East of England Ambulance Service NHS Trust

Registration Authority Smartcard Policy

Document Reference	POL044
Document Status	Approved
Version:	V5.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
Final V1.0	February 2011	Approved by IGG
Final V2.0	March 2013	For approval by EMT
V2.0	23 February 2015	Review date extension agreed by IGG following approval by EMB
V3.0	17 December 2015	Review date extension agreed by IGG and approved by ELB
V4.0	April 2016	For Approval by Executive leadership Board
V4.1	May 2018	Presented to IGG following minimal changes made to reflect reference to change in data protection legislation to reflect new corporate template
V5.0	7 June 2018	Approved by SLB

Author: Information Governance Manager	
Document Reference	Directorate: Strategy and Business Development
Recommended at date	Information Governance Group 22 May 2018
Approved at date	SLB 7 June 2018
Review date of approved document	7 June 2020 unless HSCIC changes occur earlier.
Equality Impact Assessment	Completed
Linked procedural documents	None
Dissemination requirements	All personnel via staff bulletin and intranet
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

1. Background

In autumn 2015, the NHS set out a bold vision for the future, outlining what changes were needed to bring the NHS into the 21st century and support new and improved models for delivering patient care. In November 2015, the National Information Board in health and care published a document entitled “Personalised Health and Care 2020: a Framework for Action” which set out how more effective use of technology and data would enable the vision to be realised.

The NHS is committed to making all patient and care records digital by 2020, meaning that whenever and wherever patients access services those caring for them have all of the relevant information available at their finger-tips – from diagnostic tests and clinical notes to case histories and records of personal preferences.

The National Information Board will help take forward the ambitions of the Care Act 2014, the Government Digital Strategy (2013), the Department of Health’s Digital Strategy: Leading the Culture Change in Health and Care (2012) and the proposals in the Department of Health’s Power of Information (2012). It has pledged to build upon the commitment to exploit the information revolution outlined in the NHS’s Five Year Forward View.5

As more national applications, services and directories which support the health and social care of patients are released in line with these Government documents the Registration Authority (Health Social Care Information Centre - HSCIC) with its power to approve delegated authority to local organisations to operate a local Registration Authority Service will play an increasingly vital role to provide secure access to these applications to meet the challenges of improving health and providing better, safer, sustainable care for all.

There is a single National Registration Authority (Health Social Care Information Centre - HSCIC) and the Trust is registered with it to be able to operate a local Registration Authority Service on a delegated authority basis. In order to operate an RA service the Trust must ensure that all aspects of Registration Authority services and operations are performed in accordance with the HSCIC RA policy.

The Digital Delivery Centre (DDC) at the Health and Social Care Information Centre (HSCIC) oversees a number of key national applications and infrastructure for health and social care IT, including the Spine. It connects clinicians, patients and local service providers throughout England to a number of essential national services including the choose and book system, electronic prescription service, summary care record, e-referral service and other local patient care information technology systems.

2. Introduction

The Trust delivers emergency, urgent and primary care services throughout the East of England operating from 140 sites. It therefore needs to provide its staff with access to patient information through spine and other IT related systems. The Trusts local Registration Authority Service was set up in 2012 to manage this process.

3. Purpose

The purpose of this Trust policy is to provide operational and procedural process guidance so that the Trust meets the minimum national requirements outlined in the HSCIC Registration Authority Policy. It will also highlight roles and responsibilities in relation to the RA process and explain how these roles link into existing Trust policies, practices, and systems.

The RA policy outlines the agreed processes required to support the interface between the ESR (Electronic Staff Record) and the Care Identity Service and provides guidance to ensure that relevant applications continue to be operated safely and efficiently through future developments ensuring that it meets all statutory requirements and those relating to the IG Toolkit.

This policy applies to all Trust employees, including those working at the Trust on an honorary, contractual, or temporary basis (i.e. locums, bank and agency staff). This will include any employees who are on secondment to a role that requires access to Smartcard-based systems.

