East London NHS Foundation Trust

East London NHS Foundation Trust
RA (Registration Authority) Policy

Version:	5
Ratified:	Quality Committee
Date Ratified:	September 2019
Name of originator/author:	Registration Authority Manager
Name of responsible committee/individual:	Information Governance Steering Group
Circulated to:	Members of IGSG
Date issued:	March 2018
Review date:	July 2022
Target audience:	All staff

Version Control Summary

Version	Date	Author	Status	Comment
1.0	09/12/2005	Registration Authority Manager	Final	Approved by Registration Authority Project Board-03/11/2005 Information Governance Committee-21/11/2005 Clinical Governance Committee-14/11/2005 Joint Staff Committee-08/12/2005
1.1	04/03/2010	Registration Authority Manager	Final	Approved by Information Governance Steering Group
2.0	19/12/2011	Information Governance Manager	Final	Revised in line with Trust policy format requirements. Approved by IGSG-05/01/2012
2.1	08/05/2012	Information Governance Manager	Final	Included section on RA security and maintenance
3.0	15/03/2015	Registration Authority Manager	Final	Revised in line with National RA Policy in line with Care Identity Service. National RA Policy using Care Identity Service (CIS)
4.0	15/08/2018	Registration Authority Manager	Final	Revised in line with Trust policy format requirements
5.0	11/07/2019	Registration Authority Manager	Draft	Revised in line with New Processes and National RA Policy

B	Contact Details	12

POLICY

1.0 Introduction

The Registration Authority (RA) is a department within the Trust that ensures all aspects of registration services and operations are performed in accordance with National Policies and Procedures. The RA is 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.

Healthcare Professionals need to be registered in order to ensure appropriate and secure access to Smartcard applications. The registration process for the National Programme has to meet the current national requirements. All NHS Digital applications use a common approach to security and confidentiality, based upon the NHS professional's organisation/s, role/s, and business function (Activity). The method by which Users will be enabled to access an NHS Digital application is via a Smartcard issued during the Registration Process. A Registration Authority, which is required to conform to the National Registration Policy, operates the Registration Process at a local level.

The East London Foundation Trust will comply fully with the latest published National Policies and Procedures.

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

2.0 Purpose

The Registration Authority has the following responsibilities-

- Ensuring that the National Registration processes and any local processes developed to support the National Registration processes are adhered to in full
- Ensuring that there is sufficient availability of resource to operate the registration processes in a timely and efficient manner to meet the organisational responsibilities
- Ensuring that the RA team members are adequately trained and familiar with the local and national RA processes
- Ensuring that an indexed and secure audit trail of applicants registration information is maintained
- All documents (physical and electronic copies) are kept secure in an area which only the RA team can access.
- Ensuring RA Team members are familiar with and understand Registration

Policy and Practices for GPG45 level 3 or 4 Authentications, Registration Authorities Setup and Operation and this document

- Notification of the creation and revocation of RA Managers (including their email address) to NHS Digital by sending an e-mail to ramanagers.agents@nhs.digital.gov.uk

- Ensuring that there are sufficient Smartcards and Smartcard issuing bodies and maintenance equipment for the organisation. Note: see NHS Digital RA Hardware Ordering Process

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

- Registration Authority Manager
- Registration Agents
- Registration Authority ID Checkers
- Local Smartcard Administrators

The services available are:

- User Registration
- Issuance of Smartcards
- Role Profile maintenance
- Revocation and cancellation of Smartcards
- User Suspension
- PIN/Passcode resetting
- Smartcard renewal and exchange

The above services will be available during the Trust Registration Authority Service Core hours, 08:00 to 16:00 Monday to Friday, not bank holidays. Local Smartcard Administrators are available in each Directorate to unlock/reset blocked/ cards or forgotten passcodes and Users can now register to unlock their own Smartcards.

2.1 RA/Care Identity Service (CIS)

Background

This document outlines:

- The RA Hierarchy and the principle of delegated authority to local organisations to run their RA.

- The requirements for creating a nationally verified digital identity.

- The roles and responsibilities within organisations that run their own Registration Authority activity.

- Requirements in relation to Smartcards.

