NHS

South East
Commissioning Support Unit

REGISTRATION AUTHORITY SMARTCARD USE POLICY (INCLUDES MISUSE)

Version 3

SOUTH EAST / CSU

Document Name	Registration Authority Smartcard Use Policy (includes Misuse)		
Location	Susi Policy Library		
Consultation	Warner Baker (Health and Social Care Information Centre); SECSU Performance, Delivery & Internal Assurance Group		
Approved by:	PDIAG	Date:	19.1.16
Supersedes:	Legacy Registration Authority Policies		
Description:	To inform staff on the process for the issuing of, management of and use of smartcards		
Audience:	All individuals who possess a smartcard and working on behalf of the organisation		
Contact Details:	Registration Authority Manager		

Version	Date	Author	Approver	Reason
Number	Date	Individual	Insert group or n/a	First draft / minor corrections / (insert) detail added etc.
1.0	9.12.14	Registration Authority Manager	Information Governance Steering Group	
1.1	17.2.15	Registration Authority Manager	Internal Assurance Group	Revisions required
2.0	24/2/2015	Registration Authority Manager	Internal Assurance Group	Ratified
2.1	19/1/16	Registration Authority Manager	PDIAG	Revision of policy to reflect merger to South East CSU

1.0 Introduction

1.1 Policy Statement

The Organisation will use all appropriate and necessary means to ensure that it complies with best practice for the issuing and monitoring of smartcards.

1.2 Rationale

Patient information must be kept confidential and secure. Having a common and rigorous approach to how users register, and are given access, to the NHS Care Record Service and other Health and Social Care Information Centre services is an integral part of protecting the confidentiality and security of every patient's personal and health care details. The NHS takes its commitment to protecting patient confidentiality seriously, and has set out the principles that will govern how patient information is held in the NHS Care Records Services and the way it is shared, in the NHS Care Record Guarantee (see the Information Governance pages on the SE CSU Intranet). All staff in the NHS are bound by this Guarantee.

This Policy sets out South East Commissioning Support Unit's (SE CSU) position with regard to the use of smartcards.

The purpose of this Policy is to ensure that smartcards are used in an appropriate way, and to make SE CSU supported organisations aware of what SE CSU considers to be an acceptable use of the cards. This Policy also sets out how smartcard usage is monitored by NHS England, SE CSU, CCGs, and the Health and Social Care Information Centre.

1.3 Smartcard use

Prior to being issued with a smartcard, users are required to read a set of terms and conditions laid out in the RA01part A (see Appendix B), RA01 short from (see Appendix C), RA02 (see Appendix D). When a user logs in with their smartcard terms and conditions appear on the screen by entering their pin they are agreeing to these. Users are required to familiarise themselves with the content of the terms and conditions of use to avoid inadvertent breaches which could compromise patient information.

The user should use the smartcard only in the normal course of employment together with systems where access is restricted to smartcard users.

Smartcard Users are responsible for either terminating the session (logging off) when finished or locking the computer when temporarily leaving it unattended.

Passcodes must not be written down or become known by anybody other than the legitimate owner.

At no point should smartcards be left in readers while users are away from equipment.

2.0 Scope

This policy applies to all smartcard users within SE CSU supported organisations:

- A failure to comply with this Policy may result in disciplinary proceedings by the user's organisation. Smartcard access may be restricted or denied in order to safeguard patient confidentiality.
- All such breaches will be reported to SE CSU supported organisational Line Managers and/or Sponsors and if deemed necessary reported to the Area Teams (AT's).
- All smartcard misuse incidents will either be marked up as a training issue or reported to the AT's for further investigation and or disciplinary action being recommended.
- Severe misuse will be classed as an act which could directly present a risk to a patient.
- If you are unclear about any aspect of this policy you must consult your manager or local Registration Authority Team..

3.0 Equality Analysis

The Organisation aims to ensure that its policies meet the needs of all staff and patients, and that they do not disadvantage any groups or individuals.

Equality Impact Assessments (EIA) provide a systematic way to ensure legal obligations are met and are a practical way of examining new and existing policies and practices to determine what effect they may have on equality for those affected by the outcomes.