4. Roles and Responsibilities

4.1 Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that patient rights to confidentiality are protected. The Department of Health also governs the role and responsibilities of Caldicott Guardians, who protect the confidentiality of patient information in every NHS organisation and oversee arrangements for the appropriate use and sharing of information; further details can be found in the Department of Health's Caldicott Guardian Manual 2014. The Trust's Medical Director is the Caldicott Guardian.

4.2 Senior Information Risk Owner (SIRO)

The RA function is embedded in the Trust's Information Governance structure, for which the SIRO is responsibility.

4.3 Executive Sponsor

The Director of Nursing Quality and Clinical Commissioning is the Executive Sponsor for the Trust's RA service. The Trust has an integrated RA with HR as part of its approach to Integrated Identity Management to remove duplication of identification checks and achieve associated efficiency gains. Therefore the Director of Nursing Quality and Clinical Commissioning will work closely with the Director of Human Resources.

4.4 HR Director

The Director of Human Resources is the Executive Sponsor for the ESR Interface which is linked to the RA Care Identity Service, also known as the Integrated Identity Management system (IIM) which combines the separate processes, maintained within Registration Authority and Human Resource teams, for capturing and managing an employee's identity and access to the Spine.

4.5 HR RA Agents

The HR RA Agents are staff who have been appointed to approve access to information and functionality of the RA service by granting approval of appropriate access rights so that staff have appropriate access based on the position they are employed to perform.

All Spine enabled applications use a common security and confidentiality approach. This is based upon the healthcare professional's roles, areas of work, and activities that make up the required access and the position they have been employed to undertake. Access Control Positions provide staff with the access to patient information required to perform their role within the organisation, satisfying both clinical and Information Governance needs.

Identity assurance is increasingly important for the NHS, both for recruitment and for access to the Spine. Identity must be verified in a face to face meeting. It must be done by examining original documents and seeing that identity relates to the individual who presents

themselves at the meeting. The documents that can be used to verify an identity have been jointly determined by HSCIC and NHS Employers and the list is contained in the NHS Employers 'Verification of Identity Checks' standard which can currently be found at http://www.nhsemployers.org/casestudies- and-resources/2009/01/verification-of-identity-checks.NO other documents are approved for verification of identity, including those contained within other NHS Employers standards.

Identity is required to be verified to the previous inter-governmental standard known as e-GIF Level 3. This provides assurance that the identity is valid across any organisation an individual works within. The new Care Identity Service application enforces a new user's identification to be verified to e-GIF Level 3 before a NHS Smartcard can be issued to that user. Failure to comply with the NHS Employment Check standards could potentially put the safety, and even the lives, of patients, staff and the public at risk. RA should verify that the applicant's current UK Driving Licence photo card at the face to face meeting is a true likeness of the applicant

The HR Agents will ensure that any relevant HR policies and procedures reference the Registration Authority, e.g. the Recruitment and Selection Policy. The HR department will ensure that reference to the RA function is included in the Trust's Corporate Induction programme.

