Essex Partnership University
NHS Foundation Trust

REGISTRATION AUTHORITY POLICY

PROCEDURE NUMBER:	CP29
VERSION NUMBER:	2
AUTHOR:	Head of Service – System Delivery
REPLACES SEPT DOCUMENT	CP29
REPLACES NEP DOCUMENT	
CONSULTATION GROUPS:	Information Governance Sub-Committee
IMPLEMENTATION DATE:	October 2017
AMENDMENT DATE(S):	September 2018
LAST REVIEW DATE:	November 2018
NEXT REVIEW DATE:	November 2021
APPROVAL BY INFORMATION GOVERNANCE SUB COMMITTEE:	24th September 2018
RATIFICATION BY QUALITY COMMITTEE:	15th November 2018

Policy Summary
The Registration Authority Policy aims to ensure that the Trust (EPUT) complies with requirements of the National Registration Authority Policy as dictated by NHS digital who are the lead Registration Authority and delegate responsibility for organisations to run local Registration Authority functions
The Trust monitors the implementation of and compliance with this policy in the following ways;
The regular reviewing of smartcard users access to ensure only the necessary rights are available on their card
SCOPE

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 (RA) POLICY
(Issuing and Use of Smartcards)

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

1.0 INTRODUCTION

2.0 BACKGROUND

3.0 SCOPE

4.0 RA ORGANISATION

5.0 MONITORING & REVIEW

6.0 MISUSE OF SMARTCARDS

7.0 REFERENCE TO OTHER DOCUMENTATION

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

REGISTRATION AUTHORITY (RA) POLICY
(Issuing and Use of Smart Cards)

Assurance Statement

This policy and its associated procedures set out clear guidelines to ensure that there is a system in place which ensures all risks associated with Registration Authority 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 in order to safeguard patients, residents, clients, staff and the Trust, and will apply to all staff (permanent, agency and / or contracted) within the organisation authorised for electronic access to national / local applications and records.

1.0 INTRODUCTION

This purpose of this policy is to ensure the trust can demonstrate that it complies with the minimum national requirements of the national policy that are set out by Registration Authority hierarchy.

In Public Key Infrastructure (PKI) terms there is a single Registration Authority (NHS Digital). All organisations that run a local Registration Authority do this on a delegated authority basis from NHS DIGITAL.

NHS DIGITAL as the single Registration Authority who needs to assure itself that organisations are operating appropriately and discharging their duties in an effective and consistent fashion. The national policy outlines the minimum national requirements to provide such assurance, as such; deviation from this policy document due to a local preference is not permitted.

This document describes procedures for the operation of the Registration Authority within Essex Partnership University NHS Foundation Trust, (hereafter known as 'the Trust').

The Trust needs a Registration Authority to manage the distribution and use of Smartcards and for providing dedicated support to staff requiring access to data via the National Spine.

2.0 BACKGROUND

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

- Registration Authorities Operational Process Guide
- NHS DIGITAL Registration Authority Policy
- https://digital.nhs.uk/Registration-Authorities-and-Smartcards

- The NHS Confidentiality Code of Practice (https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice)

3.0 SCOPE

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

- The trust's RA personnel (Manager, Sponsors and Agents)
- Board Director responsible for RA The trust's confidentiality experts (e.g. Senior Information Risk Owner, Caldicott Guardian, Information Governance Team)
- The trust's Information Governance Steering Sub-Committee (for purposes of monitoring the RA)
- All staff that are users of the RA service (e.g. Smartcard holders)

3.2 The use of the word staff in this document means, people who are directly employed by, or contracted to provide a service to, or are part of an agreement with the Trust.

3.3 Where services are contracted or part of an agreement, then adequate provision for the necessary compliance with RA requirements needs to be made in the contract/agreement.

4.0 RA ORGANISATION

4.1 The Registration Authority is a team within the Trust with appropriate organisational authority, who is responsible for ensuring that all aspects of registration services and operations are performed in accordance with national policies and procedures.

4.2 They are responsible for providing arrangements that will ensure tight controls over the issue and maintenance of electronic Smartcards (which supplies access to local and national applications) whilst ensuring an efficient and responsive service that meets the needs of the users.

