NHS Business Services Authority
Registration Authority and Smartcard Management Procedure

NHS Business Services Authority
Corporate Secretariat
NHSBSAIS005
## Issue Sheet

<table>
<thead>
<tr>
<th>Document reference</th>
<th>NHSBSAIS005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document location</td>
<td>F:\CEO\IGM\IS\BSA</td>
</tr>
<tr>
<td>Title</td>
<td>NHS Business Services Authority Registration Authority and Smartcard Management Procedure</td>
</tr>
<tr>
<td>Author</td>
<td>Gordon Wanless</td>
</tr>
<tr>
<td>Issued to</td>
<td>All staff</td>
</tr>
<tr>
<td>Why issued</td>
<td>For reference</td>
</tr>
</tbody>
</table>

## Revision Details

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended by</th>
<th>Approved by</th>
<th>Details of amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Release</td>
<td>21.09.09</td>
<td>-</td>
<td>IGSG</td>
<td></td>
</tr>
</tbody>
</table>
## Contents

1. Introduction .......................... 4  
2. Roles and Responsibilities ............. 4  
3. Hardware and Software Requirements for Registration Authority .................. 6  
4. Registration and Issuing of Smartcards ........................................... 7  
5. Smartcard Maintenance .................. 23  
6. Validity of this Policy .................. 25
1 Introduction

1.1 This document details the roles and responsibilities within the NHS Business Services Authority operating as a Registration Authority. This document will also detail the processes required to create and maintain users of NHS Clinical Records (NHS CRS) Systems, through the use of smartcards.

1.2 Further information concerning the management of a Registration Authority can be found at http://nww.connectingforhealth.nhs.uk/implementation/docs/RA_Operation_Process_guidance.doc

2. Roles and Responsibilities

Registration Authority

2.1 The role of the NHSBSA Registration Authority is to ensure that individuals providing healthcare services to the NHS directly or indirectly have timely access to NHS Care Records Service compliant applications (and information) in accordance with their role. It is the NHSBSA's responsibility to ensure that all the requirements of Registration Authorities are met and maintained to meet the requirements of the NHS Confidentiality Code of Practice and the Care Record Guarantee.

RA Manager

2.2 The RA Manager is approved and sponsored by the Caldicott Guardian for the NHSBSA.

The NHSBSA RA Manager is the Head of Information Governance

The RA Manager is responsible for:

- Assigning RA Agents and RA Sponsors
- Ensuring RA Agents are adequately trained and aware of their responsibilities number local and national policies and procedures
- Reporting all RA related incidents to the Caldicott Guardian/Information Governance and Security Group
- Escalating all incidents that cannot be resolved locally to the next layer of RA cascade
- Ensuring RA roles have adequate hardware and software necessary to administer the RA and have access to Spine applications

**RA Agents**

2.3 RA Agents are assigned by the RA Manager and act on his behalf at each of the NHSBSA divisions.

The NHSBSA has the following RA Agents:

- Counter Fraud and Security Management Division
  Head of Information Systems
- NHS Dental Services
  Business Manager

They are responsible for:

- Assigning users within their own Business Area.
- Ensuring RA Sponsors are trained in their responsibilities, including how to unlock smartcards and if necessary issue fallback smartcards
- Monitoring use of NHS CRS by all users within their division, including ensuring prompt deletion of users leaving the organisation
- Reporting all incidents that cannot be resolved locally to the next layer of the RA cascade
- Supporting the RA Manager in ensuring RA roles have adequate hardware and software necessary to administer the RA and have access to Spine applications

**RA Sponsor**

2.4 The NHSBSA has the following RA Sponsors:

- Counter Fraud and Security Management Division
  TBC
- Dental Service Division
  Monitoring and Assessment Manager

They are responsible for:

- Approving users as defined through the use of the RA01 and RA02 processes, detailed later in this document
• Working with the RA Manager / Agent to ensure all users are given the correct user access levels to NHS CRS applications
• Unlocking smartcards and resetting passwords

3 Hardware and Software Requirements for Registration Authority

3.1 To ensure that the NHSBSA is able to function efficiently as a Registration Authority, it is necessary that all appropriate staff have access to the appropriate hardware and software necessary for the administration of the RA and allowing access to appropriate Spine applications.

