RA Smartcard Policy v3

Policy No: PP26
Version: 3.0

Name of Policy: RA Smartcard Policy

Effective From: 08/01/2016

Date Ratified: 07/12/2015
Ratified: HR Committee
Review Date: 01/12/2017
Sponsor: Director of Strategy & Transformation
Expiry Date: 06/12/2018
Withdrawn Date

Unless this copy has been taken directly from the Trust intranet site (Pandora) there is no assurance that this is the most up to date version

This policy supersedes all previous issues
## Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Release</th>
<th>Author/Reviewer</th>
<th>Ratified by/Authorised by</th>
<th>Date</th>
<th>Changes (Please identify page no.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>January 2008</td>
<td></td>
<td>HR Committee</td>
<td>07/01/2008</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>11/10/2011</td>
<td>Heather Birleson</td>
<td>HR Committee</td>
<td>03/10/2011</td>
<td></td>
</tr>
<tr>
<td>3.0</td>
<td>08/01/2016</td>
<td>Heather Birleson</td>
<td>HR Committee</td>
<td>07/12/2015</td>
<td>Complete change to policy as new registration authority system implemented</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.6</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.7</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.8</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.9</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.10</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RA Smartcard Policy

1 Introduction

The NHS Care Records Service (NHS CRS) is an initiative that has been introduced to ensure that patient’s medical records are appropriately kept secure and confidential in line with the National Care Records Guarantee and Confidentiality Code of Practice.

The process of gaining access to the NHS CRS systems is known as the Registration Authority. The electronic system used is the Care Identity Service (CIS)

The procedures provided in this document support national policies and procedures, in conjunction with the Trust’s current Recruitment and Selection Policies. They will provide practical guidance to managers and staff employed by Gateshead Health NHS Foundation Trust.

2 Policy scope

This policy is applicable to all employees of Gateshead Health NHS Foundation Trust who require access to National Care Records Systems known as Registration Authority.

3 Aim of policy

The aims of this policy are as follows:
• To ensure that there is use of a common security and confidentiality approach when using the NHS CRS systems including the local requirements of information governance;
• To provide practical guidance, to Registration Managers, Agents and Sponsors during the issuing and maintenance of smartcards.
• To ensure such information is not discussed or communicated either outside work or to others directly concerned with the matter, including colleagues. Disclosure of any confidential information contrary to the Trust’s policies and procedures may be an offence under the Data Protection Act 1998 (as amended) or other legislation and can result in prosecution.

4 Duties (roles and responsibilities)

Registration Authority Managers
The Role of the Registration Authority Manager is required to:
• Ensure Registration Authority procedures are carried out in accordance with local and national policies.
• Ensure that Registration Authority agents are adequately trained and familiar with the local and national RA processes.
• Ensure that an secure audit trail is maintained of applicant’s registration information.
• Ensure Sponsors are familiar with and understand the process required for user registration.
• Ensure the National and local Codes of Confidentiality are adhered to.
• Ensure that employees are issued with not more than one smartcard to access CIS systems.
• Renewal of smartcard certificates within the Business Units and Departments when necessary.

Registration Authority Agent
The role of a Registration Agent also includes:
• Responsibility for the verification of Identity Checks of any user of a smartcard.
• Responsibility for ensuring that accurate information is recorded within the CIS for the issuing of smartcards.
• Alerting RA Managers of all incidents, misuses, anomalies and problems with smartcards.
• Ensuring that accurate and most up to date documentation is completed and retained appropriately in line with national requirements.
• Ensuring employees are issued with not more than one smartcard to access the systems.
• Ensuring employees are given the minimum appropriate level of access needed to undertake their role.
• Responsible for the maintenance of a register of Sponsor’s within their link areas to ensure Registration Authority requests are appropriately authorised.

Registration Authority Sponsor
The role of a Registration Authority Sponsor also includes:
• Responsibility for the authorisation of smartcards ensuring that appropriate access level to information systems is authorised
• Reporting any information security incidents to the Registration Authority Manager.
• Resetting of PIN/Passcodes within their area of work when required.

Sponsors who have been delegated responsibility for only taking on the activities of resetting passcodes will be known as ‘Card Sponsors’.

5 Definitions
The Registration Authority function is part of the Trust’s Information Governance framework to ensure that all employees providing healthcare services have timely access to the NHS CRS systems in accordance with their healthcare role.

5.1 Registration Authority Managers
The Registration Authority Managers are nominated by Gateshead Health NHS Foundation Trust Information Governance Board and the Caldicott Guardian and are responsible for the day-to-day maintenance of the Registration Authority service. Registration Authority Managers are indicated on the Trust Intranet.