- The requirement to develop and implement a local RA Policy.

- CIS simplifies the registration process for issuing Smartcards.

Purpose

To align Registration Authority with the National RA Policy using CIS to reduce the use of paper forms to create a digital identity.

3.0 Duties

All Trust RA staff will have sufficient training to carry out their RA tasks in accordance with National Policies and Procedures. They will be individuals capable of trust, as they will be handling sensitive information covered by General Data Protection Regulations. They will be key players in ensuring the NHS Code of Confidentiality and the NHS Digital Acceptable Use Policy, Terms and Conditions is followed.

The name of the Board/EMT accountable person and the RA Manager must be named within the policy.

Senior Information Risk Owner (SIRO)

RA Manager

3.1 Registration Authority Manager

The RA Manager is accountable to the Trust Executive and is responsible for the set up and day to day running of the Trust RA service. Responsible for running the RA Governance in their Organisation and cannot delegate this. The RA Manager must ensure:

- that all RA procedures are carried out in accordance with local and national policy
- Facilitate the process for agreeing the organisation's access control positions.
- Appropriate auditing is carried out.
- Operational security of (old) paper based RA records.
- Users ID checked to GPG45 level 3 or 4.
- Users are compliant with the terms and conditions of Smartcard usage and that issues are raised appropriately locally and nationally.
- Responsible for training all other RA staff who will conduct ID checking to ensure that appropriate standards exist and they can evidence good ID checking.
- RA Agents are registered.

3.2 Registration Agents

Registration Agents are responsible to the RA Manager for ensuring that the National and local processes are followed. They are responsible for:

- The issue of Smartcards and checking staff credentials at a face to face meeting.
- Id checking to GPG45 Level 3 or 4-NHS Employers check standard and recording it on the Electronic Staff Record (ESR) or CIS. This provides assurance that the identity is valid across any organisation an individual works within. This also applies to core identity attribute changes (Name, Date of Birth or National Insurance Number). Grant external Users access, renew certificates if expired.
- Ensuring Users accept terms & conditions of Smartcard use when registering them.

All incidents, misuses, anomalies and problems will be reported to the RA Manager. Smartcards can only be issued to individuals who have a national verified digital identity.

3.3 HR/Registration Agent ID Checkers

HR/Registration ID checkers are responsible to the RA Manager for ensuring that the National and local processes are followed. They are responsible for Id checking to GPG45 level 3 or 4 /NHS Employers check standard and recording it on the Electronic Staff Record (ESR) at a face to face meeting. This also applies to core identity attribute changes (Name, Date of Birth or National Insurance Number). This provides assurance that the identity is valid across any organisation an individual works within. Smartcards can only be issued to individuals who have a national verified digital identity.

3.4 Local Smartcard Administrators (LSA)

Local Smartcard Administrators are responsible to the RA Manager for ensuring that National and local processes are followed. These administrators will normally be accessible Users within a work area. The list of these administrators will be published on the Trust Intranet. The LSA should ensure that they have sufficient staff to provide cover across all working patterns within a work area. For example if the service is 24 hours there should be an LSA available on all shifts. Staff can now unlock their own Smartcard and are given guidance on how to register for this process. Also available on the ELFT intranet.

4.0 Incident Reporting

Incidents should be reported, using the Trust's Incident Reporting Procedure (Datix), and 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 Digital Health applications
- Any unauthorised alteration of patient data on NHS Digital applications
- Any unauthorised access of other Smartcard enabled systems
- Lost/damaged Smartcards should be reported via the IT Service Desk Portal rather than raising a Datix

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

The RA manager will consider all reported incidents. Any incidents considered Significant, will be reported to the Information Governance Manager depending on the nature of the incident, may result in action being taken against an individual, in accordance with Trust policy.

Only the end user for whom the Smartcard is intended should know their passcode for their Smartcard, no-one else should, including RA staff. If anyone else knows the end Users passcode it breaches the Smartcard terms and conditions of use and the Computer Misuse Act 1990.

It is mandatory that Users sign the Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.

RA staff (RA Managers, Advanced RA Agents and RA Agents), are reminded that it is their responsibility to ensure that Users comply with these terms and conditions.