The duty to undertake EIAs is a legal requirement of Race, Gender and Disability Equality Legislation. In order to ensure all groups receive equitable attention, EIAs should also be carried out in respect of Age, Sexual Orientation, Religion and Belief and Human Rights, cross-referenced to socio-economic and geographical (deprivation) factors.

The purpose of EIAs is to identify and address real or potential inequalities resulting from policy and practice development. Through this process an Organisation gains a greater understanding of its functions and is more able to be an equitable employer and service provider. (Equality Impact Assessment - appendix F)

4.0 Responsibilities

4.1 Senior Partner – Business Services

The Senior Partner – Business Services holds executive responsibility for ensuring that this Policy is implemented and monitored. Operational responsibility sits with the RA Manager.

4.2 Registration Authority Manager

Ultimate responsibility for Registration Authority (RA) rests with the RA Manager and Managing Director of the Organisation, but all staff members who own a smartcard are responsible for the safety and usage of the smartcard.

Managers at all levels are responsible for ensuring that the staff for whom they are responsible are aware of and adhere to this policy. They are also responsible for ensuring staff are updated in regard to any changes in this policy.

An organisation's RA works, as a minimum within the governance framework identified in the organisation's Information Governance Toolkit.

The responsibilities the RA Manager has for their organisation are:

- Ensure that the National Registration policy and processes are adhered to and that any local processes support the National policy and processes Registration Authorities Operational Process and Guidance – NPFIT – SIGOV-0114.10 Version 4.
- To appoint, and register RA Agents (where permitted under governance arrangements), ensuring there are sufficient resources to operate the registration processes in a timely and efficient manner.
- Ensure users have only one NHS CRS smartcard issued to them showing their User's Unique Identifier (UUID) and photograph, and that users are aware of their responsibilities relating to Information Governance and smartcard use. The issue of more than one NHS CRS smartcard to a user is not permitted.
- Implement an Audit Policy and identify a secure locked area for the storage of all registration and associated information in accordance with the Data Protection Act 1998. This includes RA Manager, RA Agent, and sponsor assignment documents, RA forms, RA reports, and inter-organisation agreements. All RA forms must be clearly marked with the user's UUID number and filed in a designated area. Once audited ensure that all paper records are archived appropriately.
- Following the implementation of UIM [User Identity Management] (March 2011), the first end to end electronic RA application, and now its successor CIS (Care Identity Service), RA is a fully automated process, without the need for paper. Any earlier RA paper records need to continue to be securely stored in a locked cabinet.
- Report all RA related security incidents and breaches to the NHSE
- Escalate all queries that cannot be resolved locally to the next level in the RA hierarchy

- Disseminate national RA information to interested parties. For example, communicate PBAC and access control information to sponsors
- Ensure there is a sufficient supply of smartcards and RA hardware, including access to the Card Management System (CMS) for sponsors (smartcard unlocking and certificate renewal), and communicate technical requirements to the Information Technology team
- Register RA Managers who have letters of appointment from organisations in the South East CSU family
- Ensure there is a process for the renewal of smartcard certificates
- When performing RA Agent duties, observe the same responsibilities as the RA Agent
- Ensure users are aware of the self-service functionality available to them, including how to unlock smartcards, reset passcodes, and renew smartcard certificates
- Consider and apply Restriction Sets that restrict which attributes an RA Agent can grant
- Ensure RA Manager contact details including email address and telephone number is recorded in the Spine User Directory

4.3 Registration Authority Agents

- Where possible maintain a list of active sponsors and any restrictions to assist the registration of users
- Ensure RA Agents are adequately trained, maintain an up-to-date Personal Development Plan and be familiar with the local and national RA policies and processes
- Register RA Agents when deemed appropriate
- Be familiar with the organisations IG Toolkit requirements
- Ensure users have only one NHS CRS smartcard issued to them showing their User's Unique Identifier (UUID) and photograph, and that users are aware of their responsibilities relating to Information Governance and smartcard use. The issue of more than one NHS CRS smartcard to a user is not permitted.
- Implement the process identified by Registration Authorities Operational Process and Guidance – NPFIT – SIGOV – 0114.10 version 4.
- Adhere to the Audit policy outlined in the RA Policy document
- Report incidents of misuse, anomalies, or problems to the RA Manager
- Renew a user's smartcard certificates if confident of the user's identity; the local RA should encourage users to self-renew their smartcard certificates via the Self Service Portal
- Unlock a user's smartcard and reset logon Passcodes when necessary

