City Hospitals Sunderland NHS
NHS Foundation Trust

REGISTRATION AUTHORITY (SMARTCARD) POLICY

Document Reference	HR30.RA.V1.2
Document status	Final
Target Audience	All staff
Date Ratified	17 December 2015
Ratified By	Policy Committee
Release Date	29 December 2015
Review Date	December 2018
Sponsor	Kath Griffin, Director of Human Resources

Version	Date of Amendments	Author	Update comments
1.0	December 2015	Lindsey Smith Registration Authority Manager / Workforce Information Analyst	
1.1	December 2015	Lindsey Smith Registration Authority Manager / Workforce Information Analyst	Final amendments following presentation to Policy Committee
1.2	February 2016	Lindsey Smith Registration Authority Manager / Workforce Information Analyst	Minor amendments made to page 9 – section 5.3

CITY HOSPITALS SUNDERLAND NHS FOUNDATION TRUST

DOCUMENT APPROVAL PROFORMA

Policy Title: Registration Authority Policy **Policy Number: HR30.RA.V1.1** **Name of Author: Lindsey Smith, Workforce Information Analyst** **Name of Sponsor:** Kath Griffin, Director of Human Resources	
New Policy:	**Yes**
Reviewed Without Amendments:	**NA**
Type of Policy:	**Risk management** ☐ **Operational policy** **Operational guidelines** ☐ **Mental Health Act** **Human Resource** **X** **Control of infection** ☐ **Drugs policy** ☐ **Other** ☐
Equality Impact Assessment: If this policy has a potential discriminatory impact please record below the person who has informed and involved the sponsor: **Name:** **Title:** **Date:** **NB: It is the sponsor's responsibility to submit the policy through the CHS approval route.**	
Checklist for the review and approval of the policy	

	Is the policy compliant with:	Yes/No	Comments
	Corporate style	**Yes**	

	Format including duties,	**Yes**	
	Content; intended outcomes clearly described	**Yes**	
	Evidence base; key references included and cited in full	**Yes**	
	Associated documentation recorded	**Yes**	
	Review/consultation process: List of groups/committees included with the policy	**Yes**	
	Appropriate stakeholders consulted	**Yes**	
	Approval: Staff side committee (if appropriate)		
	Dissemination & implementation: appropriately described	**Yes**	
	Training: requirements included (where appropriate)	**Yes**	
	Document control: table updated appropriately	**Yes**	
	Monitoring compliance/ effectiveness: adequate description and appropriate monitoring	**Yes**	
	Review date: identified and acceptable	**Yes**	
	Page numbers: correct with index	**Yes**	
	Intranet to be updated: Record the date and person responsible	**Yes**	**Deputy Head of Corporate Affairs, 29 12 15**
	Individual approval; Policy author	**Date**	**Sign**
	Director of Corporate Affairs: update version control and approval of the process	**Date**	**Sign** **29 12 15**
	Policy archived		**Not applicable – new policy**

Committee Ratification

Committee for ratification: Policy Committee

Date of approval: 17 December 2015

Chair of Committee: Mike Davison

CONTENTS

1 INTRODUCTION

NHS systems and related services like the NHS e-referral service and the Electronic Prescription Service use a common approach to protect the security and confidentiality of every patient's personal and healthcare details. The NHS Electronic Staff Record (ESR) system also uses this common approach to protect the security and confidentiality of staff employment records. This approach includes a rigorous identity check of all those who may have access to such records, and careful control of what access any individual should have.

A national system called Care Identity Services (CIS) has been established for registering end-users. This system issues users with a Smartcard, which, is used to access the systems, which fall under the National Programme for Information Technology (NPfIT). NPfIT was introduced to achieve a national approach to electronic patient records. Staff will be issued with a Smartcard based on their position, which, is known as PBAC (Position Based Access Control).

The Registration Authority (RA) is the governance framework within which NHS organisations can register individuals as users of the Care Identity Service (CIS) and other IT services ensuring maintenance of confidentiality and security of patient and staff information. Access to these computer applications will be strictly controlled in order to maintain confidentiality of the data contained within.

Public Key Infrastructure (PKI) requirements clearly state that there is only one RA, which is the HSCIC (Health & Social Care Information Centre). Therefore, all RA activity below HSCIC level is delegated authority basis meaning NHS organisations will require a local RA.

The role of local RA is to ensure that individuals providing healthcare services to the NHS directly or indirectly have timely access to NHS Care Record Services applications in accordance with their healthcare role. City Hospitals Sunderland NHS Foundation Trust, (the Trust), has a responsibility to ensure that all the requirements of Registration Authorities are met and maintained. Therefore the Trust will use its own RA to manage registrations and manage the issuing of Smartcards.