A major breach of security will also be reported by the RA manager to the LSP 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 RA Manager and Information Governance Manager will consider incidents reported to them and decide whether Trust systems or working practices should be reviewed as a result.
- documentation will be kept by the RA Manager and/or on the HR file as appropriate.

5.0 RA Manager Reporting

The RA Manager will report significant incidents to the Information Governance Manager in accordance with the Incident Reporting Policy.

5.2 RA Agent Reporting

Registration Agents will report any RA related incidents, using the Trust Incident Reporting Procedure and to the RA Manager. Additionally RA Agents will report any operational difficulties in using CIS/Spine compliant systems (especially where these have patient healthcare implications) to the RA Manager.

6.0 Monitoring

6.1 Audits

All RA functions will be regularly audited by the RA Manager and will be results will be reported to the Information Governance Steering Group (IGSG), including

- The issue of Smartcards
- The management of Smartcards
- The profiles associated with Users in relation to what they do
- The use of Smartcards
- The use of NHS Digital/Trust applications
- Identity management
- Security of supplies and equipment

6.2 Smartcards

Smartcards should be treated with care and protected to prevent loss or damage. All Users should adhere to the latest Terms and Conditions guidance given when the card was issued and any subsequent guidance. Spot checks should be carried out by the RA Manager on a regular basis to ensure Terms and Conditions are adhered to and reported to the IGSG.

6.3 Smartcard Misuse

Staff members are responsible for reporting suspected Smartcard misuse in line with Trust's Incident Reporting Policy. In serious cases the certificate associated with the

Smartcard may be suspended or revoked, and disciplinary action will be taken.

6.4 Revocation of Smartcards.

If the User is an East London NHS Foundation Trust (ELFT) employee and is moving to another NHS organisation, the Smartcard access is automatically revoked through the staff record. Non ELFT - External staff must have an end date put on their user profile when creating ELFT access. This will be a maximum of 1 year Agency Staff. A User moving to another NHS organisation should retain the Smartcard for use in the new organisation. If they leave the NHS permanently, the Smartcard Certificates will be revoked.

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

- The Smartcard has been lost or stolen
- There has been some other security breach associated with the Smartcard or Smartcard certificate.
- The card has become damaged

The RA Manager authorises the revocation of a card in consultation with the HR Manager, as appropriate.

Revocation renders the Smartcard useless, whereas deactivation removes all access to the system allowing the card to remain valid.

6.5 Locum, Agency, Honorary and Social Care Staff

- Temporary, Locum, Agency, Honorary and Social Care staff may have a legitimate need to gain access to NHS Digital Health 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 staff could already be registered and will only require a role profile added for use at ELFT.
- Line managers should be aware that temporary staff who are Smartcard holders may not have sufficient training in the use of the particular NHS Digital Application. All staff will be trained in an application before being allowed to access data.
- Locum and Agency staff need to complete a request on the IT Service Desk Portal to register for a Smartcard or access to a clinical system. Access will be assigned for 1 year and recorded by the RA team. Notification will be sent to the user, to inform them that their access will need updating.
- Honorary and Social Care staff will need an honorary contract set up with the placements team in HR. This will then generate a request for the RA team to print a Smartcard.

All applicants will need to provide all the correct identification documentation, regardless of the contract they have with the Trust eg: permanent or bank. The relevant senior manager for the Directorate will be responsible for authorising the necessary access.

All temporary staff including locum, agency, Social Care staff will be bound by this policy and other related Trust policies on security and confidentiality of information.

6.6 Contractors

The Trust will ensure all contractors who need to use the NHS Digital applications are bound by the General Data Protection Regulations and NHS Digital Confidentiality Code of Practice. This will include the process to be taken in cases of a breach and liability issues.

The Trust will ensure that all contractors sign a confidentiality agreement as part of their contractual arrangements.

7.0 Registration Authority Security and Maintenance

The RA Manager is responsible for ensuring that adequate numbers of Smartcards are available, and will maintain the Smartcards throughout their useful life. The Associate Director of ICT will ensure that there is sufficient computer equipment to support all Users of NHS Digital applications (including those for registration) containing the latest software. All RA equipment will be subject to policies and procedures governing the management and control of Trust Assets.

