

Registration Authority Policy on Smartcard Management

Version:	2
Approved by:	PASC
Date ratified:	28.7.15
Lead manager	Informatics Manager
Responsible director	Deputy Chief Executive
Date issued:	Jul 15
Review date:	Jun 18

Registration Authority Policy on Smartcard Management

1 INTRODUCTION

Registration authority permits the Trust to use Smartcards to access the 'Spine', which allow authorised NHS staff access to patient information (demographics) held electronically in a central NHS database. All organisations that run a Registration Authority do so through delegated authority from HSCIC.

2 PURPOSE

The Purpose of this policy is to set out the way in which the Trust will implement and maintain a Registration Authority (RA) for the Trust by:

- Defining the reasons, scope and purpose of the RA function
- Setting out processes involved
- Indicating responsibilities of those involved
- Setting out requirements and responsibilities for staff issuing and authorised to use smartcards to access Spine Compliant Applications.

3 SCOPE

This Policy applies to all processes, procedures and activities carried out for the purpose of RA staff and by staff members who are authorised through the RA process to access Spine Compliant Applications.

4 DEFINITIONS

Term	Acronym	Definition
The Health and Social Care Information Centre	HSCIC	The Health and Social Care Information Centre (HSCIC) is a single Registration Authority, all organisations that run a local Registration Authority do so on a delegated authority basis from HSCIC.
Registration Authority	RA	Any entity that is appointed by the Executive of a legal NHS organisation as being responsible for the identification and authentication of applicants

RA Manager	RAM	Manages the RA service provision and operation to meet the needs of an organisation and all its users. Additionally the RA Manager is responsible for briefing and registering RA agents. Also responsible to the National RA Managers Board.
RA Agents	RAAS	RAAs administers the RA function under the direction of the RA manager, responsible for performing registration and maintenance of sponsors and healthcare professionals in the organisation Ensures that the national and local RA processes are followed
Registration authority Group	RAG	The RAG will be responsible for overseeing all aspects of RA implementation and operation to ensure compliance with necessary guidelines and statutes.
Sponsors	Sponsors	Sponsors are line managers who have been identified by the Trust Executive. They have been appointed to designate and approve access to information and functionality of Spine Compliant Applications systems via the selection of the appropriate RBAC codes.
Users	Users	Individuals who will access HSCIC applications according to assigned roles.
Smartcard	Smartcard	The card issued to an authorised user which enables access to HSCIC systems
Pass-code	Pass-code	Alpha-numeric password, set-up by and private to individual users. Pass-codes should never be shared with other Users
Unique User Identification	UUID	Unique id identifying a user of Spine Compliant Applications. This Id is created when the user is registered on the CIS.
Spine Compliant	Spine Compliant	Means that an application has been approved as meeting the necessary standards for integration with the national spine application
Care Identity Service	CIS	Repository which stores users' profiles and registration information both current and historic. Smart cards are managed by this CIS.
Role Based Access Control	RBAC	The means by which NHS staff are identified by their job functions. This in turn dictates the type of access that they are granted to Spine Compliant Applications.

5 DUTIES AND RESPONSIBILITIES

5.1 Chief Executive

The Chief Executive has overall responsibility for the implementation and running of the Trusts' Registration Authority. Responsibility for

ensuring compliance with this policy is delegated to the Director of IM&T.

5.2 Senior Information Risk Officer (SIRO)

The SIRO is responsible for:

- ensuring that the work of the RA is appropriately overseen;
- ensuring effective governance is in place so assigned role profiles are appropriate and not overly restrictive or permissive.

5.4 Registration Authority Manger

The Trust's Registration Authority Manager(s) (RAM) is responsible for ensuring that RA processes are implemented and maintained in accordance with local policy and procedures, and that those policies and procedures meet the standards set in national guidance. This role will be fulfilled by the Head of Informatics; notice of RAM appointment or termination of which must be communicated to the Regional RA Manager.

The Trust has appointed a second RAM in the Informatics Department.

- ensuring that RA Agents (RAA) are assigned, sponsored and registered (where permitted under the governance arrangements);
- ensuring that all RAA are adequately trained and are familiar with the RA policies and processes;
- ensuring that all Sponsors are trained in their responsibilities including where appropriate, how to unlock Smartcards and issue Fallback Smartcards;
- ensuring that users only have one spine compliant application active Smartcard associated with them: users are not permitted to have more than one Smartcard;
- assisting Sponsors in their understanding of the Role Based Access Control (RBAC) with alignment to staff roles;
- Ensuring that there is a secure (locked) area for the storage of all registration and associated information
- Ensuring good working condition and availability of RA hardware and consumables.
- Facilitation of the process for setting the Trust's access control levels
- Responsibility for ensuring that appropriate auditing is carried out
- 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 (the creation of these processes may be delegated).

5.5 Registration Authority Agents

Registration Authority Agents (RAAs), are nominated by the RA Manager and are responsible for:

- being compliant with all RA policies, procedures and documentation in use by the Trust;
- checking and recording personal identification, confirmation of address documentation on employment application forms and verifying users' identities to e-GIF level 3 and NHS Employer standards;
- registering users onto the CIS and, when required, issuing them with a Smartcard (must include UUID and user's photograph);
- checking registration requests are from Trust authorised Sponsors;
- ensuring appropriate sponsorship is applied e.g. an admin manager has not sponsored a Consultant or that clinical activities have not been requested for Admin staff;
- complying with the fallback, replacement and revoked smartcard processes;
- undertaking the task of unlocking and resetting of Smartcard PINs, ensuring security is paramount at all times;
- Ensuring leavers from an organisation have their access rights removed in a timely way;
- ensuring all forms and related paperwork are processed and stored securely in line with Trust policy/procedures on record retention, security and confidentiality.