4.6 The RA Manager

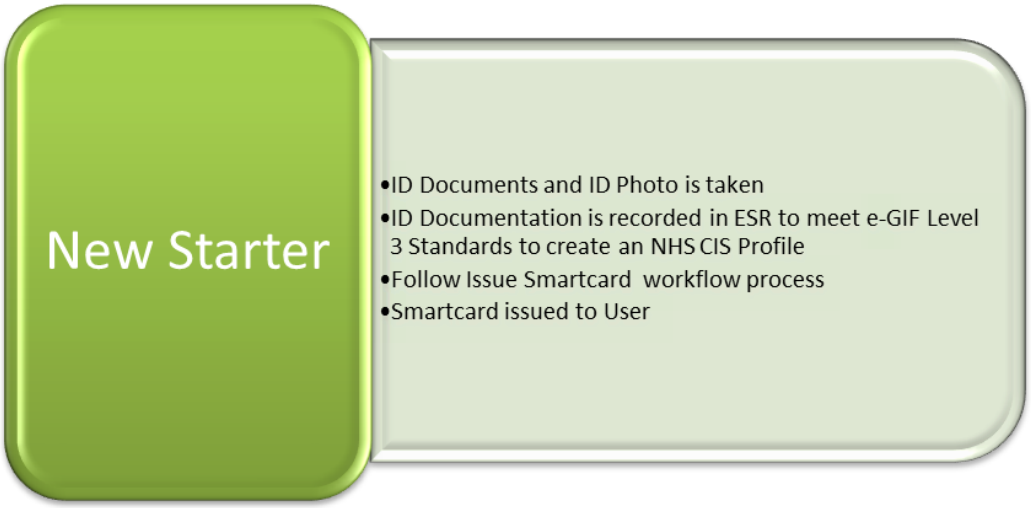
The Information Governance Manager is the Trust's RA Manager and has overall responsibility for local RA processes and governance and will work closely with the Head of IM&T to ensure a safe and secure RA service.

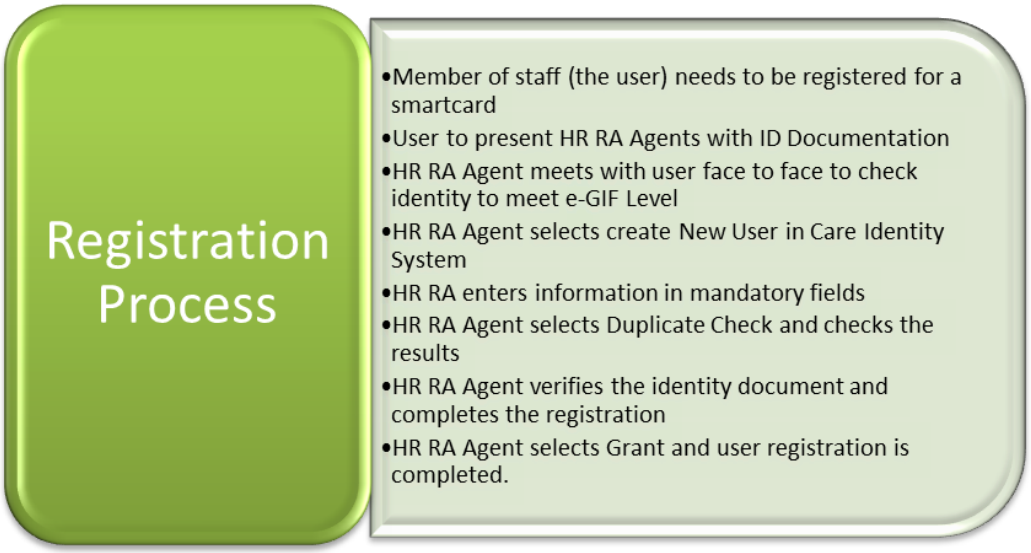
The RA Manager has a number of responsibilities including:

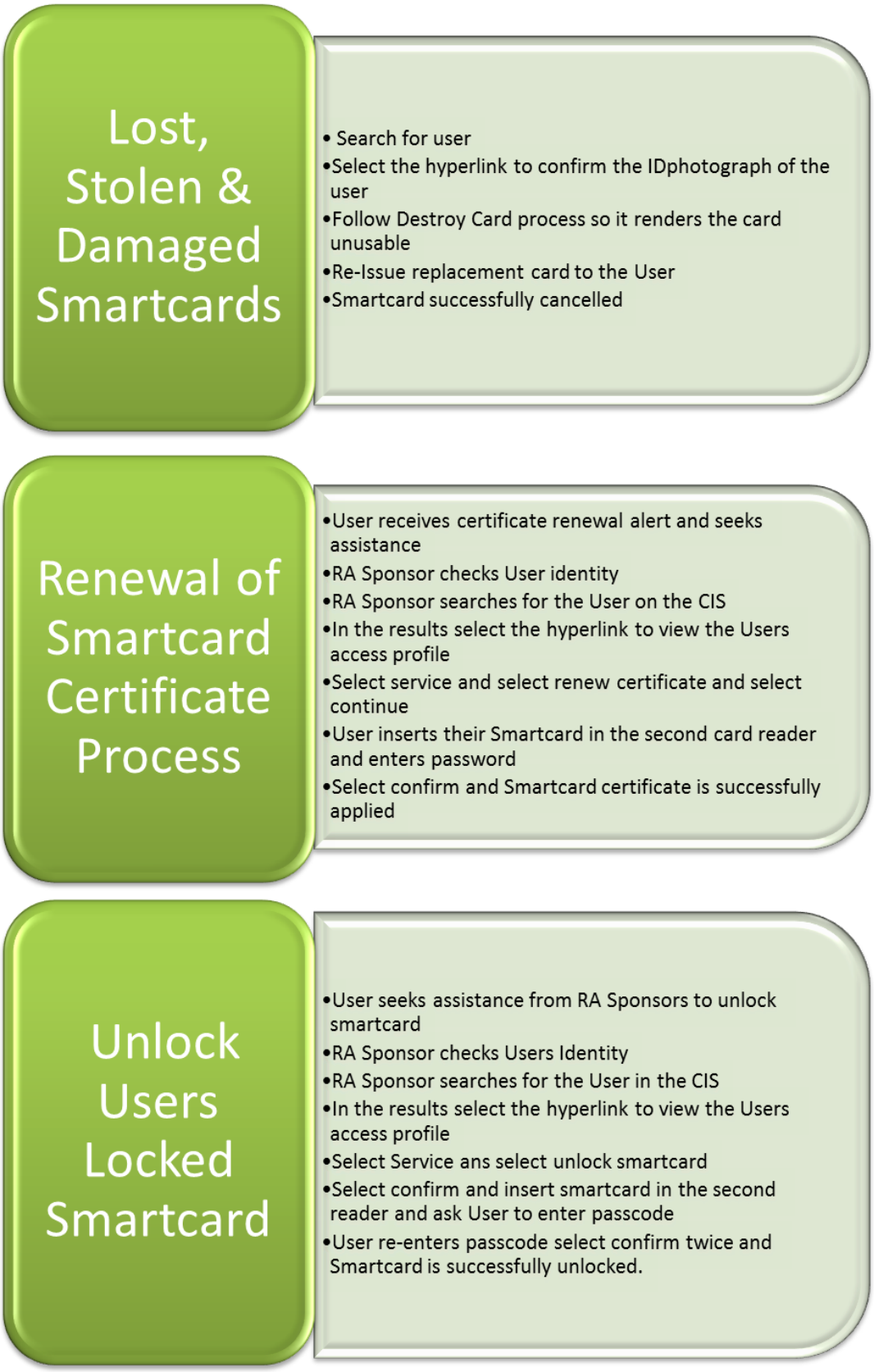
- The development of local processes that meet policy and guidance for the creation of digital identities and to ensure that the procedures for registering employees with Smartcards are developed, revised and maintained
- The production of smartcards, assignment of access rights, modifications to access and people and certificate renewal and card unlocking.
- The training of RA Agents and Sponsors and ensuring they are competent to carry out their roles and comply to policy and process.
- To facilitate the process for agreeing the Trusts access control Positions.
- To audit the RA process and Smartcard usage and take appropriate action arising from the outcome of these audits.
- To ensure leavers from the Trust have their access rights removed in a timely way.

The RA Manager will maintain a set of RA procedures which will be available to all staff to ensure the administration of the RA system is consistent. These will include approval of the position based access control system, new starters, user registration, lost, stolen and damaged Smartcard replacement and Card Unlock Process to name but a few.

