the two areas have separate processes. A single RA team will manage all RA requests through a structured approach.

2. GENERAL PRINCIPLES

2.1. Healthcare professionals who need to access national applications (e.g. electronic care records, ESR, patient administration systems) will need access to the national spine directory through the issue of a smartcard.

2.2. All national applications use common security and confidentiality approaches based upon the professional's organisation/s role/s, area/s of work and business functions.

2.3. The procedures covered in this document are the local support necessary to uphold national policies and procedures:

- Identification, appointment and registration of RA team members
- Registration and management of Spine Application users
- Management of RA smartcards, pin/passcodes and user profiles
- Management and ordering equipment
- Issue resolution

3. ROLES AND RESPONSIBILITIES

3.1. Board of Directors

The Board of Directors of the Trust will:

- Ensure that the RA process is embedded within the information governance framework for the Trust to ensure that the best interests of patients are considered.
- Nominate a Board member with overall responsibility for RA within EPUT. The Executive Chief Finance & Resources Officer has been nominated to take on this role of responsibility.
- Receive/nominate an appropriate sub-committee to receive periodic reports. For EPUT this will be the Information Governance Steering Sub Committee.

3.2. Executive Team

- The Executive Team will be responsible for embedding, within the Information Governance Framework, governance of the Registration Authority (RA).
- Identified members of the Executive Team must be directly responsible for the governance of RA: this will be the Executive Chief Finance and Resources Officer.
- The Executive Team will assign responsibility to appropriate Committees to, review and approve the appointment of the RA Manager(s) and Sponsor(s). These will be the Information Governance Committee for mental health and corporate staff and the appropriate Systmone operational group for community staff.
- Direct RA Manager(s) and Sponsor(s) to work within the Information Governance Framework for the organisation and review and approve, where

appropriate, inter-organisational agreements, fall-back smartcard distribution and usage policy and the use of same for testing during Commissioning and other local processes as proposed by the RA Manager.
- Given the increasing importance of RA within the Information Governance Framework the Executive Team will ensure that RA is a standing agenda item at appropriate Trust Committees/groups e.g. Integrated Governance Steering Sub Committee.

3.3. RA Manager

The RA Manager and the RA team, on the Executive Team's behalf, will be responsible for the strategic overview of the Trust's RA system and must ensure that all RA procedures performed in line with the National Policy and local procedures in CIS (Care Identity Service).

The RA Manager has specific responsibility for:

- The approval on CIS of the EPUT RA agent role which allows relevant RA agents to approve the creation and modification of positions that have been agreed by the Information Governance processes and structures within the Trust within CIS.
- The RA Managers and the RA team are also responsible for ensuring the quality of registration arrangements.
- Under the guidance of the RA Manager, the RA team will be responsible for undertaking monitoring / audit of the RA function, use of Smartcards, investigations of breaches in liaison with the Information Governance Manager and ensuring timely reporting of outcomes to appropriate Trust Committees.

3.4. RA Agents

Registration Authority Agents are responsible to the RA Manager for the accurate creating and granting of requests within CIS. These requests may relate to the following:

- Creating a new user
- Modifying a user
- Closing or re-opening a user
- Granting an Access Control Position
- Granting the modification of an Access Control Position
- Granting certificate renewals
- Actions in relation to workgroups, if necessary
- Technical support for Smartcard problems (passcodes, certificates, card readers etc.)
- Ensuring all new users digitally sign terms and conditions of Smartcard use.
- Staff will receive the latest version of the terms and conditions (at least annually) when the new version is available nationally, as a reminder. It will be the responsibility of each staff member to ensure they have read and understood the terms and conditions of use.

- RA Agents will be responsible for ensuring that any / all incidents (misuse, anomalies and problems) are reported to the RA Manager and Information Governance Manager for investigation as well as being reported via Datix.
- The RA team under delegated responsibility from the RA Manager will maintain a list of RA Sponsors and Agents within the organisation.

