London Ambulance Service NHS
NHS Trust

Registration Authority Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: Policy for managing the Trust Registration Authority and smartcard management for access to Connecting for Health applications and services.

.

Sponsor Department: IM&T Information Security

Author/Reviewer: Registration Authority Manager. To be reviewed by December 2015.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
28/06/2013	2.2	IG Manager	Document Profile & Control update
26/02/2013	2.1	Information Security Manager	Changes of the Introduction as requested by ADG
11/12/2012	1.14	IS Manager	Additional changes
24/10/2012	1.13	IG Manager	Further changes and formatting
12/10/2012	1.12	Information Security Manager	Shortening and simplifying text as required by ADG
21/03/2012	1.11	IG Manager	Document Profile & Control update
27/02/2012	1.10	Information Security Manager	Final amendments
25/02/2012	1.9	Information Security Officer	Minor changes
15/12/2012	1.8	Information Security Officer	Inclusion of Terms and Conditions requirements in Sections 5.1.6 & 5.2.7
08/12/2011	1.7	Information Security Officer	Minor amendments to initial draft text.
23/11/2011	1.6	Information Security Officer	Minor amendments to initial draft text.
15/11/2011	1.5	Information Security Officer	Initial draft for consideration.
19/02/09	1.4	Records Manager	Minor Reformatted
10/12/2008	1.3	Head of Records Management	Minor amendments to text & appendix
24/10/2008	1.2	Information Security Manager	Addition of responsibilities, order changed and RA05 added into leavers/changes procedure .
29/08/2008	1.1	Head of Records Management	Minor changes following IGG mtg
15/08/2008	0.5	Information Security Manager	Merging of repeated information.
11/07/2008	0.4	Information Security Manager	Cosmetic changes, Lost smartcard procedure updated.
17/06/2008	0.3	Information Security Officer	Rollup changes, addition of Service Desk and security requirements.
01/04/2008	0.2	Information Security Officer	Draft Changes.
28/03/2008	0.1	Information Security Officer	Initial draft for consideration.

For Approval By:	Date Approved	Version
ADG	19/12/12	2.0
IGG	29/08/08	1.0
Ratified by (if appropriate):		
RCAG	21/10/08	1.1

Published on:	Date	By	Dept
The Pulse	28/06/13	Web Communications Officer	Comms
LAS Website	28/06/13	Web Communications Officer	Comms
The Pulse	20/02/09 (v.1)	Records Manager	GDU
LAS Website	10/03/10 (v.1)	Records Manager	GDU

Equality Analysis completed on	By
22/02/2012	IM&T team
Staffside reviewed on	By

Links to Related documents or references providing additional information		
Ref. No.	Title	Version
6244	Registration Authorities Governance Arrangements for NHS Organisations	6th April 2006
NPFIT-SI-SIGOV-0114.01	Registration Authorities Operational Process Guidance	3.1
1656	Confidentiality - NHS Code of Practice	November 2003
4713	NHS Care Record Guarantee	5.0
EGUI07901	NHS Employers Verification of Identity Checks	July 2010
NPFIT-FNT-TO-IG-0007.38	National RBAC Database	26b
ISBN: 0 7115 0468 7	e-Government Interoperability Framework	6.1
TP/006	Serious Untoward Incidents Policy	2.0
	Data Protection Act, 1998	
	Freedom of Information Act, 2000	
	Computer Misuse Act, 1990	

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1. Introduction

The LAS Registration Authority (RA) is the authority responsible for ensuring that 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.

In order to provide Healthcare Professionals with appropriate and secure access to NHS Connecting for Health applications, electronic Smartcards are issued to individuals based upon the NHS professional's organisational, role/s, and business function (Activity). To maintain the security of who may access Connecting for Health applications, Smartcards are issued using a formal registration process. Each Trust is required to run a local Registration Authority function, which conform to the National Registration Policy.

The LAS local RA consists of the RA manager, RA agents, and Sponsors within the local Information Governance structure.

The LAS RA utilises **User Identity Manager (UIM)** software to manage access control to NHS Care Records Service (CRS) and facilitate an interface to the Electronic Staff Record (ESR). UIM uses electronic forms and digital signatures to ensure that NHS patient medical information is kept secure and confidential in line with the "NHS Confidentiality Code of Practice" and the "NHS Care Record Guarantee".