- Ensure users are aware of the self-service functionality available to them, including how to unlock smartcards, reset passcodes, and renew smartcard certificates
- Ensure RA Agent contact details including email address and telephone number, are recorded in the Spine User Directory
- For RA Forms or UIM ensure that the Registration Authorities Operational Process and Guidance - NPFIT-SIGOV-0114.10 Version 4 is followed correctly

4.4 Sponsor

- Ensure sponsors are adequately trained, and where necessary know how to unlock smartcards, add and remove starters and leavers
- Assist sponsors in understanding the Position Based Access Control (PBAC) model and in finding information about users they sponsor
- Authorise and approve user registrations
- Be familiar with the different types of access profiles to approve
- Ensure that access profiles submitted to a Registration Authority follow the current National PBAC Database
- Work with RA Agents to maintain access to NHS CRS compliant applications within their area of responsibility that is consistent. This includes access profile change and removal, and the revocation of smartcards and smartcard certificates
- Be familiar with the applications they sponsor users for within the organisation
- Renew a user's smartcard certificates if confident of the user's identity. Users should be encouraged to self-renew their smartcard certificates via the Self Service Portal
- Unlock a user's smartcard and reset passcodes with the user present. Users should be encouraged to set their passcodes via the Self Service Portal, and unlock their smartcards when necessary via the Smartcard Service Centre

4.5 All staff with Smartcards

All staff with smartcards are responsible for ensuring that they have read and adhere to this policy

5.0 Smartcard ownership

- The smartcard issued to the user is the property of the NHS
- The smartcard should be returned to the NHS if the user leaves the NHS

- The smartcard should not be purposefully damaged or defaced in any way
- The smartcard and associated passcode should be kept private and secure and retained by the user only
- Smartcards are issued with personalised certificates, valid for 2 years
- Users are issued with a personal Unique User Identifying number (UUID)
- A User can only have one smartcard. In the event of having more than one, the Registration Authority should be contacted
- Any smartcard losses must be immediately reported to the Registration Authority

6.0 Security

Users are required to set a personal passcode (4 to 8 characters in length, alpha/numeric and is case sensitive) when they receive their smartcard. This provides an additional layer of security to help prevent unauthorised access to the system and the information held within it.

Smartcard users should always protect their passcode by keeping them private and not disclosing them to anyone.

Smartcards should be kept safe – as it provides access to sensitive patient data and must be kept secure at all times.

Smartcards should never be shared or used by anyone else – user details are logged at all times when using smartcard enabled systems and activity tracked to the owner of the card.

Automated systems are used to monitor and record activity to audit the effective operation of the systems and for other lawful purposes. Individual users can be identified from the information recorded and this information will be accessed and used to investigate allegations of breaches of security and/or confidentiality.

The RA Manager should be notified IMMEDIATELY in the event of the loss, disclosure or suspected theft of your smartcard – it will be cancelled remotely and a new one issued.

Card holders are not permitted to have more than one card or user's unique ID number (UUID).

7.0 Unacceptable use of smartcards (Misuse)

Types of Misuse can include (but are not limited to):

- Smartcard or application misuse
- Theft of a smartcard
- Non-compliance of a local or national RA policy e.g. card sharing, password sharing
- Any unauthorized access of national applications
- Any unauthorized alteration of patient data
- Smartcard left unattended in the reader. The card should be removed and handed to the person's manager
- Inappropriate issuing of cards by the RA Manager/RA Agents
- False registrations – this will be escalated to the NHS Counter Fraud Team immediately
- Excessive card losses i.e. more than 2 Smartcards reported lost within any 12 month period

Breach of Confidentiality will be reported to the NHSE for onward investigation and could result in disciplinary action being taken against the user.

8.0 Monitoring of smartcard use

Spot checks may be undertaken by any organisational sponsor or user to ensure that card sharing is not occurring.SE CSU in agreement with supported organisations may monitor smartcard use at any time without prior notification. Such monitoring would occur for reasons including, but not limited, to the following:

- Technical maintenance or problem resolution.
- During an investigation into alleged misconduct, including unauthorised or excessive use of the smartcard applications, or in connection with the prevention or detection of criminal or illegal actions.
- During an enquiry concerning compliance with this Policy.

