



REGISTRATION AUTHORITY, SMARTCARD & NHS NUMBERS POLICY & PROCEDURE

BADGER GROUP
Badger House
121 Glover Street
Birmingham, B9 4EY

Destroy All Previous Issues

This document is the property of Badger and must not be reproduced, published or used by any third party without prior written authorisation from Badger.

Contents

1	INTRODUCTION	1
2	POLICY	1
3	BACKGROUND	2
4	SCOPE OF THE POLICY	2
5	Roles & RESPONSIBILITIES	2
6	SMARTCARDS PROCEDURE	4
6.1	New starters without Smartcards	4
6.2	New Starters with Smartcards	5
6.3	Existing Staff with a role change requiring a Smartcard	5
6.4	Personal Detail and Role Changes for Smartcard Holders	5
6.5	Leavers	6
7	NHS NUMBERS	6
8	PRINCIPLES FOR THE USE OF THE NHS NUMBER	6
8.1	Find the NHS Number	6
8.2	Use the NHS Number	6
8.3	Share the NHS Number	7
8.4	Duplicates or Errors identified on PDS	7
9	DEPLOYMENT	7
10	INCIDENT REPORTING	7
11	CONFIDENTIALITY	7
12	SMARTCARD TERMS AND CONDITIONS	8
13	GUIDANCE	8
13.1	Terms & Conditions	9
13.2	Glossary of terms	10
14	APPENDIX I – SMARTCARD DOCUMENTATION REQUIREMENTS	11
14.1	Identifiers	11
14.2	Applicant Contact details	11
14.3	ID card	11
14.4	Identity Verification	11
14.5	Acceptable Documents	11

DOCUMENT CONTROL

Document Storage

Location: P:\Ops Team\Central Policies & Procedures - Development - Word Docs\IG - IG Soc - GDPR Policies\IG-43 - Registration Authority Smartcard NHS Numbers Policy Procedures V1.4.docx

Version Control Log (Only last 3 versions, earlier versions can be found in the appropriate Archive directory for the document)

Version	Date	Author	Description of Changes
V1.2	July 2019	S Owen	Under review
V1.3	Dec 2019	S Owen	Reviewed, Minor changes
V1.4	August 2022	V Young	Reviewed, Minor change to 6.4

Approval

Version	Name	Position	Signature	Approved Date
V1.0	EMT	Executive Management Team		10 March 2017
V1.1	IGSG	IG Steering Group		21 March 2018
V1.2	Badger Executive	Executive Team		25 July 2019

Glossary

Term	Description
PDS	Personal Demographics Service
RA	Registration Authority
SCR	Summary Care Records
UUID	Unique User ID – allocate to Smartcard holders
CIS	Care Identity Service
PII	Personally Identifiable Information

1 INTRODUCTION

Badger is a provider of Urgent Primary Care and GP Out of Hours services across Birmingham and Solihull. Badger's Registration Authority (RA) work is carried out using the online NHS Digital Care Identity Service in conjunction with Midlands and Lancashire CSU (MLCSU)

Badger is categorised as a 'NHS Business Partner/ALS' i.e. supplying healthcare services to the NHS, and therefore has an obligation to comply with the Data Security & Protection (DSP), Cyber Security and information governance requirements of NHS Digital.

Badger has an internal Registration Authority (RA) function that undertakes the necessary requirements in accordance with agreed process to manage Smartcards prior to submission to the MLCSU that undertakes the final authorisation and production of the Smartcard..

Smartcard usage within Badger is currently limited to accessing the personal demographic service (PDS) for initial registration of patients. Staff will be issued with Smartcards. All Smartcard holders are registered with the RA at MLCSU and in Badger records.

PDS is the national electronic database of NHS patient details containing information relating to patient names, addresses, birth dates and NHS Numbers. The NHS Number is unique to an individual and a common means to ensure that a patient is correctly identified.

Once an applicant has been successfully registered, they will have a Unique User ID (UUID), pin-code and a Smartcard issued to them. The use of the card will permit access to the appropriate functionality of the Adastral system.