3.2 IT Requirements

3.2.1 For the management of the RA and access to the relevant spine applications, the RA Manager and each RA Agent will require the following equipment:

- PC or laptop with 5 or more USB ports or USB hub;
- N3 network connection;
- Supply of blank Smartcards;
- Smartcard printer;
- Digital camera / web cam
- Two Smartcard readers

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.

An adequate supply of smartcards must be retained, to allow for the creation of smartcards for new staff, and for replacement when cards are lost / stolen / broken.

At least one spare ink cartridge should be retained with each Smartcard Printer.

3.2.2 Any user that requires access to Spine applications will require for following equipment:

- PC or laptop;
- N3 network connection
3.3 Card Security

3.3.1 All Users must be made aware of their responsibilities for security of their smartcard.

3.3.2 When applicants sign the RA01 form (as described later in the document) for their initial registration, they 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.

3.3.3 Cards which appear to have been lost or stolen must be reported promptly and action taken to ensure that their use is revoked in accordance with the advice in Section 4.

3.3.4 The security of the NHS systems underpins 'The NHS Care Record Guarantee' which is a commitment to use the records we hold about patients (past and present) in ways that respect their rights and promote their health and wellbeing, see: http://www.connectingforhealth.nhs.uk/crdb

3.3.5 If there are any breaches of this agreement in the use of the smartcard, the card should be confiscated and the RA Manager and Caldicott Guardian must be informed.

4 Registration and Issuing of Smartcards

4.1 In order to use the NHS CRS users must have a smartcard that defines their types of access to specific applications, such as the Personal Demographic Services (PDS).

4.2 Overview of Process

4.2.1 The RA Sponsor, in conjunction with the responsible manager for a member of staff decide whether a smartcard application should be put to the RA Manager or Agent, whilst at the same time deciding on what systems can be accessed together with the appropriate role(s) to be given to the user.

4.2.2 The RA Manager / Agent is responsible for verifying the identity of a user prior to a smartcard being issued and subsequent registration on the Spine User Directory (SUD).
4.2.3 The process itself has 4 steps:

1. Complete RA01 (application and authority for a card – this should only be necessary once during any period of continual service) and / or a RA02 (assignment of user profile) form/s
   - RA Sponsor countersigns application and approves job roles, etc.
   - RA Manager / Agent checks and confirms identity seeing proof 'Beyond Reasonable Doubt'
2. A Photograph is taken of the applicant
3. Enter or amend applicant’s details on Spine User Directory and role profile
   - Name details
   - Organisation they require access to
   - Roles and additional functions
   - Import data and upload images
4. Produce the smartcard with user choosing PIN

4.3 Completion of RA01 and RA02 forms

4.3.1 Form RA01

Once an RA Sponsor and the appropriate line manager have decided that it is appropriate for a member of staff to be issued with a smartcard and what role(s) they should be given for accessing NHS CRS applications, the applicant is given form RA01 together with RA Short Form Conditions, which should be read by the applicant prior to be issued with a Smartcard.

Once completed by the applicant the RA Sponsor should request identification and complete the remainder of the form and pass it to the RA Manager/Agent.

The RA Manager/Agent meets with the applicant, ensuring they are aware of their responsibilities for use of the smartcard and NHS CRS applications. The RA Manager/Agent also confirms the identity of the applicant by viewing their id documents. The unique number of the ID document(s) should be entered on the RA01 form, and date and community document type should also be entered. No copies of these documents are taken.

The minimum ID Requirements are:
TWO ID documents and ONE ‘active in the community’
document, or
ONE ID document and TWO ‘active in the community’
documents

There is a list of id documents that are acceptable available
through the CfH website, but normally these are current
Passport and current photo card Driving Licence.

For ‘active in the community’ documents again there is a long
list but these can be a non-photo Driving Licence (not
provisional), Utility Bills (not mobile phone), Bank Statements,
not older than three (3) months, or this year’s Council Tax
statement. In essence this is a confirmation of residence.

The full list of id is located in CfH’s RA Operation Process
Guide.

4.3.2 Form RA02

Form RA02 should be completed by the RA Sponsor.