3.5. RA Sponsors

Sponsors are responsible for ensuring only appropriate access to Spine linked applications is granted.

This will be achieved by completing the appropriate RA forms (see appendices) and sending them to the RA email account (rasupport@nhs.net) with "RA support" in the subject line. Forms will only be accepted that come from the sponsors email account as this acts as proof of their approval for the granting of the role. Incomplete forms will not be processed but returned to the sponsor.

The Trust will agree a number of sponsors in each clinical or operational area, as appropriate.

These sponsors will only sponsor staff and positions for which they have responsibility. The sponsors must have a valid smartcard that contains the sponsor access rights B1300. Additionally the RA Manager and the AD Systems and Information Governance, will have the authority to grant these sponsor requests in all areas in the absence of the appropriate sponsor.

All changes in relation to an individual are part of a management process and procedure that are embedded in the trust, the sponsorship responsibilities for these approval requests will reside in a combination of line managers, and RA staff. The model that will be followed is:

- A manager will, as part of normal procedures, inform HR if staff changes are required – these will include hiring a new member of staff into an agreed post subject to establishment control procedures, changing their personal details or moving them from one post to another.

- The service manager must advise the service sponsor so that the service sponsor can inform the RA staff if any changes are required to access on smartcards because of this.

- It is the service manager's responsibility to advise sponsors of leavers and ensure the RA02 forms are submitted to the RA Team.

- As a further audit, to ensure access remains legitimate, the RA team will remove access to Systmone for anybody who has not accessed a unit in the last three months. Renewed access will require a new RA02 request.

- On receipt of a completed RA02 form from the appropriate sponsor, RA staff will enact the necessary changes and will record the details of the request on the CIS system.

3.6. Smartcard Unlockers

Within each service and base, some staff should be appointed to act on behalf of the trust in order to provide smartcard unlocking services to users of spine applications. To enable them to do this they will be given additional access rights on their card B0263 and on appointment will receive instruction on the process.

They will have responsibility for:

- Unlocking of smartcards
- Renewing expiring certificates, where staff have difficulties in doing this themselves.

Card Unlockers will be identified by the Service Managers with support from the RA team, with delegated authority from the Board Director for RA activity as being suitable persons by virtue of their status and role.

All smartcard users will be encouraged to register on CIS to be able to self-unlock their smartcard.

4. RA ORGANISATION

4.1. The RA staff are a team within the Trust with appropriate organisational authority to be responsible for ensuring that all aspects of the registration services and operations are performed in accordance with national policies, procedures and legal obligations.

4.2. The RA team is responsible for providing arrangements that will ensure tight control over the issue and maintenance of smartcards whilst providing an efficient and responsive service to meet the needs of users.

4.3. All RA team members must have sufficient training to carry out their RA tasks in accordance with national policies and procedures.

- The RA team must be individuals capable of trust, as they will be handling sensitive information covered by the Data Protection Act and giving access in accordance with guidelines set out by the Access Control team and local policies. They will be key players in ensuring the NHS Code of Confidentiality is followed.

- RA Managers and Agents need to be familiar with the Registration Authorities Policy and operational guidance, which describes procedures around registration and issuing of cards. They must also be familiar with the registration software, CIS, and how the electronic process for approving and granting requests must be carried out.

- The RA team within the Trust must also be aware of the Access Control Positions created to govern access rights within the trust.

4.4. The EPUT Registration Authority comprises of the following personnel:

- EPUT Board Director with RA responsibility
- RA Manager – who is trained and knows the agent function and is connected to the national team via the national RA Manager's Distribution list and delegates this responsibility to the RA team
- RA Agents who check identity to Level 3 standards at point of Smartcard issue. Who are also responsible for the granting of Access control positions on the receipt of the RA02 from an appropriate sponsor
- Those fulfilling the role of RA Sponsor within the organisation
- Those fulfilling the role of Card Unlocker within the organisation