This document outlines the policy, process, roles and responsibilities to ensure that Badger is compliant with the terms and conditions for NHS Smartcard use.

2 POLICY

Badger will:

- Comply with NHS Digital national policy in relation to Registration Authority and the issue and use of Smartcards
- Ensure there is effective local governance with clearly assigned roles and responsibilities for the RA and Smartcard processes.
- Ensure there is adequate skills, knowledge and trained staff to manage the RA process
- Arrange for the provision of Smartcards for staff whose role dictates the requirement of a Smartcard.
- Ensure that Smartcards holders are properly trained in the use, safekeeping and they are fully aware of their responsibilities and commitments
- Implement processes and procedures to ensure that there is monitoring of the use, misuse, of the Smartcard and that appropriate disciplinary procedures are in place
- Implement systems and procedures to manage registration of users and Smartcards.
- Operate an integrated procedure between Badger HR and RA process.
- Ensure that appropriate equipment and software is installed, operational and maintained for the use of Smartcards.
- Maintain a working protocol with the MLCSU for the production of the Smartcards.

3 BACKGROUND

'NHS Digital launched the Care Identity Service (CIS) in February 2015 to replace the former spine identity management service. The CIS ensures only authenticated healthcare staff, with a legitimate reason to do so, can access systems and patient information held on the NHS Spine. Health and social care workers are issued with a Smartcard which, when inserted into a reader with their passcode, gives them access to the NHS Spine at the level necessary to perform their role, so protecting the security and confidentiality of patients' information.

The Registration Authority (RA) was created to manage and control the access Healthcare Professionals & Smartcard holders have to the CIS.

The change introduced new Authentication, Directory and Smartcard Identity Registration services for secure access to patient information. CIS issued by RA Managers (RAMs) and their RA staff including RA Agents, Sponsors, ID Checkers and Local Smartcard Administrators.

Badger uses AdastrA (supplied by Advanced Health & Care Software) as the patient management system. The system is compliant with the NHS Digital requirement for N3 connectivity and interfacing with the NHS Spine. The system has the capability to interface with the PDS to verify patients demographics. Badger authorised Smartcard holders are able to access these details. Users access AdastrA via their Smartcard and Personal Identification Number (PIN) to authenticate their identity and comply with Badger process for system security.

The RA Manager & Agents along with the RA Sponsor, are responsible for ensuring the development, and compliance with local RA policy and processes and ID Checkers. Local Smartcard Administrators are responsible for creating a digital identity for Clinicians, Manager/Team Leader and non-clinical staff who require access to data held on Smartcard enabled systems; assignment of the appropriate access rights to an individual

Midlands and Lancashire CSU are responsible for the production of Smartcards and following authorised notification will make necessary changes to role access rights.

4 SCOPE OF THE POLICY

This policy applies to all processes, procedures and activities carried out by Badger RA Managers, Sponsors, ID checkers and local administrators authorised to use CIS. This is a limited number of individuals and is strictly contained in order to ensure appropriate governance and standards are maintained whilst supporting the needs of the business.

The policy also applies to all staff authorised by the Registration Authority to access PDS where access is a requirement of their role.

5 ROLES & RESPONSIBILITIES

The senior roles of RA Sponsor and the RA Manager are confirmed to the individual in writing and formally recorded within their HR records and approved by the Executive Team.

RA Sponsor & Manager	<ul style="list-style-type: none"> ○ Accountable for the running of RA activity in their organisation, ○ Accountability for developing the Policy and maintaining the processes, ○ Ensuring the accurate input of information on NHS Digital Care Identity Service (CIS). ○ Perform the role of Information Asset Owner (IAO) in relation to all aspects of the Registration Authority. ○ The RA Manager assigns the user to the Access profile where the request has been approved by the Sponsor
----------------------	---