5.2 Registration Authority Agents and Advanced Agents
Registration Authority Agents consist of trained appropriate members of staff within Gateshead Health NHS Foundation Trust. Registration Authority Agents are responsible to the Registration Authority Managers for ensuring that National and local processes are adhered to. Advanced Agents are designated members of the HR Department.

5.3 Registration Authority Sponsors
Registration Authority Sponsors are nominated by senior members of the Trust and consist of Associate Directors, Executive Directors, Service Line Managers, Heads of Service and Team Leaders or members of staff who they have delegated responsibility to.

Registration Authority Sponsors are appointed and entrusted to act on behalf of Gateshead Health NHS Foundation Trust in determining access rights and role profiles for posts within their area of work.

A list of sponsors can be found on the Trust Intranet.
5.4 The Information Governance Committee

The Information Governance Committee will act as the local Registration Authority Executive. The Trust RA Managers where appropriate are required to provide an update of any untoward incidents to the Information Governance Committee on the following:

- Registration of Sponsors;
- Loss or theft of a Smartcard;
- Misuse of a Smartcard;
- Smartcard configuration issues resulting in inappropriate access to patient information;
- Failure of Registration Authority personnel to comply with this policy or procedures;
- Failure of third party organization to comply with this policy or procedures.

6 Registration Authority Operational Process and Documentation

6.1 Operational Process

The Care Identity Service (CIS) is an electronic system to register, issue Smartcards and assign access to users which is integrated with the Electronic Staff Record (ESR).

Once a candidate has accepted the post the RA Manager or Agent will ensure that all appropriate personal information has been completed in CIS prior to a smartcard being activated and issued.

On the first day of induction all new employees will be required to provide identity documents and will be issued with a smartcard.

All current employees who require access to NHS CRS systems will also be required to report to the RA Manager or Agent in order that a smartcard may be issued.

All current employees already in possession of a smartcard will be required to follow the guidance in section 6.1.4 if they require access changes.

6.1.1 Verification of Identity

Verification of identity must be carried out in line with the Trust’s Recruitment and Selection policy and within Registration Authority national guidance.

Employees must present original, current (i.e. not more than 3 months old) documentation which includes the individual’s name, to the RA Manager or Agent (see section 6.1.2 of this document).

6.1.2 Identity Documentation

Employees will be required to produce 3 documents of ID from the list below. These must be either two personal identity documents and one ‘active in the community’ document or one personal identity document and two ‘active in the community’ documents.

a) Acceptable Personal Identity Documents:
   - Current UK, EU and other nationalities passports. Non-EU nationals’ passport should contain UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK;
• Current EU and non-EU Photo-card Driving Licence;
• UK Birth Certificate;
• Residence permit issued by Home Office to EU Nationals on inspection of own-country passport;
• Adoption certificate;
• Marriage/Civil Partnership certificate;
• Divorce or annulment papers;
• Police registration document;
• Certificate of employment in HM Forces;
• Current benefit book or card or original notification letter from the Department of Work and Pensions (DWP) confirming legal right to benefit;
• Recent Inland Revenue tax notification;
• Firearms certificate;
• Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms);
• GV3 form issued to people who want to travel in the UK without valid travel documents;
• Home Office letter IS KOS EX or KOS EX2;
• Building industry sub-contractor’s certificate issued by the Inland Revenue.

b) Acceptable ‘Active in the Community’ Documents
• Recent (i.e. not more than three months old) utility bill or a certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms (note: mobile telephone bills should not be accepted as they can be sent to different addresses). Utility bills in joint names are permissible;
• Local authority tax bill (valid for current year);
• Current UK photo card driving licence (if not already presented as a personal ID document);
• Current Full UK driving licence (old version);
• Bank, building society or credit union statement or passbook containing current address;
• Most recent mortgage statement from a recognised lender;
• Current local council rent card or tenancy agreement;
• Current benefit book or card or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit;
• Confirmation from an electoral register search that a person of that name lives at the claimed address;
• Court Order.

Only documents included in the above list will be accepted as proof of identification by the RA Manager or Agent. Organisational ID card/badges will not be recognised as acceptable proof of identification.

6.1.3 Employees appointed with no previous Smartcard
Sponsors are required to identify on the Vacancy Control Form where a smartcard is required to access the NHS CRS Systems.

The appointee will be required to register a pass code within CIS as part of the registration process, with the Sponsor for their department.
The smartcard will be produced by the RA Manager or Agent and issued at induction.