Major misuse will be reported to the NHSE by the RA Manager

9.0 Authorisation to use smartcards

Sponsors are responsible for ensuring that staff who require access to smartcard compliant systems and/or applications are sponsored for registration, have the appropriate access to the CRS systems through smartcard position assignment to fulfill their role. This should be undertaken when a new member of staff joins a department/practice.

The new user's details are entered in CIS by a member of the RA Team as part of the registration process and a smartcard issued.

Smartcard applicants will be required to provide three forms of personal identification as part of the RA process (failure to provide 3 forms of ID will result in the user not being able to be registered until such time as the ID requirements can be provided). Acceptable forms of ID are described in Appendix A.

It is the Sponsor's responsibility to inform the RA Agent/Manager of any required changes to access positions and profiles. SE CSU leavers' details will be forwarded to the RA Team by Human Resources and / or Managers. SE CSU supported organisations Sponsors are required to ensure their staff lists are kept up-to-date on the Spine User Directory.

10.0 Pharmacy smartcards and 5 "F"s code

The SE CSU RA team will issue smartcards to pharmacy staff working at sites within the SE CSU geographical area which currently covers Kent and Medway, Surrey, Sussex and London CCGs. Locum Pharmacist\Dispensers may be issued with the locum five "F"s code only if their locum status can be verified and have a registered home address within the SE CSU geographical area. Please note if a pharmacist works as a regular locum at up to 10 sites, then they will have all sites added to their smartcard rather than be given the locum code. The five "F"s code will only be issued in exceptional circumstances and at the discretion of the SE CSU RA Manager.

11.0 Training

The RA Team will provide training on how to use the smartcard when it is delivered to the user. Further requests for training can be made by contacting the SE CSU Service Desk.

12.0 Communication

This Policy will be communicated effectively to all staff via SE CSU intranet. SE CSU RA Team will ensure that all managers/Sponsors are aware of their responsibilities.

13.0 Reference documents

This Policy is supported by the following policies and procedures

- Information Security Policy.
- Data Protection and Confidentiality Policy.
- Data Protection Act 1998 and all relevant legislation.
- Computer Misuse Act 19?
- Verification of Identity Checks – http://www.nhsemployers.org/primary/Employment-checks.cfm

14.0 Review

14.1 Next formal review

Review will take place on the first anniversary of adoption or when there is a change of national policy

14.2 Latest version

The audience of this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available at the location indicated in the document control section of this document. Those to whom this protocol applies are responsible for familiarising themselves periodically with the latest version and for complying with protocol requirements at all times

Appendix A; Acceptable forms of Identity (ID)

e-GIF level 3 Identity proof

Acceptable Photo Personal Identity Documents.

Current UK, EU and other nationalities passports. Passports of non-EU nationals should contain UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK. In cases of doubt or suspected fraud, enquiries should be made with the nearest Immigration Service Office for advice;

Current EU and non-EU Photo-card Driving License (providing that the person checking is confident that non-UK Photo-card Driving Licenses are genuine).

Acceptable Non-Photo Personal Identity Documents.

- 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;

Active in the Community Documents

Active-in-the-community documents shall have all the following properties:

1. Documents must be issued by a trusted source;

2. Each document must be an original or notarised document, not a photocopy;

3. The document must be valid at the time it is used (i.e. it must be current/not more than 3 months old);

4. The document must contain the individual's name;

5. The document must attest to at least one of the following:

    the individual's address;

    the individual's standing in the medical community (e.g.: license to practice, or long-term employment by a healthcare organisation);

6. The document must be difficult to forge.

Acceptable 'Active in the Community' Documents

- To confirm address, the following documents are acceptable:
- 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 license (if not already presented as a personal ID document);
- Current Full UK driving license (old version) (if not already presented as a personal ID document);
- 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.

The applicant shall provide either:-

2 forms of personal photo ID and 1 active in the community document;

or

1 form of personal photo ID and 2 active in the community documents;

or

2 forms of personal non-photo ID and 2 active in the community documents.

Appendix B: RA01

RA01 Short Form Conditions –

Registration for NHS Care Records

Service application's Smartcard

Please note:

This document should be read by everyone prior to completing an RA01 Short Form and is going to be issued a smartcard. If there are any queries regarding this document please contact your Registration Authority.