The NHSBSA organisation code is T1450.

User rights are assigned through Role Based Access Control
(RBAC) and details the level and complexity of access that the
user will have with the application and ultimately patient data.
This access has to be justifiable and is fully audit trailed; the RA
Sponsor granting the access takes the responsibility for the
appropriateness they have given the user.

4.4 Entering or Modifying an Applicant’s Details on Spine User
Directory

4.4.1 Logging on to the Spine User Directory (SUD)

Entering or Modifying an Applicants details can only be carried
out by the RA Manager or RA Agent, who has an authorised
Smartcard and at least one card reader.

To logon to the SUD:

• Connect to the NHS Spine Portal at
  https://portal.national.ncrs.nhs.uk
• Select the ‘Launch Spine User Directory’ Link
• Selecting the ‘Launch Spine User Directory’ will take you through to the NHS CRS User Registration Service.

• Click on the Registration tab

• Check whether the user is already registered by using the People Search. (Very important to ensure that duplicate entries are not made)
• If the person you wish to register has never been issued with a smartcard, you will need to create the person on the Directory by selecting the ‘Create Person’ option.

Selecting the ‘Create’ person option takes you through to the Create Person screen

Enter details from the RA01 form.

• Passcodes:

If the user is present allow them to enter their ‘passcodes’ although this may be done at a later date – there are two types:
The **Account Recovery Passcode** is used by registered users to prove their identity to a member of the Registration Authority, this may be undertaken remotely.

The **Employee Passcode** is currently used to verify the identity of registered users to a member of the BMS (Booking Management Service) for the Choose and Book application.

Each Passcode may be **different**, must be set up by and known only to the user. These Passcodes must be made up of a minimum of 8 characters (alpha numeric, upper/lower case) up to a maximum of 25. This allows for the use of a short phrase.

- **E-GIF Compliant:**

  Click on arrow next to “e-Gif Compliant” and if they have been adequately identified then select level 3. (This implies that the applicants identity has been established Beyond Reasonable Doubt through ID checks and personal corroboration to the Registration Agent)

- **Create an entry and note the UUID Number:**

  Once you have finished, press the ‘Create’ button, this will create the person in the Directory.

  On the 2nd page of the RA01 the registration agent signs and enters their UUID under issuing RA. Enter applicants UUID which has been generated by the database. This is a twelve digit number and eventually will be printed on the smartcard under the Chip.

- **Associating the applicant with the NHSBSA:**

  Once you have registered the person you will need to associate them to the NHSBSA which they are to be registered by selecting ‘Create Organisational Person’
This will take you to a search screen where you can identify the organisation you wish to associate the user to. Here you enter the NACS code of T1450.
Add the user’s job title – this is free text field.

Also, a local e-mail address can be added in the box under the Fax Number field (see arrow 2 – below) and press ‘Add Value’

Select Create (see arrow 3)

- Creating the user’s role:

Once you have finished associating the person to the NHSBSA, you need to set up the user’s role profile. Click on the ‘Roles’ tab to take you through the relevant screen
Click on ‘Create New Role’

This will take you to the screen where you add the user’s job role and business

Click on the ‘Add Value Button’ next to the Job Role field to take you into the Job Role Search Dialogue
Enter applicant’s job role code from the of RA02 (codes listed earlier in this document) and press Search.

Click on job role hyperlink to take you back to the previous screen, where the job role field will be populated with your choice from the previous screen.

Now click on the ‘Add value’ button next to the ‘Business Functions’ field to take you into the Business Function Search Dialogue. Enter business function code from the RA02 (for PDS the code is B0264).
Click on business function hyperlink and then press Close. This will take you back to the previous screen. Simply press ‘Create’ to complete the user’s profile.

Now the user photograph needs to be taken and upload to the relevant profile.

4.4.2 Digital Photograph

The required standard is a facial / head and shoulders image of the applicant against a plain light coloured background, similar to a passport photograph.

Any reasonable definition digital photograph (1 Mega Pixel is ideal) will suffice.
Note: Photographs showing detailed background or office scenes should be avoided as they may be rejected at the card printing stage.

- **Creating Smartcard:**

Choose the ‘Smart Card’ tab

Select ‘Import Person & Issue Card’

The screen will display the details of the card being produced.