4.3 <u>Roles and Responsibilities</u>

In order to discharge the responsibilities delegated from NHS DIGITAL in relation to Registration Authority activity the roles and responsibilities are as follows:

- A Board/EMT person accountable for RA activity within the organisation that must be overtly identified and named.

  For the trust this is Mark Madden, the Executive Chief Finance Officer and Resources Officer. This ensures that the RA Manager knows who to raise issues with.

- The Board/EMT individual must report to the Board/EMT annually on RA activity and must sign off on the RA Data Security and Protection Toolkit (DSPT) submissions.

- A RA Manager (Tracey van Wyk, Head of Service – System Delivery) is responsible for running the governance of RA within an organisation. As such, a RA Manager must agree and sign off on local operational processes and should assure themselves regularly that these processes are being adhered to (**NOTE:** local processes cannot contradict the national RA Policy documentation). A RA Manager also has the responsibility for registering RA staff in their own organisations and any child organisations, as appropriate. A RA Manager is also responsible for ensuring the effective training of RA Agents and Sponsors within their organisation.

- Roles available in the Registration Authority software, Care Identity Services, allow the RA Manager to delegate certain aspects of RA activity. These include Advanced RA Agents, RA Agents (ID checking only) and Local Smartcard Administrators. The following table indicates which responsibilities can and delegated.

RA Manager CANNOT delegate	**RA Manager CAN delegate**
• Responsibility for running RA Governance in their organisation • Responsibility for ensuring local processes are in place that meet policy and guidance for the creation of digital identities, production of smartcards, assignment of access rights, modifications to access and people and certificate renewal and card unlocking • Assignment of RA Agents and sponsors and the registration of RA Agents and Sponsors • The training of RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process. A RA Hosting organisation parenting another RA Hosting organisation is responsible in providing training to the RA Manager in the next level down • Facilitation of the process for agreeing the organisation's access control positions • Responsibility for ensuring that appropriate auditing is carried out • Responsibility for ensuring users are compliant with the terms and conditions of Smartcard usage • Verification of user's ID to e-GIF level 3 when they register users • Responsibility for ensuring the security of paper based RA records • Responsibility for ensuring all service issues are raised appropriately locally and nationally	• Creation of local processes that meet policy and guidance for the creation of digital identities, production of smartcards, assignment of access rights, modifications to access and people and certificate renewal and card unlocking • Operation of core RA processes of registering a user, the approval and granting of access, the modification of personal details and the modification of access rights • The implementation of the local auditing process • Ensuring users accept terms & conditions of Smartcard use when registering them • Operational security of (paper based RA records • Raising service issues as appropriate and through the correct channels

- Identity checking must be carried out by those holding an RA role – RA Managers and the RA Agent roles.

5.0 MONITORING & REVIEW

5.1 The Trust's ITT Directorate will manage the RA function provided by the Trust and monitor the performance of the service in line with the associated procedural guidelines.

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

5.3 Auditors will look to confirm that:

- Smartcards are handled securely by users
- RA documents are used and stored appropriately
- Access to Spine Applications and Records is controlled appropriately
- Unused smartcards are stored safely and appropriate records kept

5.4 To aid audit the following electronic records will be maintained:

- The number of smartcards held
- The number of smartcards issued
- The number of smartcards revoked

5.5 The RA Team will provide the Information Governance Steering Sub Committee with regular updates, based on the audits, of any information breaches in relation to the use of smartcards (minimum quarterly).

5.6 An annual summary on the RA registration function (e.g. information on numbers registered, amendments and revoked registrations, breaches) will be presented to the Information Governance Steering Sub Committee.

6.0 MISUSE OF SMARTCARDS

6.1 A staff member may report suspected smartcard misuse to their line manager, or the RA Team whichever is most appropriate. Depending on the severity of the allegation a written report may be required. In all cases suspected misuse should be reported to the Information Governance Team.

6.2 If it is suspected that a smartcard is being misused the certificate associated with the smartcard must be immediately suspended or revoked.

6.3 If smartcard misuse by a staff member is discovered the appropriate measures will be taken in line with the Trusts' disciplinary policy.

6.4 Formal incident reporting of such events should be carried out in line with the appropriate Trust policies and procedures.

7.0 REFERENCE OTHER DOCUMENTATION OR LEGAL OBLIGATIONS

7.1 Other Trust policies / procedures:

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

7.2 Other documentation:

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

7.3 Legal Obligations:

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

7.4 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