Guidance

- This document has a Glossary and you should reference it to ensure you fully understand the terms used.
- All applicants need to be aware that by signing the RA01 Short Form they are committing to the obligations identified in this document and those referenced by this document.
- Once you accept these conditions, you need to have the RA01 Short Form approved by a Sponsor. If you do not know who your Sponsor is please contact your local Registration Authority.
- If your application is successful, you will become an authorised user of the NHS Care Records Service applications and will be issued with a Smartcard. This will contain a digital certificate and has your photograph printed on it along with your Unique User Identification (UUID). Your Smartcard will provide you with access to certain patient data in accordance with the access profiles approved by your **Sponsor**(s) on a RA02 form.
- These RA01 conditions contains a number of obligations relating to your use of the Smartcard and the NHS Care Records Service applications and you should review these sections carefully.
- The personal data which you and your sponsor provide on the RA01 Short Form is required by your local Registration Authority to verify your identity and to confirm that you are eligible for registration. All personal data held about you and your sponsor will be processed in accordance with the Data Protection Act.
- You are not authorised to use NHS Care Records Service applications unless a Smartcard has been issued to you.
- If your job role changes and/or any of your access profiles require amendment, you should contact your **Sponsor** who will need to complete an RA02 Profile Additions and Modifications form. This is available from any Registration Authority.

- If your name changes you will need to complete and submit an RA05 Change of Details form and notify your local Registration Authority.

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 provides on the RA01 Short Form (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 .

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

By signing the declaration set out in the RA01 Short Form, I, the applicant:

1. consent to the collection 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 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. 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 (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 (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 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.

RA01 - Glossary of terms

- **Access Profile** means the specific areas of NHS Care Records 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.
- **Application for registration** means the RA01 Form, completed by an applicant and a sponsor.
- **Authorised user** means a person who is authorised to use the NHS Care Records 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 1998 as amended and supplemented from time to time.
- **NHS Care Records Service applications** are those applications provided by HSCIC as part of the National Programme for Information Technology
- **Passcode means an 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 Records 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 Records Service applications

Appendix C

Applicant's Name:
RA01 Short Form Part 1
Registration for NHS Care Records Service applications
Please note:

All applicants **must have read and agreed** to the conditions detailed in the **RA01 Short Form Conditions Version 1.2.** If you do not have a copy please request one from your Registration Authority **before** completing this document. All your personal data is processed in accordance with the Data Protection Act 1998 but it is important that you read the full "Notices to applicants on the collection of personal data" set out in the RA01 Short Form Conditions.

Guidance

This form is made up of the following two parts:

- **Part 1** to be completed by you, the **applicant,** who requires access to NHS Care Records Service applications;
- **Part 2** to be completed by your **Sponsor & RA**. Your **Sponsor** will probably be your Clinical Manager/Line Manager or Supervisor.

Please complete the following details:

Title (e.g. Dr, Mr, Mrs etc.):	
First Name:	
Middle Name(s):	
Family Name (Surname):	
Preferred Full Name:	
National Insurance Number:	
Date of Birth[1]:	
Post title:	
Occupation:	
Registering Organisation Name/Code:	
Site Name[2]:	
Telephone number[3]:	
Email address[3]:	
Previous Registration Details:	

Key 1. Only captured for the purposes of e-GIF level 3 compliance

2. The name of the site where the applicant usually works at the time of registration

3. Either NHS email address or mobile number required to utilise Self-service Centre functionality e.g. Self-Unlock. Additionally required for all Registration Authority Managers, Agents and Sponsors

Applicant's details and declaration

I have read and agree to be bound by the terms and conditions stated in the RA01 Short Form Conditions version 1.2 or later:

Applicant's signature:_____

Date (dd/mm/yyyy):

Applicant's Name:

RA01 Short Form - Part 2 **Sponsor use only**

Sponsor's declaration

I confirm that the **Applicant** specified in Part 1 should be issued a Smartcard.

Sponsor's signature: _____

Sponsor confirmation of identity declaration

NOTE: this section should only be signed in the presence of an RA Manager or Agent

(The applicant will, additionally, be required to produce two forms of acceptable non-photographic proof of personal identification and two confirmation of address documents).