7.1 Registration Authority Mobile Equipment Security

Mobile RA equipment must be locked in a secure area at all times when not in use. Any incident relating to the loss or theft of RA equipment or documentation should be reported to the RA Manager immediately so that adequate security measures can be taken and the incident logged on Datix.

7.2 RA Forms

RA Forms will no longer be used for CIS Registration/assigning access, but any paper records/scanned copied must be kept in accordance with the national guidance – for 6 years or until the person's 70th birthday.

RA - online Forms

There will be a form on the IT Service Desk Portal for external staff to apply for a Smartcard or for access to be assigned to ELFT. The agency/locum worker will then be contacted by the Registration Authority to have an Identity check to GPG45 Level 3 or 4 and be issued a Smartcard. An end date (Maximum 1 year) for the access for external staff must always be entered on CIS. If an external user is leaving the Trust but is moving to another NHS organisation the card should be retained by the user.

Revoked access

The Smartcard access will automatically be revoked in the case of the following as access is controlled by the staff record:

- Staff suspension pending disciplinary investigations
- Maternity leave
- Long term sick leave
- Secondment

7.3 Smartcards

Name on Smartcards

The name registered on CIS is controlled by the name which is on the photographic evidence supplied ie: Passport/Driving Licence, but a preferred name can be printed on the Smartcard.

The Trust Name is not printed on Smartcards, as the cards are transferable between all NHS organisations.

Lost, Stolen and Broken Smartcards
Lost and damaged Smartcards should be reported to the RA/Smartcard Team via the IT Service Desk Portal as soon as is practicable.

In the case of theft the RA Manager must be informed so that checks may be made to ensure that the Smartcard has not been misused and the incident logged on Datix.

8.0 References

8.1 General Websites
https://digital.nhs.uk/Registration-Authorities-and-Smartcards

9.0 Associated Documentation

9.1 Related Policies and Processes
The Trust will ensure that processes supporting the identification, registration and management of staff will be integrated with other policies and processes within the Trust as appropriate.

9.2 Trust Policies

http://elftintranet/sites/common/private/search_quick21.aspx?q=information%20governance%20policy&orderby=0&url=ObjectInContext.Show(new%20ObjectInContextUrl(2%2C29769%2C1%2Cnull%2C970%2Cundefined%2Cundefined%2Cundefined%2Cundefined%2Cundefined))%3B

Appendix A

GLOSSARY
NHS Digital
Formerly known as Health and Social Care Information Centre

Local Service Provider (LSP)
Local Service Provider of Information Technology

National Care Records System (NCRS)
National IT System storing patient care records

Pass-code/PIN
The digit entered into the computer when logging onto the system. This allows the system to know that the person using the Smartcard is the person whose Smartcard

it is. *This should only be known by the User*

Registration Authority (RA)
The Registration Authority ensures that all aspects of Registration adhere to National Policies and Procedures. It is also responsible for ensuring tight control over the issue of Smartcards and the security of information

RA Agent
RA Agents are responsible for checking candidates' credentials and issuing Smartcards

RA Agent ID Checker only
RA/HR are responsible for checking candidates' credentials and recording on the Electronic Staff Record (ESR)

Position Based Access Control (PBAC)
Positions are created then assigned through the staff record for ELFT staff and by the RA Agent/Manager for non ELFT staff ie: Agency/Locum. The position denotes which access/system is available to the User

Smartcards
The cards used to gain access to the relevant systems with an electronic chip. These have the Users' name and photograph printed on them, but not the name of an Organisation, as they can be transferred from Trust to Trust

Care Identity Service
Where information is held on all Users nationwide

User
Staff members who have Smartcards and use the associated systems

Unique User ID Number (UUID Number)
The Unique User Identifying number assigned to each User

Workgroup
Set up for groups of people to work in different areas of patient care to view records as long as they have a legitimate relationship to do so

Appendix B

Contact Details
Registration Authority (Smartcard) Team via The IT Service Desk Portal or Telephone: 0207 655 4004

Address: The Green
1 Roger Dowley Court,
Russia Lane,
London. E2 9NJ