	<ul style="list-style-type: none"> ○ Responsible for training all other RA staff who will conduct ID checking to ensure appropriate standards are maintained and can be evidenced as part of IG Toolkit requirements ○ To be familiar with and adhere to the Registration Authorities guidelines and governance arrangements for NHS Business Partners.. ○ To ensure that users have only one NHS Smartcard issued to them showing their Users Unique Identifier (UUID) and photograph ○ To ensure that National registration Policy and processes are adhered to ensuring local processes are aligned with National Policy and Processes. ○ To ensure integration with other business processes, e.g. HR processes for starters, leavers, suspensions, and terminations. ○ To report all RA related security incidents and breaches in accordance with Badgers Adverse Events Policy ref:CG-02. ○ Develop an internal framework to manage RA and Smartcards ○ Ensure that Agents are correctly registered with the Registration Authority at MLCSU using the full authentication process or ensure that MLCSU are informed of changes in the role of RA Lead. ○ Ensure that the role profiles are agreed with the MLCSU and are implemented. ○ Oversee the administration of the Smartcard database ○ Immediately report to the RA Agent at the CCG/CSU(s) any lost, stolen, or misplaced cards. ○ Inform the RA office at the MLCSU of any Smartcards that need to be suspended or revoked. ○ Ensure Smartcard holder's access rights are removed or suspended from the system when leaving ○ Ensure that holder is aware of their responsibilities and acts in accordance with these responsibilities ○ Ensure that employees within Badger are aware of their responsibilities in relation to use of and access to the system
Local Smartcard Administrators	<ul style="list-style-type: none"> ○ Support existing users ○ Renew expired certificates ○ Unlock Passwords ○ Change Passwords ○ Maintain electronic register of Badger issued Smartcards
RA Agents/Smartcard Users (Clinicians, Manager/Team Leader and non-clinical staff)	<ul style="list-style-type: none"> ○ Provides appropriate identification as per NHS Employers Identity Check standards to ensure their identity is verified ○ Keep their PIN Number secure and confidential and not share this with anyone, including colleagues ○ Keep their Smartcard secure and with them at all times during working hour ○ Pass duplicate patient records to the Patient Amalgamation Queue when identified during operational times (Refer to A08 – Patient Amalgamations for further details) ○ Ensure that no one else uses/has access to their Smartcard and take reasonable steps to protect it from misuse ○ Smartcard holders must not leave their PC logged in and unattended; must not leave Smartcards unattended; must not share or provide access to their Smartcards or passwords. ○ Report any loss, theft or suspected misuse to the Team Leader who will report the matter to the Badger RA Sponsor, who in turn then report the loss to the appropriate MLCSU Registration Authority

ID Checkers – HR/Workforce Team	<ul style="list-style-type: none"> ○ Verify identity in a face to face meeting as per NHS Employers Identity Check standards. It must be done by examining original documents and seeing that identity relates to the individual who presents themselves at the meeting. ○ Take photographs for New Starters to be uploaded using the online portal for Smartcard application
IG Lead & SIRO	<ul style="list-style-type: none"> ○ Report all RA activity to the Executive Team in the quarterly IG Report. ○ Report all RA activity to the Board in the Monthly Operations report.
Caldicott Guardian	<ul style="list-style-type: none"> ○ Provide support and guidance
Midlands and Lancashire Commissioning Support Unit (MLCSU)	<ul style="list-style-type: none"> ○ Approve Online applications for Smartcards ○ Produce and issue Smartcards ○ Make changes to available access roles ○ Work with Badger RA Manager to maintain the protocol/arrangement ○ Inform Badger of changes in process or regulation that may impact the policies/procedure
Trainers	<ul style="list-style-type: none"> ○ Provide training for users ○ Identify RA champions
Team Leaders	<ul style="list-style-type: none"> ○ Provide guidance and coaching on Smartcard usage during Operational periods ○ Report issues identified or highlighted by staff on the Team Leader Report
Quality & Compliance	<ul style="list-style-type: none"> ○ Main contact for the MLCSU to receive exception reports. ○ Investigate breaches ○ Liaise with Badger SIRO, IG Lead and Caldicott Guardian to resolve sensitive breaches. ○ Liaise with HR and Management to deal with disciplinary issues arising from the investigations.