5. Overview of Smartcard Services






Lost, Stolen & Damaged Smartcards
• Search for user
•Select the hyperlink to confirm the IDphotograph of the user
•Follow Destroy Card process so it renders the card unusable
•Re-Issue replacement card to the User
•Smartcard successfully cancelled
Renewal of Smartcard Certificate Process
•User receives certificate renewal alert and seeks assistance
•RA Sponsor checks User identity
•RA Sponsor searches for the User on the CIS
•In the results select the hyperlink to view the Users access profile
•Select service and select renew certificate and select continue
•User inserts their Smartcard in the second card reader and enters password
•Select confirm and Smartcard certificate is successfully applied
Unlock Users Locked Smartcard
•User seeks assistance from RA Sponsors to unlock smartcard
•RA Sponsor checks Users Identity
•RA Sponsor searches for the User in the CIS
•In the results select the hyperlink to view the Users access profile
•Select Service ans select unlock smartcard
•Select confirm and insert smartcard in the second reader and ask User to enter passcode
•User re-enters passcode select confirm twice and Smartcard is successfully unlocked.

5.1 The RA Agents

RA Agents are responsible for performing ongoing administration for Smartcard users. They also ensure that National and local RA processes are followed.

Their responsibilities include :

- Escalating issues to the RA Manager
- Keeping records of all cards that are issued
- Unblocking Smartcards
- Renewing certificates

5.2 Smartcards

NHS Smartcards are a plastic card containing an electronic chip (like a chip and PIN credit card) that is used to access Spine enabled systems. The chip stores the Unique User Identifier (UUID) within the Spine directory consisting of users digital identity information and access rights. The user is requested to input their passcode after inserting the NHS Smartcard into a Smartcard reader which is authenticated against the Spine. After authentication, the Spine returns a list of all active access positions assigned to the user. This allows the user to access the NHS Smartcard enabled system(s) assigned to them from any location that has an active N3 connection. The combination of the NHS Smartcard and the passcode together help protect the security and confidentiality of every patient's personal and healthcare information. Smartcards require renewal every two years before they expire.

All users must have only one NHS Smartcard issued to them showing their UUID and photograph and *should sign the Terms & Conditions of their Smartcard before using it. (Appendix 1) Cards must not be shared or left unattended at any time. Smartcard login details should be kept confidential otherwise it breaches the Computer Misuse Act 1990.*
In the event that a user has lost, stolen or damaged their NHS Smartcard, the user should report this immediately to the Trusts RA Manager and log the incident onto the datix system.

6.0 ESR & Care Identity Service

The Care Identity Service is the new Smartcard registration application available to all organisations to perform Registration Authority activities at a local level. As an integrated application with the Trust's ESR system, it provides greater levels of governance, accountability, auditability and enables more efficient ways of working.

7.0 Equality Impact Assessment

Position Based Access Control (PBAC) is a key pre-requisite to implementing the Care Identity Service. PBAC builds on the existing Role Based Access Control (RBAC) security model, which provides access to the Spine systems appropriate to the job that the staff have been employed to do.

PBAC links the job to the access rights it requires, thereby reducing the need for access rights to be assessed on an individual basis. PBAC provides a simple and effective mechanism for providing users with the access they need in the course of their work, whilst also ensuring that these access rights are properly managed and appropriate for the job they are doing. PBAC grants these rights according to the Access Control Position to which their job is assigned. Once the rights attached to each Access Control Position have been approved - along with the jobs included in these different positions - the process of granting access rights for staff becomes much simpler. PBAC ensures greater consistency within

NHS organisations about how access to care records is controlled and managed. PBAC also facilitates the management of access via the ESR interface to CIS.

The Trust has been operating two access systems and is working to consolidate its role based access control process into its position based access control process.

8.0 RA Service

The following services will be available

- User Registration
- Unblocking of Smartcards
- Smartcard renewal

This information and contact details will be published on the intranet.