The RA must comply with *Registration Authorities: Governance Arrangements for NHS Organisations* - **http://systems.hscic.gov.uk/raSmartcards/documents/ragovgateway.pdf**

2 PURPOSE & SCOPE

The Trust is obliged to have a RA to manage and maintain the distribution and use of Smartcards and implement a suitably stringent access control model. The Trust will comply fully with the latest national policies and procedures (see Section 9).

This policy describes the procedures for the operation of the RA within the Trust and details the following:

- RA operating procedures within the Trust
- Roles and responsibilities of all staff involved in the RA process
- How the Trust will adhere to national requirements for verifying identity
- How governance of RA activity will be run in the organisation
- Outlines what action will be taken if Smartcards are misused

3 DUTIES

3.1 Board of Directors

The Board of Directors is responsible for monitoring and approving a framework to support robust information governance and RA arrangements that are compliant with all relevant legislation, guidelines and NHS best practice standards.

3.2 Chief Executive

The Chief Executive has ultimate responsibility for ensuring that RA arrangements are in place and are compliant with all relevant legislation, guidelines and NHS best practice standards.

3.3 Senior Information Risk Owner (SIRO)

The SIRO has responsibility for providing focus for assessment and management information risk at Board level.

3.4 Director of Information Technology and Information Governance

The Director of Information Technology and Information Governance has responsibility for information governance within the Trust

3.5 The Director of Human Resources

The Director of Human Resources is the nominated Director lead for the management of this policy and is directly responsible to the Chief Executive for facilitating its implementation following consultation with the staff side representatives

3.6 RA Manager

The RA Manager is responsible for:

- Running the RA Framework in the organisation.
- Development of local processes that meet national policy and guidance and approval of any changes to them.
- Implementation of the RA policy locally and therefore must be aware of national requirements and obligations, ensuring the Trust policy adheres to them
- Assigning, sponsoring and registering RA Agents and Sponsors
- Training RA Agents and Sponsors ensuring they are competent to carry out their roles and that they comply with all policies and processes
- Facilitating the process for agreeing the Trust's access control positions
- Auditing the RA processes
- Ensuring users are compliant with the terms and conditions of Smartcard usage
- Ensuring the organisation's RA processes verify the identification (ID) of users to Electronic Government Interoperability Framework (e-GIF) level 3 when they are registered
- The security of old paper based RA records
- Ensuring that all service issues are raised appropriately, locally and nationally
- Ensuring national confidence can be maintained in delegated RA operations

3.7 RA Sponsor

The RA Sponsor within the Trust is responsible for:

- Approving access to individuals and raising requests for new users.
- Approving user's access rights via access control positions.
- Directly assigning users under position management.
- Unlock Smartcards and renewing Smartcard certificates.

The Sponsor does not verify a user's ID.

3.8 RA Agent Advanced Role

The RA Agent Advanced role, carries out all the RA Manager activities except those related to governance requirements that cannot be delegated. They also carry out all of the RA Agent activities.

3.9 RA Agent

RA Agents are responsible for:

- Checking ID on an operational basis.
- Granting users access assignment.
- Renewing Smartcard certificates for users if self-service functionality is not being used.
- Ensuring users at the time of registration or when assigned a role in Trust, comply with the terms and conditions of Smartcard usage.
- Adhering to 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, certificate renewal and card unlocking

3.10 Local Smartcard Administrators

Local Smartcard Administrators are responsible for**:**

- Unlocking Smartcards
- Renewing Smartcard certificates

The RA Manager will assess whether other departments need to have a role of Local Smartcard Administrator added to a role within their department, to help deal with routine RA queries.

Appendix 1 gives a breakdown of staff in the roles within the Trust's Registration Authority.

3.11 Employees

All employees who are Smartcard users must adhere to the content of this policy. This includes the regulations set out in the National Terms and Conditions document which can be viewed at **Appendix 2.**

3.12 Managers

All Managers are responsible for ensuring any incidents of Smartcard misuse are reported via the incident reporting system and a full investigation carried out.

4 DEFINITIONS

Care Identity Service (CIS) is the system used to control access to NHS systems and issuing of Smartcards to end-users.

Spine is part of the NHS Care Records Service, which is creating an electronic care record for all England's patients. It is a national, central database where summary patient records automatically upload information to the summary patient record.

Electronic Government Interoperability Framework (e-GIF) level 3 is the national standard for identity verification and defines the appropriate personal identification documentation which must be produced to verify a person's identity.