5.6 Registration Authority Sponsors

Sponsors are nominated by the RA Manager

Sponsors will typically be Locality Managers and / or Team Managers with line management responsibilities for Spine Compliant Applications Registered by the RA Manager.

Sponsors are responsible for:

- Raising requests for new users to access Spine Compliant Applications;
- Assisting the RAAs in determining who should have what access and maintaining the appropriateness of that access;
- assisting the RAAs in making sure that Smartcard users are given the minimum appropriate level of access needed to perform their

- job;
- the accuracy of the information on the RA forms;
- user registrations within the area of their responsibility and within their own organisation unless there is a formal, documented inter-organisational agreement in place;
- undertaking appropriate level of training prior to carrying out their Sponsor role;
- ensuring they understand the RBAC Database and any application based material published on HSCIC website; and the implications of granting the job roles and activities defined within;
- accessing and familiarising themselves with the briefing material provided by the application providers relating to the applications which users need to access;
- NOT verifying users ID;

5.7 Recruitment Manager

The manager is responsible for:

- Assisting with the integration of relevant RA and HR policies and procedures
- helping determine the approach to registration of all end users including registration of locums and temporary staff.
- Ensuring all relevant starters, leavers and changes are notified to RA staff so that they can:
 - update on the CIS
 - create new accounts for new starts
 - change/remove accounts when roles/responsibilities change
 - terminate access for Trust leavers

5.8 Information Communication Technology Manager

The ICT Manager is responsible for:

- ensuring all desktops/ laptops and other relevant devices have all necessary software and configuration to allow access the two relevant HSCIC systems for authorised staff.
- liaison with the RAMs, ensure all necessary software for smartcard and spine application applications is installed an up to date.
- taking the lead to ensure all technical guidance documentation is accurate, appropriate and up to date.

7 REGISTRATION AUTHORITY PRINCIPLES

7.1 Principles

The following principles apply:

- The Trust must ensure compliance with all RA requirements of RA.
- The RA is a vital element of information governance for the Trust in its responsibility to maintain confidentiality of service user personal data.
- Only staff registered via RA will have access to Spine Applications.
- The Trust will base its policy on National RA policy requirements.

8 SECURITY (Admin, Data Protection & records)

The RA Manager is responsible for all administrative processes and ensuring compliance with the HSCIC policies and associated requirements.

<http://systems.hscic.gov.uk/rasmartcards>

All information relating to the verification of identity is to be treated as strictly confidential and used only for the purposes of registration procedures. All new users to the Trust must complete new CIS Create New user form, even if they have previously registered in a previous organisation, to gain registration with this Trust: Forms can be found below:

<http://systems.hscic.gov.uk/rasmartcards/cis/forms/cisforms>

Possible future uses could arise should the Trust move to integrate the RA and recruitment processes. Should this be so, all information related to identity should again be treated as confidential and only used for these prescribed purposes.

Records and documentation required for evidence and used for authentication must be retained in accordance with the Trust's Records Retention Schedule. The following guidance is also applicable to the retention of identification information for NHS level 3 authentications:

- Where practical, file copies of the supporting evidence should be retained. Alternatively, the reference numbers and other relevant details of the identification evidence obtained should be recorded to enable the documents to be obtained again.
- Document storage should be in a locked and secure place at all

times and may be audited Access to stored documents is strictly limited to appropriately authorised staff whose role includes requires it.

Any misuse of information or breach of security by staff whilst using Spine Compliant Applications will be dealt with under the relevant Disciplinary Procedure. Staff must acknowledged that it is a criminal offence to pass this information to anyone who is not entitled to receive it and breaches of confidentiality could result in prosecution.

9 IMPLEMENTATION OF POLICY AND TRAINING REQUIREMENTS

This implementation of this policy and associated procedures will be the responsibility of the Trust RA Manager in liaison with the Human Resources and ICT departments.

All staff requiring a smartcard will receive specific training prior to any card being issued with more general awareness training via the Trust Inset Training days and Corporate/Clinical Induction.

10 MONITORING COMPLIANCE

The effectiveness of the policy will be monitored by the Trust RA lead, and who will report to the IG work stream of the Clinical Quality, Safety, and Governance Committee.

Areas of actual and/or perceived risk will be identified and managed through the Trusts risk management procedures.

The Trusts' compliance will be subject to periodic internal and external review via audit, with finding and action plan monitored by the Trust Management Team and Board.

The RA Policy and procedures are subject to audit by internal and external auditors. Audits would typically cover:

- 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 Spine Compliant Applications
- identity management
- security of supplies and equipment

15 REFERENCES

Information Governance Policy
Incident Reporting Procedure

Appendix A -EQIA

1. Does this Procedure, function or service development affect patients, staff and/or the public?

NO

2. Is there reason to believe that the Procedure, function or service development could have an adverse impact on a particular group or groups?

NO

*3. If you answered **YES in section 2**, how have you reached that conclusion? (Please refer to the information you collected e.g., relevant research and reports, local monitoring data, results of consultations exercises, demographic data, professional knowledge and experience)*

4. Based on the initial screening process, now rate the level of impact on equality groups of the Procedure, function or service development:

Negative / Adverse impact:

Low.....

(i.e. minimal risk of having, or does not have negative impact on equality)

Positive impact:

Low.....

(i.e. not likely to promote, or does not promote, equality of opportunity)

Date completed ... 06/July/2015.....

Name ... Muhammad Akram

Job Title ...Head of Informatics.....