8.1. Training HR and RA staff

Training on both the ESR and Registration Authority systems is a mandatory element for the Trust's HR and RA staff. This will maximise the staff's knowledge of the two systems to ensure that they have the ability to use the systems as per the requirements specified by the Trust, ESR and NHS Connecting for Health.

8.1.1 ESR Training

'Captivates' is the ESR e-learning tool that has been developed by the NHS ESR Central Team to assist in the learning of the functionality.

It is expected that all staff who will use the ESR-UIM Interface should complete these modules and document the completion dates for future review. ESR users can also access the ESR online user manual.

8.2 Information Governance Group

The IGG will review the RA function; review relevant policies and procedures; and approve access profiles.

9.0 Incident Reporting

Examples of incidents that must be reported on a Datix incident reporting form (accessible on the intranet) and to the RA Manager are:

- Smartcard or application misuse
- Theft of a smartcard
- Non-compliance of local or national RA policy
- Any unauthorised access to RA applications
- Any unauthorised alteration of patient data

10. Training

ID Training
Care Identity Service Training
Audit Process Training
Smartcard Unlocking Process Training
Identify Access Control Position Training.

11. Process for Monitoring Compliance and Effectiveness

Compliance with the RA policy and effectiveness of the procedures will be audited. Regular audits will cover:

- The issue of Smartcards
- The management of Smartcards
- The profiles associated with users in relation to what they do
- The use of Smartcards
- The use of Connecting for Health applications
- Identity management
- Security of supplies and equipment
- Exception reporting – to highlight users who consistently try to or do access information which they have not been authorised to view/use

The results and recommendations of the audits will be submitted to the Information Governance Group.

12. Standards/Key Performance Indicators

- NHS ESR interface to UIM : Deployment Assessment
- IG Toolkit : standards 303, 304

13. References and Associated Documents

- Registration Authorities : Governance Arrangements for NHS Organisations
- Confidentiality : NHS Code of Practice
- NHS Employment Check Standards
- Trust Confidentiality Code of Conduct
- Trust Information Security Policy
- Trust Management of Serious Incidents Policy

Appendix 1 - Smart Card Terms & Conditions

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

Notice to applicants on the collection of personal data

In accordance with the requirements of Department of Health, the personal data (as defined in the current data protection legislation) that the applicant provided as part of the application process to access NHS CRS together with any personal data processed in relation to the applicant in support of their application is collected for the purpose of identifying the applicant and processing this application and evaluating the applicant for suitability as an authorised user; if accepted, to generate a personalised certificate and Smartcard for the authorised user and for the purpose of managing the applicant's use of any NHS Care Records Service applications or applications that utilise NHS Care Records Service authentication.
In particular, this personal data will be used to validate and verify the applicant's identity to ensure that the applicant is correctly identified and appropriately authorised for access. The personal data in relation to the applicant will be processed by local Registration Authority/Authorities and may be shared with other Registration Authorities for the purpose of processing this application, in accordance with the requirements of the current data protection legislation 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 current data protection legislation, this personal data will neither be used nor disclosed for any other purpose other than where required by law, and will be retained in accordance with the Registration Authority's data retention policy. It is the applicant's responsibility to ensure that their registered name is accurate and kept up-to-date. The applicant may contact their local Registration
Authority or Sponsor in relation to any queries they may have in connection with this application.