Electronic Staff Record (ESR) interface is the link between ESR and CIS developed to ensure consistency of data between the two related systems.

Health and Social Care Information Centre (HSCIC) is the organisation responsible for maintaining and developing the NHS national IT infrastructure.

Information Governance Toolkit (IGT) is a performance tool produced by the **Department of Health (DH)**. It draws together the legal rules and central guidance set out above and presents them in one place as a set of information governance requirements.

National Programme for IT (NPfIT) is being delivered by the **Health and Social Care Information Centre (HSCIC)** and aims to bring modern computer systems into the NHS to improve patient care and services.

Registration Authority (RA) is the governance framework within which NHS organisations can register individuals as users of the Care Identity Service (CIS) and other IT services ensuring maintenance of confidentiality and security of patient and staff information.

Role Based Access Control (RBAC) is the access framework that involves creating an access profile per user.

Position Based Access Control (PBAC) is the ability to assign access rights per post within the Trust and is the mechanism of choice for the Trust.

5 RA OPERATING PROCEDURES

5.1 The Operating System

The production of Smartcards is carried out on a system called Care Identity Services (CIS). This system was introduced in February 2015 and is designed to streamline working practices by simplifying processes. The system also reinforces governance requirements where appropriate so it is important that all RA staff are clear on any changes to policy.

5.2 Position Based Access Control (PBAC)

PBAC assigns access rights to posts within the Trust. Strict control of access to patient care records is fundamental to the operation of the NHS Care Records Service (NHS CRS) as well as the Trust's stated vision and values.

PBAC provides a simple and effective mechanism for providing users with the access they need in the course of their duties, whilst ensuring access rights are properly managed and appropriate for the position. PBAC grants rights according to the 'access control position' to which their job is assigned within ESR. When rights attached to each 'access control position' have been approved, along with the jobs in these different positions, the process of granting access rights for staff becomes much simpler.

5.3 Registration of new Trust Employees

The Trust is fully operational with Integrated Identity Management (IIM)) processes. This is the integration of the business processes between HR and the RA to eliminate duplicate processes, speed up the registration process, and improve information security and information governance. The two main benefits are:

- Elimination of duplicate processes: ID details inputted into ESR are recognised by CIS and therefore allow the registration to progress without the need of a supplementary ID check.

- Automatic closure of spine access; when an individual's employment is ended in ESR this automatically revokes the spine access for the organisation.

The Trust is required to meet the NHS Employment Check Standards for all staff, volunteers, contractors etc. providing NHS services. Responsibility for these checks sits with the HR Department.

ID checks adhere to National e-GIF Level 3 standards and must be recorded on ESR by an RA Agent. Once completed the RA Agent will register the individual through CIS and issue a Smartcard.

Trust employees who require access to spine-enabled applications will be given 2 cards on their first day of employment:

- NHS Smartcard – for access to relevant local and national Spine enabled IT applications
- A Trust ID card – displaying the name, job role and department of the employee and also containing access for the proximity door system.

5.4 Issuing an NHS Smartcard for a registered user

It is recommended that this process be carried out direct through the CIS system. The RA Agent will access the individual's record to issue the Smartcard (applies to individuals who may have joined the trust from another NHS Trust).

5.5 Renewing Smartcard Certificates

RA managers, RA agents, and sponsors can renew users' certificates. Certificates should only be renewed if they are within three months of expiry or there is the belief that they may have

been compromised (i.e. transactions have been found that may not have been performed by the user and the Smartcard has been entirely in the care of the user).

Certificates can only be renewed in the presence of the user, as they will need to reset their Smartcard PIN. The RA manager, RA agent, or sponsor will need to verify the user's identity by comparing the photograph on the Smartcard with the user. Sponsors can only renew certificates for users. RA agents can renew certificates for all users except RA managers. RA managers can renew certificates for all users. Any user requiring this service must contact the Employment Services Team within HR.

Users can renew their certificates (provided they have not yet expired) via the Self Service Portal without having to visit their local RA. Users will be presented with an automated renewal message, which will direct them to the Self Service Portal upon authentication of the Smartcard. This message will only appear when the card is within 30 days of expiry.

5.6 Unlocking Smartcards

This procedure can be carried out by RA Managers, Agents and Sponsors, in instances when a user has entered the incorrect PIN 3 times in a row or when they have forgotten their PIN. Any user needing this service must contact the Employee Services Team in HR.

5.7 Lost Smartcards

Anyone who loses their NHS Smartcard will be charged a replacement fee of £5. Employees will be asked to sign a form authorising a deduction from their pay and a replacement card will then be issued. Repeated loss of a Smartcard may result in disciplinary action.