I confirm that the **Applicant** does not have any acceptable Photographic Identity Documents; I have known the individual for more than three years and I confirm the identity of this applicant.

Sponsor's signature: _____

RA use only

Registering Organisation Name			
	Sponsor	**RA Agent/Manager**	
Name			
Smartcard UUID			
Date completed			
Sponsor present	**Yes/*** **No***	**Passport, Photo card Driving Licence, or Birth cert. no.**	
Sponsor confirms identity?[4]	**Yes/*** **No***	**Confirmation of address seen?**	**Yes/*** **No***
Signed statement and signed passport photo seen?	**Yes/*** **No***		
Issued Smartcard UUID number:			

4. Where sponsor confirms identity then 2 forms of acceptable non-photographic proof of personal identification and two confirmation of address documents must be seen by the RA
***Delete where applicable**

Appendix D

Applicant's / User's Name:
RA02 Form – User Profile Additions and Modifications Form for NHS CRS applications

Please note:

- This form can be completed online but must not be submitted online as it requires your signature.
- When completed, **print** the RA02, sign and send to your local Registration Authority.
- Indicate which Organisation, Job Role(s), Area(s) of Work Activity(ies), and Workgroups(s) **or** Position are required to be added or removed for the user. Please complete an additional RA02 if there is not space on this form
- Enter Add/Remove/Modify to indicate action intended and strike through all blank fields.

User Name:	User Smartcard UUID number:

Organisation	Code	Occupation	Action

Position Name (If this is completed skip to start date)	Action

Job Role	Code	Action

Area of Work	Code	Action

Activity	Code	Action

Work Group Name	Action

Start Date*	dd/mm/yy	hh:mm	End Date*	dd/mm/yy	hh:mm

* If the dates are blank the profile starts now and ends never. If the Start or End Date is set the RA must ensure the appropriate action is taken e.g. if the End date is set, the profile on this form must be removed when the End date/time has passed.

	Sponsor (Sponsor to complete below)	RA Agent/Manager (RA to complete below)
Name		
Smartcard UUID		
Date completed		

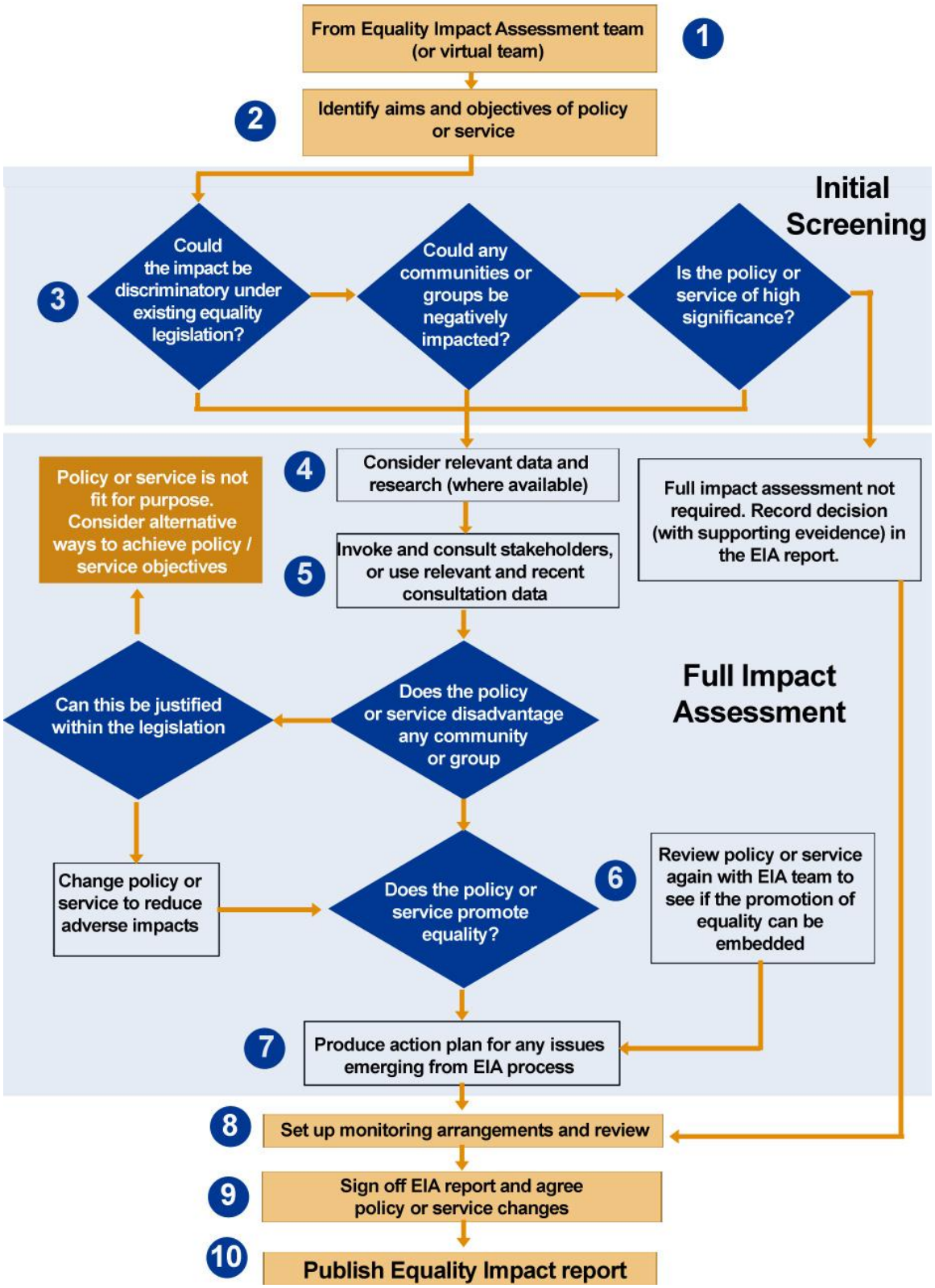
Sponsor's declaration:

I confirm that the **Organisation**, **Job Role(s), Area(s) of Work Activity(ies), and Workgroups(s) OR Position(s)** detailed in this RA02 form are correct and should be applied by the Registration Authority to the user detailed above.

Sponsor's signature: _____

Notes to Registration Authority Agents: Ensure the form has been completed by one of your local organisation Sponsors or a Sponsor from an organisation you have an appropriate agreement with. If this is not the case then do not action and advise the requestor. If in doubt contact your RA Manager. Ensure RA and Sponsor changes are carried through to CMS as well as SUD.

Appendix E: EIA



Equality Impact Assessment Report Outline

Remember that your EIA report should demonstrate what you do (or will do) to make sure that your service/policy is accessible to different people and communities, not just that it can, in theory, be used by anyone.

1. Name of Policy or Service

Smartcard Use Policy

2. Responsible Manager

Registration Authority Manager

3. Date EIA Completed

3. Description and Aim of Policy/Service (including relevance to equalities)

To ensure that the Organisation adheres to its obligations

5. Brief Summary of Research and Relevant Data

A Guide to Equality Impact Assessment

6. Methods and Outcome of Consultation

Information Governance Steering Group, Integrated Governance Committee, HR, Senior Management Team, SCC, Staffside, Communications

7. Results of Initial Screening or Full Equality Impact Assessment:

Equality Group	**Assessment of Impact**
Age	
Gender	
Race	
Sexual Orientation	
Religion or belief	
Disability	For staff who have visual impairment, updating staff re requirements during dissemination, Policy can be described to staff verbally. Managers can contact Communications re the possibility of a Braille version
Deprivation	

Dignity and Human Rights	Staff are treated as individuals with individual needs and requirements which are taken into consideration when policies are disseminated. Staff were consulted via SE CSU intranet, SCC

8. Decisions and/or Recommendations (including supporting rationale)

9. Equality Action Plan (if required)

10. Monitoring and Review Arrangements (including date of next full review)

The policy will be reviewed one year from the date of issue, thereafter it will be reviewed every 3 years. The policy will be monitored by the Information Governance Steering Group to ensure it continues to adhere to the Freedom of Information Act 2000.

Appendix F: Contact Details

Job Title	Responsible for
Senior Partner – Business Services	Executive responsibility
Partner – Head of ICT	Strategic direction for IT
Registration Authority Manager	Assisting the IT Manager with user registration
Head of Information Governance	Managing the development and implementation of Information Governance Projects