6 SMARTCARDS PROCEDURE

All requests for a new Smartcard under the sections below must comply with the information, evidence and identity checks contained within Appendix I.

6.1 New starters without Smartcards

1. All pre-employment checks will be made face to face by HR and access requirements will then be identified by the HR and Operations Department dependent on the individual role.
2. HR will complete the Badger User Rights Request Form, Ops-F-003, and where appropriate include the request for a Smartcard.
3. The SIRO and/or IG Lead will authorise the Badger User Rights Request Form and pass to the RA Manager
4. Where a Smartcard is appropriate to the role the new starter will be given the Badger Smartcard Guidelines Information at induction.
5. The RA Manager will complete the online application on <https://portal.national.ncrs.nhs.uk/portal/> to create an NHS Digital Identity using the same information used for the employees/clinicians pre-employment checks.
6. The Midlands & Lancashire Clinical Support Unit (MLCSU) will issue the Smartcard to the RA Manager,

7. The RA Manager will meet with the employee to enable them to electronically sign the terms & conditions and choose their pin number,
8. The RA Manager will add the authorised access rights to the staff members Smartcard and pass the Smartcard to the employee along with the guidelines for using the Smartcard

6.2 New Starters with Smartcards

1. HR will request and record the existing Smartcard number on the Badger User Rights Request Form OPS- F-003
2. Dependent on the role that the individual will perform the SIRO and/or IG Lead will authorise the Badger User Rights Request Form and pass to the RA Manager
3. The new starter will be given the Badger Smartcard Guidelines Information at induction
4. The RA Manager will return the Smartcard to the new starter with addition of the authorised access for Badger along with the guidelines for using the Smartcard.

6.3 Existing Staff with a role change requiring a Smartcard

1. The individuals Line Manager will complete a Badger User Rights Request Form OPS- F-003
2. The Badger User Rights Form is to be passed to either the SIRO or IG Lead for authorisation
3. Once authorised by the SIRO or IG Lead the form will be passed to HR/RA Identity Checkers for any appropriate identification as per NHS Employers Identity Check standards
4. HR/ID checkers will inform the individual of any additional documents required
5. Once all required identification is available and checked the RA Manager will create an NHS Digital identity on <https://portal.national.ncrs.nhs.uk/portal/>.
6. The Midlands & Lancashire Clinical Support Unit (MLCSU) will issue the Smartcard to the RA Manager,
7. The RA Manager will meet with the employee to enable them to electronically sign the terms & conditions and choose their pin number,
8. Whilst with the employee the RA Manager will add the authorised access rights to the staff members Smartcard and pass the Smartcard to the employee along with the guidelines for using the Smartcard

6.4 Personal Detail and Role Changes for Smartcard Holders

Any changes to a person's core identity attributes (Name, Date of Birth or National Insurance Number) need to go through the same face to face check with the RA Identity Checkers (HR Workforce Team) and provide appropriate documentary evidence (view only, no copy to be taken).

For Role changes the individuals Line Manager will complete a Badger User Rights Request Form OPS- F-003.

6.5 Leavers

1. HR will complete Staff Termination Form HR-F020 and record the Smartcard Issue date (if issued by Badger)
2. If the employee had a Smartcard prior to joining Badger, the Position Assignment which can be found on CIS will be recorded instead
3. Leavers who are likely to continue to remain within the NHS should retain their Smartcard following removal of all access rights granted by Badger
4. Leavers who will no longer work for the NHS should return their Smartcard for safe destruction and cancellation
5. The Staff Termination Form HR-F020 will be passed onto the Local Smartcard Administrators or to the RA Manager in their absence
6. Local Smartcard Administrator or RA Manager will remove the Badger Positions from the leavers Smartcard
7. User Access Rights database and Staff Termination Form will be updated to reflect that the necessary action has been completed.

Regular audit checks of the User Access Rights database will be undertaken to ensure compliance with authorisation procedures and integrity of Badger records.