5.8 Smartcard Governance

All Trust Staff have a duty to keep patient and staff information secure and confidential. The Smartcard provides users access to patient and/or staff information appropriate to their role. All users must keep their Smartcard safe and:

- Always keep their Smartcard safe and secure
- Never tell anyone their PIN
- Never allow anyone else to use their Smartcard
- Never leave their Smartcard unattended
- Never leave their Smartcard in the card reader when not actively using it
- Immediately report its loss, theft or damage to the HR.

If a Smartcard is misused then it may be revoked and access changed without notice. The appropriate action will be taken which may result in disciplinary proceedings and or criminal prosecution.

If a Smartcard user is found to have done any of following, then appropriate action will be taken:

- Accessed unauthorised records
- Modified records without justification
- Transferred records without justification
- Disclosed information to other parties
- Deleted computer records without justification

All of the above are criminal offences under the Computer Misuse Act 1990. An offender is liable to a fine, 5 years' imprisonment or both. Such offences will constitute gross misconduct and may result in summary dismissal. Unauthorised access, modification, transfer, disclosure, or deletion of manual records may be subject to disciplinary action as may misuse of the Trust's e-mail and internet services.

Any misuse of information by staff whose role includes RA elements will be dealt with under the Trusts Disciplinary Procedure. It is a criminal offence to pass registration identify information to anyone who is not entitled to receive it and may result in prosecution.

6 MONITORING COMPLIANCE / EFFECTIVENESS OF THE POLICY

All organisations need to ensure that staff members and those working on behalf of the organisation issued with an NHS Smartcard comply with the terms and conditions of issue. Breach of the terms and conditions and or/organisational procedures relating to Smartcard usage will be linked to disciplinary measures (as stated in section 5.8).

The Trust will report and monitor compliance with IG toolkit requirement 13-303 and 13-304.

The tables below document how the Trust will report and monitor compliance with the IGT requirement 13-303 and 13-304

Standard/Process/issue	IG Toolkit Requirement No: 13-303			
	Methods	By	Committee	Frequency
There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority.	RA Standard Operating Procedures Quarterly RA report	RA Manager RA Manager	IG Group	Quarterly

Standard/Process/issue	IG Toolkit Requirement No: 13-304			
	Methods	By	Committee	Frequency
Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	RA Implementation Plan RA Quarterly Report – reporting on any disciplinary matters/incidents relating to Smartcard misuse	RA Manager RA Manager	IG Group	Annually Quarterly

The RA will continually promote the compliance of Smartcard use and improve the necessary processes.
Any breaches of security will be investigated in accordance with the Trust's Disciplinary Procedure.

7. DISSEMINATION, IMPLEMENTATION AND TRAINING

7.1 Dissemination

- Email to Senior Manager Forum, Matrons and Consultants
- HR Policies on CHS Intranet
- Team Brief
- Dedicated RA page within HR Intranet pages

7.2 Implementation

A summary of the policy will be notified to managers following implementation. Further advice and guidance will be available from the HR Department.

7.3 Training

All staff with RA responsibilities will receive the appropriate training.

RA Agents, RA Agent Advanced, RA Sponsors and RA Administrators will receive appropriate training from the RA Manager and complete e-learning package provided by HSCIC.

The RA Manager will complete RA Manager e-learning package provided by HSCIC.

All Smartcard users must receive guidance or training before accessing any local or national application for the first time. It is the user's responsibility to ensure they have received suitable guidance before accessing any spine or non-spine based application via their Smartcard.

8 CONSULTATION, APPROVAL, RATIFICATION AND REVIEW

Consultation

- Human Resources Strategy Group
- Information Governance Steering Group
- Joint Consultative Group

Approval

- Executive Committee

Ratification

- Policy Committee

Review

- Every 3 years.

9 REFERENCES

There are various legislative and policy imperatives that apply to all care organisations, in all matters concerning the storage and use of person identifiable information. These include:

- The Data Protection Act 1998
- The Computer Misuse Act 1990

- E Communications Act 2003
- Electronic Signatures Regulations 2002
- NHS Confidentiality Code of Practice
- The Records Management NHS Code of Practice
- The Freedom of Information Act 2000
- The NHS Care Record Guarantee for England (PDF, 128.2kB)
- The Code of Practice for the Management of Confidential Information

10 ASSOCIATED TRUST DOCUMENTATION

- Disciplinary Procedure
- Employment Checks Policy
- Internet & Email Policy
- Confidentiality Policy
- Secondary Employment Policy
- Standards of Business Conduct Policy
- Data Protection and Personal Information Handling Policy
- Information Governance Framework
- IM&T Security Policy
- IG Toolkit