6.1.4 Employees appointed with a smartcard
Employees transferring within the NHS will be required to produce to the RA Manager or Agent any existing smartcard that has previously been issued by an NHS organisation.

The employee will be required to report to induction with their Identification in order that their smartcard can be updated.

The RA Manager or Agent will access CIS and adapt the smartcard information in accordance with the details outlined by the sponsor or from ESR.

6.1.5 Smartcard Access and Role Changes
Any changes required to a Smartcard access must be authorised by an RA Sponsor. A request must be completed by the Sponsor and forwarded to the RA Manager or Agent.

The RA Manager or Agent will complete the changes by amending CIS and advise the employee once the changes have been made.

6.1.6 Removal of Access
Employees who undertake a period of long term authorised leave (i.e. Maternity, Sickness, Adoption) may retain their smartcard, however all access to the NHS CRS systems will be revoked during their period of leave. This process should be undertaken in line with smartcard and access role changes as outlined in section 6.1.5

Employees who are classified as on unauthorised leave may have their access revoked and cancellation of the smartcard arranged.

Employees who resign from their post may retain the smartcard, providing they can provide confirmation of employment with another NHS organisation to the RA Manager or Agent. If the employee is transferring to another NHS Organisation or GP Practice where the smartcard will be required, a request must be made by the RA Sponsor. The RA Manager or Agent will remove the security access relating to this Trust.

Employees who are leaving the Trust and are not remaining in the NHS should hand back their smartcard and the RA Sponsor should notify the HR Department. The RA Manager or Agent will ensure that all information held within the registration system is deactivated and the smartcard is destroyed.

Employees who have been suspended or are taking part in disciplinary proceedings may retain their smartcard but their access to the NHS CRS systems will be revoked for their period of absence from the Trust. This process should be undertaken in line with smartcard and access role changes as outlined in section 6.1.5

Should an employee leave the Trust during or at the end of any suspension period, the RA Sponsor should send the request for the cancellation of the smartcard and the deactivation any associated access.
The employee must in any event upon termination of employment with the Trust return their smartcard to the Line Manager/Sponsor.

6.2 Documentation

Care Identity Service (CIS) is the electronic registration application that is available to all organisations to perform Registration Authority activities. This system improves automation, supporting an enhanced registration process.

There may be circumstances where RA staff do not use CIS but the minimum mandatory data needs to be captured in a paper format to be entered into the electronic system CIS at a later time.

The CIS Forms are a contingency process for RA staff in the event of CIS not being used. RA staff will subsequently need to enter the information from the forms in CIS.

Registration Authorisation forms must be completed by the designated Sponsor to ensure appropriate levels of access to NHS Care Records systems have been authorised.

All documentation used throughout the Registration Authorisation process, is in line with national guidance and can be accessed via the Trust’s intranet.

Details of the appropriate CIS forms are listed below.

- CIS - Create New User (RA use only)
- CIS - Request Creation of New User (Sponsor use only)
- CIS - Modify User Personal Details
- CIS - Position Assignment Modification
- CIS - Cancel Smartcard

6.2.1 CIS Create New User form (RA use only)

The information in the CIS Create New User form must be entered in CIS in the event CIS is not being used to register a new Smartcard user. This form is to be used by the following RA roles to register a new Smartcard user in CIS.

- RA Manager
- Advanced RA Agent
- RA Agent

The above RA roles must ensure that the applicant’s identification is verified to e-GIF Level 3. Identification documentation presented by the applicant as per the Identity Checks laid out in section 6.1.2 and a photograph of the individual must be captured at the meeting that is suitably labelled to be uploaded to CIS. New Smartcard Users will still be required to access the Care Identity Service to electronically accept the Terms and Conditions of Smartcard use once they have been issued their NHS Smartcard.

6.2.2 CIS Request Creation of New User form (Sponsor use only)

The CIS – Request Creation of New User form is to be used by Sponsors to request the creation of a new user in the Care Identity Service which must then be sent to their local Registration Authority who will arrange a meeting with the applicant to verify identification.

6.2.3 CIS Modify User Personal Details form

The CIS - Modify User Personal Details form is to be used by RA staff responsible for verifying identification in the event a change needs to be made to a user’s personal
identity. Identification must be verified to e-GIF Level 3 and Smartcard Users must present proof of identity as per the Identity Checks laid out in section 6.1.2 to request a change to a user’s personal details as result of the following circumstances:
· Marriage
· Change of Name by deed poll
· User name incorrect in CIS

6.2.4 CIS Position Assignment Modification form
The CIS - Position Assignment Modification form is to be used by RA staff or Sponsors to request the assignment or un-assignment of a position to an existing user’s access profile.