7 NHS NUMBERS

Badger is required to improve patient safety by making effective use of the PDS and enabling consistent use of the NHS Number to reduce the number of data quality issues due to mis-associated records. It is an Information Governance requirement that the NHS number is recorded as near to the first contact with Badger and the verified NHS number is used in all communications

8 PRINCIPLES FOR THE USE OF THE NHS NUMBER

8.1 Find the NHS Number

Using the Adastral system staff issued with Smartcards authorised by Badger will be able to locate the NHS number and where appropriate, automatically populate the Adastral patient record with the demographic information retained on the spine. All staff issued with a Smartcard will receive and be trained utilising STB50 Performing a PDS Trace – Quick Reference Guide for Call Handlers and Receptionists. The latest version of STB50 can be found on Adastral/Web Communications/Training and Information/STB50.

8.2 Use the NHS Number

Badger where appropriate will use the NHS Number:

- To link a person to their health/care record
- To search for an electronic record
- To identify people presenting for care
- On electronic records, notes, forms, letters, documents and reports which include person identifiable data and are used for that person's care
- As the key identifier for service users

8.3 Share the NHS Number

Where appropriate Badger will share the NHS Number:

- With other organisations so they can use it in managing patient care
- In communications – written, verbal and electronic – during telephone calls, on all letters, referrals, forms, documents
- Internally and with other organisations that Badger may contact as part of the provision of a persons care
- And ensure that the NHS Number Is included when providing service users with any letters or forms

8.4 Duplicates or Errors identified on PDS

- After retrieving a record from the PDS, users need to confirm that it is the correct patient
- If after confirming a patient detail it is identified that information on the PDS is incorrect
- The staff member is to inform the Team Leader on duty who will record it on the Team Leader Report
- Badgers Practice Liaison Officer will contact the patients' own GP to inform them of the error, so that they are able to update their patient's information on the National Spine

9 DEPLOYMENT

Badger has deployed the use of the NHS number on its Aadastra system using the available technology solution. All relevant staff:

- Have had their online applications completed and have been issued with a Smartcard
- Have been trained in the use of the PDS system to access the PDS record
- Are aware of their responsibility in accessing the PDS and the use of Smartcards

10 INCIDENT REPORTING

Incidents will be reported to the RA Authority. The RA Authority will request for the incident to be investigated by the IG Lead for Badger.

Incidents must be raised in accordance with CG-02 procedures to enable assurance and governance is completed, investigation is thorough, findings are recorded, action taken and any recommendations arising tracked to conclusion.

Examples of incidents include:

- Smartcard or application misuse
- Smartcard theft
- Non compliance with local or national policy
- Unauthorised access to systems with NHS Digital Portal
- Any unauthorised alteration of patient data

Where appropriate the Badger Disciplinary procedure will be followed, depending on the severity and nature of the incident.

11 CONFIDENTIALITY

All users are personally responsible for ensuring that no breaches of information security result from their actions in the use of their Smartcard. Employees are reminded of their obligation under the terms and conditions of their employment and in relation to their clinical codes of conduct, in respect of any breach of confidentiality.

12 SMARTCARD TERMS AND CONDITIONS

RA Agents/Smartcard users are required to accept Smartcard terms and conditions electronically. Users who have not signed the electronic terms and conditions will not be able to use their cards.

13 GUIDANCE

This document has a Glossary and all Staff issued with a Smartcard are required to be familiar with the reference material to ensure full understanding of the terms used.

All applicants are responsible for ensuring that they understand that they are committing to the Badger obligations identified in this document and those referenced by this document. RA Management is responsible for ensuring that Staff are trained and have achieved the required standard of knowledge prior to accessing the spine and PDS.