4.5. The Trusts' RA Executive is the Executive Chief Finance and Resources Officer. Their duties, that are allowed to be delegated under the National Registration Authority Policy, have been delegated to the RA Manager and, in turn, to the RA team; who are responsible for the strategic planning and day-to-day management of the RA services. They will be responsible for assigning staff to access positions and dealing with card problems. They will provide Reports on RA Activity when requested by the Information Governance Steering Sub Committee on:

- Staff who have left and access has been removed
- Staff who have had access granted or changed
- Remedial activity (needing to unlock Smartcards, technical issues etc.)
- Any misuse or untoward incidents in relation to Smartcards and access together with remedial actions

4.6. The RA services provided will be:

- User Registration
- Access Control Position Maintenance
- Creating Positions
- Modifying Positions
- Cancelling Positions
- Revocation and cancelling of Smartcards
- User Suspension
- PIN/Passcode resetting
- Smartcard certificate renewal and exchange
- Identification and Appointment of RA Team Members
- Equipment ordering approval
- Registration of RA Team Members
- Registration of Spine Application Users
- Management of Spine Application Users
- Management of RA Smartcards
- Management of RA PIN/Passcodes
- Equipment ordering and management
- Existing Paperwork – storage and disposal

- Issue resolution
- Development and streamlining of procedures where possible

4.7. The RA function will be available between the Trusts core working hours of 9am – 5pm Monday to Friday excluding bank holidays. Users who need support should contact the RA support helpdesk by either email or phone.

5. REGISTRATION PROCESSES AND PROCEDURE

5.1. The CIS system has the functionality to be paperless and therefore there are no national RA paper forms for requesting or amending user rights. Currently EPUT will continue to use the EPUT created forms based on the national information requirements (see appendix) which will be completed online and submitted to the RA team via the sponsor's email account. Existing paper records must be retained in line with the requirements contained within HSC 1999/053, which stipulates the retention duration for Human Resource type records.

5.2. Registering a new user and personal detail changes:

- If a new employee joins the trust or an existing employee takes on a role which requires them to utilise spine compliant systems then they will require a smartcard and appropriate access rights.

- The new user will supply appropriate identity credentials to the RA team at point of smartcard issue, following the receipt of an RA01 and, where necessary an RA02 form, from an appropriate sponsor.

- These standards can be viewed at http://www.nhsemployers.org/your-workforce/recruit/employment-checks/identity-checks.

- The individual will have these details recorded in CIS by an RA agent who will also record on the system who is sponsoring the request from the details on the completed RA forms. Where an individual does not already have a smartcard, the RA agent will issue the smartcard (For users of Systmone the card may not be fully active until necessary training has been undertaken). At the point of receiving their smartcard a new user will be asked to digitally sign the national terms and conditions of smartcard use and be reminded that failure to adhere to these requirements may result in disciplinary action being taken against the individual. Furthermore the user will be reminded that using their access rights inappropriately to obtain personal information in relation to an individual that is not related to providing their care, or managerial tasks in relation to their care, may also be subject to disciplinary action.

Where a user's personal details change (for example a surname change due to deed poll or marriage), the user will need to complete an RA05 form, confirm they have updated their details on ESR and produce the necessary verification document to the RA team, who will update the CIS system and reissue a smartcard in the new name.

5.3 Managing Access Rights – Access Control Positions:

- In CIS, access rights are contained within Access Control Positions. These are created, amended and cancelled as a process independent from users. Users are then assigned to these positions, moved between positions, assigned to multiple positions or unassigned from positions.

- Approving and granting Access Control Positions require advanced RBAC activities. B0274 Perform RA Activities Advanced (grant the content of an access control position) is given to the RA team, additionally the RA manager and the senior RA agent will be given R5080 (the senior RA agent will only use these rights in the absence of the RA manager to ensure continuity of service).

- During the deployment of the CIS system, a number of standard access roles were created for Systmone Access, which were agreed at the appropriate SystmOne Operational meetings. Any changes, additions or deletions from these should go through a similar approvals process.