London Ambulance Service (LAS) has implemented the ESR-UIM Interface and introduced processes/procedures that covers both directly and externally employed staff, in the following areas:

- New Starters
- Managing change
- Leavers

This document is the Registration Authority Policy for the London Ambulance Service. It is relevant to both RA and ESR users to ensure that the Trust's Registration Authority operates in accordance with Connecting for Health regulatory requirements.

2. Scope

This Policy covers the registration process requirements for access to NHS CRS systems containing person identifiable information. It is applicable to all This Policy applies to all members of staff working in or on behalf of the LAS (this includes contractors, temporary staff, and all permanent employees).

3. Objectives

To mandate requirements that ensure only authorised personnel have access to NHS CRS systems containing person identifiable information.

To ensure appropriate staff are aware of their responsibilities and follow the correct procedures.

4. Responsibilities

LAS Trust Board

The LAS Trust Board defines the Trust's policy in respect of Information Security, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the Registration Authority.

Senior Information Risk Owner (SIRO)

The SIRO is accountable to the Trust Board for Information Security and is assigned overall responsibility for the organisation's RA.

Information Governance Group (IGG)

Chaired by the SIRO this Group will monitor the implementation of this policy and review performance reports on the RA function. The IGG reports through to the Trust Board through the Risk Compliance and Audit Group (RCAG) and has the responsibility to ensure that this policy is monitored and adhered to.

The IGG is responsible for approving the nomination of Sponsors and the assignment of Role Based Access Control (RBAC) positions.

Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and this Policy supports the Caldicott function.

Information Security Manager

Responsible for maintaining and reviewing information processing systems against information security controls and maintaining Information Security Management System (ISMS) pertaining to technical policies, standards and guidelines.

The Information Security Manager acts as the RA Manager and has the following responsibilities for the Trust:

- Assign, sponsor, and register an appropriate number of RA agents;
- Ensure there are sufficient resources to operate the registration processes in a timely and efficient manner;
- Ensure that the National Registration policy and processes are adhered to and that any local policies and processes support the National policy and processes;
- Maintain separation of duties;
- Implement an Audit policy;
- Report all RA related security incidents and breaches to the IGG;
- Ensure there is a sufficient supply of Smartcards and RA hardware.

Line Managers

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

RA Agents

Registration Authority Agents are appointed by the RA Manager Assign, and are responsible for ensuring that the National and local processes are followed and for the accurate input of information.

Registration Agents will:

- Ensure that all incidents, misuses, anomalies and problems will be reported to the RA Manager;
- Adhere to this document and "Registration Authorities: Governance Arrangements for NHS Organisations";
- Ensure users have only one NHS CRS Smartcard issued to them and that users are aware of their responsibilities relating to Information Governance and Smartcard use;
- Adhere to the Information Governance Toolkit requirements and ensure that all RA forms and associated information is maintained and securely stored according to national policy;
- Maintain their contact details, including email address and telephone numbers, in the Spine User Directory.

RA Sponsors

Sponsors are appointed and entrusted to act on behalf of the Senior Management Team in determining who should have what access and maintaining the appropriateness of that access.

They must be familiar with the different types of access profiles, as designated by the IGG and carry out two specific responsibilities:-

- Identify the type of access to information a user needs via an NPfIT application – the organisation they belong to and their Role Profile;
- Attend a face to face meeting to vouch for the identity of a user who they know to have worked for two or more continuous years in the Trust.

All staff and third parties

All staff and contractors, whether they are users or administrators of the RA function, are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5. Glossary

ACP - Access Control Position	A method used to assign access rights based on job role.
Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
CMS	Card Management System
ESR	Electronic Staff Record
IGG	Information Governance Group
IIM	Integrated Identity Management
NHS CRS	NHS Care Records Service
PBAC	Position Based Access Control
RA	Registration Authority
RBAC - Role Based Access Control	An access policy determined by the system, not the owner.
RCAG	Risk Compliance and Assurance Group
UIM	User Identity Management
UUID	Users Unique Identifier

6. Registration Authority Function

6.1 The RA function within the LAS is shared between the Human Resources and IM&T Security Team, who are jointly responsible for managing the distribution and use of smartcards.

6.2 The LAS RA is responsible for providing a secure, accountable and authoritative service in line with National Registration Processes.