Select ‘Change Picture’ to add the picture to the named user;
Select Photograph for access to the directory or location of the picture;

![Image Capture](image.png)

Browse – to select the directory of the image or camera;

![Browse](image.png)

This will allow selection of the relevant folder and image – for example;

![Select file to upload](image.png)
When selected the image will be displayed in the left window (as below)

Size the picture for a facial (portrait) view in the ratio of approximately 3:4 the actual image will be displayed in the right hand frame – this can be attempted multiple times by clicking again in the left window.

When completed ‘Upload the image’ using the tab circled at the bottom of the screen (see above).
If the image is as required then ‘save’ the entry as shown.

This will now activate the software to produce a card – to terminate from this function select another tab such as ‘registration’.

You have now successfully added a photograph to the card profile for the user.
4.5 Storage of Documentation

All forms are stored securely as they contain confidential information. There is a requirement to keep them until the applicants 70th birthday or 6 years after leaving the service, whichever is the later; as other employment / HR personnel documents as required by the Records Management: NHS Code of Practice, Records Retention and Disposal Schedules. (Formerly HSC 1999/053 ‘For the Record’)

4.6 Change of User’s Role Profile

When there is a change in a user's profile, it is essential that their profile on the Spine User Directory is amended.

Form RA02 should be completed by the registration agent and signed by the sponsor to show which roles or activities have to be added or removed. Print a copy for the records.

To make changes in Spine User Directory select Roles tab

Then select the option to create, edit or delete roles as appropriate
5 Smartcard Maintenance

5.1 New Staff Already Having Smartcards

Where a new member of staff already has a smartcard; complete form RA02.

Insert name of new organisation, job role and activity.

Amend Spine User Directory by associating them with the NHSBSA and create a new role as authorised.

5.2 Leavers

If staff leave but will still require access to CFH applications, their links with the NHSBSA must be deleted in the SUD and they should retain their card. To do this an RA02 form will need to be completed. Once this is done you can go into the SUD, locate the user, select the NHSBSA and click the 'Delete Organisation Person' link and enter in the 'Status Information' field the relevant reason for the change. Then click the 'Deactivate' button. (*Care must be taken here not to delete the person as this irrevocably removes them from the useable database and if done by mistake they must then go through all of the ID stages again*)
When staff leave and will no longer require access to CFH applications within any NHS, or associated organisation, their profile will need to be deleted from the SUD and the card destroyed. To do this an RA03 form will need to be completed and within 24 hours the card and form returned to the RA Agent or RA Manager. Without the card, the form must be completed as the certificates will need to be revoked to render the card inactive.

5.3 Lost / Stolen / Broken Cards

If a card needs to be replaced because it has been lost stolen or no longer works, you must complete the RA03 form and send it to the RA Agent or RA Manager where the old card will be revoked and a new card issued if required.

The security of the card and that of applications that can be accessed with the card relies upon a security technique of two-factor authentication.

What you have – The Smartcard
What you know – The PIN Number

Changing the PIN Number / or Unlocking Card can be achieved by specialist software (known as CMS) available to a Sponsor, RA Agent or RA Manager.

5.4 Card Security

When applicants sign the RA01 form for their initial registration, they 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.

Cards which appear to have been lost or stolen must be reported promptly and action taken to ensure that their use is revoked in accordance with the advice in Section 5.

The security of the NHS systems underpins 'The NHS Care Record Guarantee' which is a commitment to use the records we hold about patients (past and present) in ways that respect their rights and promote their health and wellbeing, see: http://www.connectingforhealth.nhs.uk/crdb

If there are any breaches of this agreement in the use of the smartcard, the card should be confiscated and the NHSBSA
Registration Authority and Caldicott Guardian must be informed.

6 Validity of this Procedure

6.1 This procedure is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

6.2 This procedure should be reviewed annually under the authority of the NHSBSA Leadership Team.

6.3 The NHSBSA will regularly audit its RA management practices for compliance with this procedure.

The audit will:

- Identify areas of operation that are covered by the NHSBSA’s policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the procedure to cover missing areas if these are critical to RA management, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.
- The results of audits will be reported to the IGSG.