By signing this declaration I, the applicant:

1. Consent to the use of my personal data in the manner described in the "Notice to applicants on the collection of personal data" above. I also agree to provide any additional information and documentation required by the Registration Authority in order to verify my identity;

1. Confirm that the information which I provide in the process of my application is accurate. I agree to notify my local Registration Authority immediately of any changes to this information;

3. 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 (www.dh.gov.uk site) and (where applicable) in accordance with my contract of employment or contract of provision for service (whichever is appropriate) and with any instructions relating to the NHS Care Records Service applications which are notified to me;

7. Agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate my Smartcard, NHS Care Records Service applications components or any access profiles given to me;

8. Agree not to deliberately corrupt, invalidate, deface damage or otherwise misuse any NHS Care Records Service applications or information stored by them. This includes but is not limited to the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality;

9. Acknowledge that my Smartcard may be revoked or my access profiles changed at any time without notice if I breach this Agreement; if I breach any guidance or instructions notified to me for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. I acknowledge that if I breach this Agreement this may be brought to the attention of my employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);

10. Agree that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of Smartcards for the NHS Care Records Service applications. The Registration Authority is not responsible for the availability of the NHS Care Records Service applications or applications which use NHS Care Records Service authentication or the accuracy of any patient data;

11. Acknowledge that I, or my employer, shall notify my local Registration Authority at any time should either wish to terminate this Agreement and to have my Smartcard revoked, e.g. on cessation of my employment or contractual arrangement with health care organisations or other relevant change in my job role; and

12. Acknowledge that these terms and conditions form a binding Agreement between 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.

Appendix 2 - Checklist for the Development or Review & Approval of Procedural Document

This should be completed and attached to any procedural document when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ N/A	Comments
1.	**Purpose**		
	Are the reasons for the development of the Document stated?	Yes	Full revision as a result of introduction of IIM
2.	**Definitions**		
	Have all key terms been clearly defined?	Yes	
3.	**Consultation**		
	Have relevant stakeholders and/or users been consulted with?	Yes	IG team; IGG
4.	**Equality Impact Assessment**		
	Has the Trust Equality Impact Assessment Screening Form been completed and attached by the author and approved by the responsible Executive Director?	Yes	
5.	**Monitoring**		
	Has the Monitoring Table been fully completed and attached?	Yes	
6.	**References/Associated Documents**		
	Are key references cited?	Yes	
	Are linked documents identified where appropriate?	N/A	
6.	**Approval**		
	Does the Document identify which committee/group will approve it?	Yes	ELB
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	N/A	via intranet
	Does the plan include the necessary training/support to ensure compliance?	N/A	Departmental arrangements
8.	**Review Date**		
	Is the review date identified?	Yes	

Information Governance Lead (or delegated authority)			
This Procedural Document complies with the Policy for the Development of Procedural Documents			
Name	Gail Butler	Date	20 April 2016
Clinical Quality Team			
The Procedural Documents complies with the relevant NHSLA standards			
Name		Date	
Please attach to the procedural document and forward to the relevant committee for approval			

Appendix 3 – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
ESR interface to UIM : Deployment Assessment	RA Manager	Submission of required evidence		Evidence is mandated in the assessment	NHS ESR	RA Manager will address any actions or changes required	With IGG and IG team
IG Toolkit	IG team	Online submission	annual	Evidence is mandated in the toolkit	NHS CfH online	IG lead	With IGG and IG team
Monitoring compliance with policy and effectiveness of procedures	RA Manager	Running reports	6 monthly	Audits of RA activity.	IGG	IG lead	With IGG and IG team

Appendix 4 - Equality Impact Assessment: Executive Summary

Executive Summary Page for Equality Impact Assessment:	
Document Reference:	Document Title: RA Smartcard Policy
Assessment Date: 5 March 2016	Document Type: Policy
Responsible Director: Director of Nursing Quality and Clinical Commissioning	Lead Manager: Compliance and Standards Lead
Conclusion of Equality Impact Assessment: The Framework is E&D neutral and has no impact, positive or negative.	
Recommendations for Action Plan: None	
Risks Identified: None	
Approved by a member of the executive team:	
YES	**~~NO~~**
Name: Sandy Brown	Position: Director of Nursing Quality and Clinical Commissioning
Signature: By email	Date: 7 March 2016
This whole document should be stored with the master document and a final approved electronic copy must be sent to the Equality & Diversity Lead at Bedford Office	