- Within Corporate service the system-generated positions were adopted and these have now been converted to CIS positions, any changes, additions or deletions from these should go through an approvals process via the Information Governance Steering Sub Committee.

- The RA agents will use the approval and self-grant functionality within the system to make the amendment. They will record on the CIS system the sponsors' details. The Email and attached RA forms will be stored securely for audit purposes.

- Where an individual leaves the trust then the RA team will disassociate the user from the access control positions they are assigned to within the trust.

- It is the team leader's responsibility to advise the sponsor who will then advise the RA team by completing an RA02 when a member of staff leaves the trust. If the user is moving to or is planning to do so in the future, another healthcare organisation, that is the extent of the action needed. The staff member should retain their smartcard. If however, the user is leaving healthcare for good an RA03 should be submitted so that their profile can be 'closed' within CIS and their smartcard should be destroyed.

5.4 Management of Smartcards:

- Smartcards should be treated with care and protected to prevent loss or damage. Staff should not deface them in any way. On using their smartcard for the first time, they will be presented with an electronic version of the Terms & Conditions, which they need to read and understand before electronically signing them.

- There will be situations where a smartcard might need to be revoked, for example, the card may have been damaged, a new photograph is required, or a smartcard is lost.

- Revocation of a smartcard will usually be as a result of disciplinary action and the RA staff will need necessary authorisation from the service lead that this step is required. If so, this will be done within CIS using the 'Cancel Smartcard' link.

- If a smartcard is lost, the user must complete a DATIX and their manager must complete an RA03 and submit it to the RA team to issue a new smartcard via CIS.

- Where a card is damaged, or the photograph needs updating, this is done via the manage smart card functionality within CIS. The identity of the user will need to be re-verified at a face to face meeting, this will be done by comparing their appearance with the image contained on their CIS record.

5.5 Fall-back Smartcards:

- Currently, it is not considered necessary as part of business continuity arrangements that fall-back, or short-term access, smartcards is used. Should this change these can be created using the CIS workflow utilising the links within the 'Manage fall-back' section of CIS

5.6 PIN/Passcode Unlocking/Changing:

- Users who have forgotten their PIN/Passcode or who have been locked out of Spine Applications because of three failed login attempts; if they are registered for self-service they will be able to unlock their smartcards themselves; otherwise, they will need to contact their local card unlocker or the RA team. A face-to-face meeting will then need to be arranged to have the smartcard unlocked.

- Where a user suspects or may know that their smartcard has been used by another person they need to deliberately enter their password incorrectly to block the smartcard and use the options detailed above to get it reset. They should also advise their line manager so a Datix can be raised and any other necessary action taken.

5.7 Temporary, Locum, Local Authority, Bank, Contract Staff:

- Temporary staff may need access to spine applications as part of the work they are required to perform. It is possible to issue a smartcard to these users and assign them to an access control position. CIS allows this to be for a limited period if desired. The Service Lead needs to consider this at the outset.

- A temporary member of staff working as part of a team may not need access should the record access be the responsibility of someone else.

- Does the member of staff have the necessary training to effectively use the national / local application

- If these two criteria are met the smartcard issuance and assigning access controls position processes above can be used to grant access.

6. INCIDENT REPORTING

6.1 All staff must report incidents where they feel that there is a risk to patient health, confidentiality, system security or the Trusts' reputation.

6.2 Incidents must be reported to the RA team who will ensure that the Information Governance Manager is informed of the breach, a Datix report is raised, and a full investigation will commence.

Examples of incidents are:

- Smartcard or application misuse
- Smartcard theft / loss / damage
- Failure or unavailability of Spine applications
- Non-compliance of local or national RA policy
- Any unauthorised access of Spine applications
- Any unauthorised alteration of data
- Inappropriate maintenance activity by an agent or manager

6.3 The RA team will consider all incidents reported to them. All incidents will be logged on an incident log and then be escalated, as appropriate to the agreed Committees / Board Director with responsibility for RA.