All Staff/Users

- If an application is successful, an individual will become an authorised user of the NHS Care Identity Service applications and will be issued with a Smartcard. This will contain a digital certificate and has a photograph of the individual printed on it along with the Unique User Identification (UUIID). The Smartcard will provide access to certain patient data in accordance with the access profiles approved by Badger.
- The personal data which provided is required by the local Registration Authority to verify the identity of the individual and to confirm eligibility for registration. No personal data will be copied however all required paperwork must be shown in the original format to initiate the smartcard application.
- No individual is authorised to use NHS Care Identity Service applications unless a Smartcard has been issued to that person
- If the job role changes and/or any of access profiles require amendment, contact should be made with the RA Manager who is able to make these changes via the online portal
- Any name change should be notified to the RA Manager who will submit a change request via the online portal.

Notice to applicants on the collection of personal data

In accordance with the requirements of Department of Health and Social Care, the personally identifiable information (PII)(as defined in the Data Protection Act 2018) that the applicant provides 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 Identity Service applications .

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 2018as 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 2018, 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 RA or Sponsor in relation to any queries they may have in connection with this application.

13.1 Terms & Conditions

The applicant, by issue of a Smartcard agrees to the following terms and conditions applying to them as the authorised holder the Smartcard:

1. Consent to the face to face viewing and 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 this application is accurate. I agree to notify my local Registration Authority immediately of any changes to this information;
3. 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 Identity 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. Agree that I will only use my Smartcard, the NHS Care Identity Service applications and all patient data in accordance with The NHS Confidentiality Code of Practice (as available on the www.dh.gov.uk site) and (where applicable) in accordance with my contract of employment or contract of provision for service (which ever is appropriate) and with any instructions relating to the NHS Care Identity Service applications which are notified to me;
7. Agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate my Smartcard, NHS Care Identity 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 Identity 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 Identity

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 Identity Service applications. The Registration Authority is not responsible for the availability of the NHS Care Identity Service applications 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 myself 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.

13.2 Glossary of terms

- **Access Profile** means the specific areas of NHS Care Identity Service applications which the user is authorised to access.
- **Applicant** means an individual who is in the process of registering to become an authorised user.
- **Authorised user** means a person who is authorised to use the NHS Care Identity Service applications and has been issued a Smartcard.
- **Certificate** means An X.509 public key certificate binds an identity and a public key. The public key together with the identity and related information are digitally signed with the private signing key of the Certification Authority that issues the certificate. The format of the certificate is in accordance with ITU-T Recommendation X.509.
- **Data Protection Act** means the Data Protection Act 2018 as amended and supplemented from time to time.
- **NHS Care Identity Service applications** are those applications provided by HSCIC as part of the National Programme for Information Technology
- **Passcode** means a **alpha numeric set of characters used to permit access to NHS CRS functionality.**
- **Personal Data** means data from which an applicant can be identified, as defined in more detail in the Data Protection Act.
- **Registration Authority (RA)** means any entity that is appointed by the Department of Health as being responsible for the identification and authentication of applicants.
- **Smartcard** means the card issued to an authorised user which enables access to NHS Care Identity Service applications.
- **User's Unique ID Number** means the number to the left of the photograph on the Smartcard, underneath the chip, also referred to as the UUID.
- **Smartcard Serial Number** means the number on the back of the Smartcard which is the manufacturer's card identifier.
- **Sponsor** means the individual identified by the organisation who has been assigned to approve access to information and functionality of NHS Care Identity Service applications

14 APPENDIX I – SMARTCARD DOCUMENTATION REQUIREMENTS

14.1 Identifiers

One of the following:

- National Insurance Number
- Passport Number
- Driving Licence Number

14.2 Applicant Contact details

- Telephone Number
- Mobile Number
- Email

14.3 ID card

- Passport sized photographs (Company ID Photo can be used)

14.4 Identity Verification

- 2 x photographic identification documents and one document showing the applicant's address,
- or 1 x photographic identification document and two documents showing the applicant's address

14.5 Acceptable Documents

- Utility Bill (no mobile phone bills & bill must have been issued within last 3 months)
- Financial Statement
- Driving License
- Benefit statement from DWP
- Confirmation from Electoral Register Search
- HMRC tax notification (not P45 or P60)
- Local Authority Tax Bill
- Local Council rent card or Tenancy Agreement
- Mortgage statement from recognised lender