Appendix 1

Role	Assigned Job Roles
RA Manager	Workforce Information Analyst
RA Agent Advanced	Workforce Systems Officer
RA Sponsor	Training Manager Assistant Training Manager
RA Agent	Employment Services Officer Employment Services Assistants
Local Smartcard Administrator	TBA

Appendix 2

NHS Care Records Service Smartcard Terms and Conditions V1.0b 1st January 2010

Notice to applicants on the collection of personal data

In accordance with the requirements of Department of Health, the personal data (as defined in the Data Protection Act 1998) that the applicant provided as part of the application process to access NHS CRS together with any personal data processed in relation to the applicant in support of their application is collected for the purpose of identifying the applicant and processing this application and evaluating the applicant for suitability as an authorised user; if accepted, to generate a personalised certificate and Smartcard for the authorised user and for the purpose of managing the applicant's use of any NHS Care Records Service applications or applications that utilise NHS Care Records Service authentication.

In particular, this personal data will be used to validate and verify the applicant's identity to ensure that the applicant is correctly identified and appropriately authorised for access. The personal data in relation to the applicant will be processed by local Registration Authority/Authorities and may be shared with other Registration Authorities for the purpose of processing this application, in accordance with the requirements of the Data Protection Act 1998 as amended and supplemented from time to time. This personal data may also be used to ensure that accurate information can be recorded regarding the applicant's use of systems.

In accordance with the Data Protection Act 1998, this personal data will neither be used nor disclosed for any other purpose other than where required by law, and will be retained in accordance with the Registration Authority's data retention policy. It is the applicant's responsibility to ensure that their registered name is accurate and kept up-to-date. The applicant may contact their local Registration Authority or Sponsor in relation to any queries they may have in connection with this application.

By signing this declaration I, the applicant:

1. Consent to the use of my personal data in the manner described in the "Notice to applicants on the collection of personal data" above. I also agree to provide any additional information and documentation required by the Registration Authority in order to verify my identity;
2. Confirm that the information, which I provide in the process of my application, is accurate. I agree to notify my local Registration Authority immediately of any changes to this information;
3. I agree that the Smartcard issued to me is the property of the NHS and I agree to use it only in the normal course of my employment or contract arrangement;
4. Agree that I will check the operation of my Smartcard promptly after I receive it. This will ensure that I have been granted the correct access profiles. I also agree to notify my local Registration Authority promptly if I become aware of any problem with my Smartcard or my access profiles;
5. Acknowledge that I will keep my Smartcard private and secure and that I will not permit anybody else to use it or any session established with the NHS Care Records Service applications. I will not share my Passcodes with any other user. I will not make any electronic or written copies of my Passcodes (this includes function keys). I will take all reasonable steps to ensure that I always leave my workstation secure when I am not using it by removing my Smartcard. If I lose my Smartcard or if I suspect that it has been stolen or used by a third party I will report this to my local Registration Authority as soon as possible;
6. I agree that I will only use my Smartcard, the NHS Care Records Service applications and all patient data in accordance with The NHS Confidentiality Code of Practice (www.dh.gov.uk site) and (where applicable) in accordance with my contract of employment or contract of provision for service (whichever is appropriate) and with any instructions relating to the NHS Care Records Service applications which are notified to me;
7. Agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate my Smartcard, NHS Care Records Service applications components or any access profiles given to me;

8. Agree not to deliberately corrupt, invalidate, deface damage or otherwise misuse any NHS Care Records Service applications or information stored by them. This includes but is not limited to the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality;
9. Acknowledge that my Smartcard may be revoked or my access profiles changed at any time without notice if I breach this Agreement; if I breach any guidance or instructions notified to me for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. I acknowledge that if I breach this Agreement this may be brought to the attention of my employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);
10. Agree that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of Smartcards for the NHS Care Records Service applications. The Registration Authority is not responsible for the availability of the NHS Care Records Service applications or applications which use NHS Care Records Service authentication or the accuracy of any patient data;
11. Acknowledge that I, or my employer, shall notify my local Registration Authority at any time should either wish to terminate this Agreement and to have my Smartcard revoked e.g. on cessation of my employment or contractual arrangement with health care organisations or other relevant change in my job role; and
12. Acknowledge that these terms and conditions form a binding Agreement between me and those organisations who have sponsored my role(s). I agree that this Agreement is governed by English law and that the English courts shall settle any dispute under this Agreement.