6.4 If necessary, the RA team, under guidance of the RA Manager, will revoke a user's access rights pending direction from the Board Director. Any incidents considered significant will be escalated to the Senior Management Team depending on the nature of the incident. Removing the capacity for a member of staff to use any of the national / local applications must not prejudice the disciplinary procedure (i.e. because a card or profile is deactivated it does not necessarily mean that the person to whom the card belongs has done anything wrong).

6.5 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 Board Director will consider incidents reported to them and decide whether systems or working practices should be reviewed as a result.

6.6 Incidents involving breaches of security or that demonstrate that a user may not be considered trustworthy should be reported to Human Resources and the Board Director by the RA Manager so that any disciplinary measures required may be taken. Human Resources will decide which other members of staff need to be involved (e.g. line manager, IT manager). These will be referred to in the Trust disciplinary procedures.

6.7 The Board Director and RA Manager will consider the appropriateness of reporting to the NHS Digital any major breaches in order to ensure any risks resulting from the event can be taken account and mitigated against.

7 MANAGEMENT AND USE OF RA EQUIPMENT

7.1 The RA Team, with delegated responsibility from the RA Manager, will ensure that adequate stocks of smartcards are available. This supply of cards is to be used for internal requirements in relation to any services that the trust may acquire.

7.2 IT Services will ensure that there is sufficient computer equipment to support users of RA services. All RA equipment will be subject to policies and procedures governing the management and control of IT Assets for the trust.

7.3 It is the RA Team's responsibility to ensure the IT department is kept up to date and can plan for roll out of any new software such as new versions of the Identity Agent.

7.4 All RA Users must take reasonable measures to prevent the loss or damage to RA equipment including smartcards.

7.5 New smartcards are obtained through the RA team.

8 TRAINING

8.1 All Trust RA members will have sufficient training to carry out their RA tasks in accordance with national / local policies and procedures.

8.2 Starters:

- All new starters will be registered and trained, as required, as part of their Service Induction within the Trust.

8.3 General Users:

- All national / local application users must:
    - Have sufficient training to carry out their application tasks without risk
    - Be trained sufficiently prior to the use of smartcards
    - Be trained on the aspects of application use relevant to their role(s) – this guidance may be written as well as verbal
    - Be trained on the national and Trust RA processes

8.4 Temporary, Locums, Bank, Agency and / or Contract Staff:

- Training of temporary staff, who are smartcard holders, will be reviewed at each point of employment to ensure they have sufficient training in the use of the particular application needed to be accessed for their current role.

9 INTER-TRUST, CSU/CCG/ PRACTICE AGREEMENTS

9.1 The Trust and other partner organisations will operate and manage separate Registration Authorities. The Trust can manage RA users on behalf of the other organisation where staff are shared or work is carried out in shared facilities under written agreement only. The agreement needs to ensure there is clarity over the obligations, liabilities and how misuse of cards is to be handled.

10 REFERENCE OTHER DOCUMENTATION OR LEGAL OBLIGATIONS

10.1 Other Trust policies/procedures

- Adverse Incident (CP3)
- Information Governance & Security (CPG50)
- Data Protection & Confidentiality (CP59)
- Information Sharing and Consent (CP60)
- Consent to Examination or Treatment Guidelines (CG16)
- Records Management (CP9)
- Fraud, Theft & Corruption (CP11)
- Code of Conduct (CP15)
- Conduct & Capability (HR27)
- Safeguarding (CLP37 Children & CLP 39 Adults)
- Corporate Records (CP61)
- Legal Services (CP63)

10.2 Other documentation:

- NHS Care Record Guarantee
- Confidentiality: NHS Code of Practice

10.3 Legal Obligations:

- General Data Protection Regulations (GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- Computer Misuse Act 1998
- Common Law of Confidentiality

The lists of documents and legal obligations above are not exhaustive and others may be developed between reviews of this procedure that should be taken into consideration when using smartcard-enabled systems to process person identifiable information, such as, SystmOne.

END