6.2.5 CIS Cancel Smartcard form
The CIS – Cancel Smartcard form is to be used by RA staff or Sponsors to request the cancellation of a Smartcard. RA staff entering the information in CIS should select the appropriate CIS workflow to cancel the Smartcard.

6.2.6 Archiving Documentation
All completed documentation must be kept secure in line with the requirements set out in the National Health Records Code of Practice and the Record Management Policy (OP10).

6.3 Difficulties with Smartcards

In the event of an employee discovering there is a problem with the use of their smartcard they must in the first instance report the difficulty to the IT Service desk who will endeavour to resolve the problem.

The IT service desk will redirect any issues they are unable to resolve to the RA Agent within the HR Department who will carry out further investigation to resolve the problem.

6.4 Lost or Stolen Smartcards

Lost or stolen smartcards must be reported to the RA Manager or Agent. The RA Manager or Agent will arrange for the information held within the smartcard to be revoked and a new card issued as appropriate.

6.5 Pin/Passcode Resetting

Employees who have forgotten or wish to change their PIN / Pass-code must contact their RA Sponsor in order for the necessary process to be arranged. The RA Sponsor will be responsible for resetting the PIN/Pass-code in the presence of the employee.

Employees must notify their sponsor if they suspect that their pin/ passcode has become known and could be used by another member of staff. In order to maintain security it is recommended that employees periodically change their passcode.

6.6 Out of Hours Support

Card Sponsors should be identified within all Departments across the Trust to assist with PIN/Passcode resetting at all times. In the event that a Card Sponsor is not available during
out of hours the employee should contact the Acute Response Team (ART) who will arrange to meet the employee and reset their PIN/Passcode.

6.7  **Locum Access**

All locum staff must be registered with a smartcard in line with section 6.1 and 6.2 during standard working hours. Locum staff working outside of standard hours will be required to report to the senior clinician/ manager in charge of the department who will advise on how access to the NHS CRS systems will be supervised.

Locum staff will be required to provide documentation to the Senior Clinician detailing their working arrangements for the Trust along with evidence of their employment with the locum agency e.g. locum ID badge including a photograph as verification of identity.

6.8  **Honorary Contracts**

A nominated Sponsor within the department that the individual will be working on an honorary contract basis will be required to authorise access to CRS Systems. Authorisation should be carried out in line with guidance set out in section 6.1.2 and 6.1.3 and appropriate RA documentation will be held centrally within the HR department.

Any changes or revoking of access to the smartcard should be carried out in line with section 6.1.2 and 6.1.3 and should be authorised by the Sponsor.

6.9  **Service Level Agreements**

Employees working as part of a Service Level Agreement with the Trust will be required to liaise with the identified Sponsor within the department they are based in order to discuss specific arrangements for the issuing of a smartcard. The sponsor will be required to contact the RA Manager of the Trust to ensure appropriate authorisation can be arranged.

6.10  **Incident Reporting**

Incidents may be reported by any member of staff where they feel that there is a risk to patient health, confidentiality or Gateshead Health NHS Foundation Trust. Incidents should be reported, using the existing Trust incident reporting procedures named DATIX.

Any major breach of security will also be reported by the RA Manager to the Systems Management and Development Group and the Caldicott Guardian

7  **Training**

RA Managers, Agents and Sponsors will be required to undergo specific relevant training within the application of the Policy.

8  **Equality and diversity**

The Trust is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds. This policy has been appropriately assessed.
9 Monitoring compliance with the policy

<table>
<thead>
<tr>
<th>Standard/process/issue</th>
<th>Monitoring and audit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Method</td>
</tr>
<tr>
<td>Audit of Compliance with Policy</td>
<td>IG Toolkit</td>
</tr>
</tbody>
</table>

10 Consultation and review

This policy has been reviewed in consultation with the JCC Policy Sub Group and LNC.

11 Implementation of policy (including raising awareness)

This policy will be circulated by the Trust Secretary as detailed in OP27 Policy for the Development, Management and Authorisation of Policies.

12 References

This Policy will operate in conjunction with the following:
- National Registration Policy and Guidance
- NHS Care Record Guarantee
- NHS National Framework 2008
- Information Governance Toolkit
- Data Protection Act 1998
- Confidentiality NHS Code of Practice 2003

Trust Policies

- PP10a Recruitment and Selection Policy/Procedure
- PP10b Recruitment and Selection of Consultant Medical staff
- PP10c Appointment and Employment of Locum Medical staff
- OP06 IT and Information Security Policy
- OP10 Records Management