6.3 The LAS RA is made up of the following personnel:

- Registration Authority Manager
- Registration Sponsors
- Registration Agents

6.4 The RA conducts the following duties:

- User registration
- Role profile maintenance
- Adding role profiles
- Changing role profiles
- Revocation and cancellation of smartcards
- User suspension
- Passcode resetting
- Changes to shared secrets
- Smartcard renewal and exchange

7 Governance

7.1 The RA is responsible for ensuring that all aspects of registration services and operations are performed in accordance with National Policies and Procedures. It is responsible for providing arrangements that will ensure tight control of the issues and maintenance of smartcards, whilst providing an efficient and responsive service that meets the needs of users.

7.2 The management and use of smartcards will be subject to audit to ensure that national and local policies are being followed. Specifically the audit will confirm that:

- Smartcards are handled securely by users;
- RA documents and smartcards are used and stored appropriately;
- Access to CfH applications and records are controlled appropriately;
- Unused Smartcards are stored safely and appropriate records kept;
- Role Based Access Control (RBAC) role allocation and de-allocation is performed appropriately;
- Random checking of RBAC roles with those requested by the Sponsor.

7.3 Applicants signing the application form are signing an agreement and acceptance to Terms and Conditions regarding the correct use of the card. In particular they agree not to permit anyone else to use their card.

7.4 Lost or stolen cards must be reported promptly to the RA Team and action taken to ensure that their use is revoked.

7.5 Breaches of the agreed terms and conditions of Smartcard use will result in the revocation/confiscation of the card by the RA Manager and a report to the Caldicott Guardian.

7.6 Staff should report incidents to the RA Team and in line with the Trust's Serious Incident Policy and Procedure. Examples of incidents are:

- Smartcard or application misuse
- Smartcard theft/loss
- Non compliance of local or national RA policy
- Any unauthorised access of NPfIT applications
- Any unauthorised alteration of patient data

7.7 The RA manager will consider all incidents reported; any incidents considered significant will be escalated to the Information Governance Group (IGG) and the Caldicott Guardian depending on the nature of the incident. Upon the agreement of the IGG, any major breach of security will be reported to the National RA.

8 Hardware and Software requirements for Registration Authority

8.1 To ensure that the LAS RA is able to function efficiently RA staff will have access to the appropriate hardware and software necessary for the administration of the RA and allowing access to appropriate Spine applications.

8.2 For the management of the RA and access to the relevant spine applications, the RA Manager and each RA Agent will be provided with the following equipment:

- PC or laptop with 3 or more USB ports or USB hub;
- N3 network connection;
- Two Smartcard readers;

The issuer of Smartcards will additionally require access to:

- Supply of blank Smartcards;
- Smartcard printer;
- Digital camera / web cam;
- At least one spare ink cartridge.

8.3 The RA Manager and Agents must ensure that all equipment is securely stored. In particular the Smartcard printer and blank smartcards must be stored in a secure location at all times, in a location that can only be accessed by authorised staff.

8.4 Users that require access to Spine applications will be provided with the following equipment:

- PC or laptop;
- N3 network connection
- 1 Smartcard reader

8.5 The RA Manager will ensure that adequate numbers of Smartcards are available and for maintaining the Smartcards throughout their useful life.

8.6 Line managers will ensure there is sufficient computer equipment to support all users of national applications (including those for registration). All RA equipment

will be subject to policies and procedures governing the management and control of LAS Information assets.

IMPLEMENTATION PLAN	
Intended Audience	This document is applicable to the RA function staff and those that hold a Smartcard
Dissemination	The Policy will be published on the Pulse
Communications	During the next routine announcement of policy updates this policy will be included, it does not require an individual announcement
Training	No training is required, all RA staff are familiar with their roles

Monitoring:

Aspect to be monitored	**Frequency of monitoring AND Tool used**	**Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported**	**Committee/ group responsible for monitoring outcomes/ recommendations**	**How learning will take place**
The issuance of Smartcards is to be subject to audit. The held stock of consumables for issuing Smartcards is to be checked	Yearly Every 6 months	The Information Security manager will report results to the Information Governance Group	RCAG.	Dissemination of findings and action to be taken where change to practice is required

Appendix 1

Information Governance Toolkit Compliance Statement

The LAS are required to provide an appropriate level of information governance based upon the requirements of the Information Governance Toolkit (IGT). This Policy supports the following requirements of the Information Governance Toolkit v9:

Requirement 9- 303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority
Requirement 9-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use