NHS
East and North Hertfordshire
Clinical Commissioning Group

HBL Registration Authority Policy

Policy Owner	Phil Turnock, Director of ICT Services
Policy Author	Mark Peedle
Version	1
Directorate	HBL ICT Services
Approved By:	HBL ICT Senior Team
Date of Approval:	TBC
Date of Review:	February 2020

Change History

Version	Date	Author	Reviewer(s)	Revision Description
V0.01	October 2015	Mark Peedle		
1	February 2016	Mark Peedle		
1.1a	January 2018	Mark Peedle		Scheduled Review

Implementation Plan:

Development and Consultation	HBL ICT RA Manager HBL Partner(s) to who HBL ICT provide Registration Authority (RA) services who are currently: ▪ NHS Bedfordshire CCG (06F) and the CCG's constituent GP Practices (0CG). ▪ NHS Luton CCG (06P) and the CCG's Constituent GP Practices (0CG) ▪ NHS Herts Valley CCG (06N) and the CCG's Constituent Practices (0CG) ▪ NHS East and North Herts CCG (06K) and the CCG's Constituent GP Practices (0CG) ▪ Hertfordshire Community NHS Trust (RY4)
Dissemination	▪ HBL Partner(s) to who HBL ICT provide Registration Authority (RA) services, their Boards and IG Structures and all staff who are issued with an NHS Issued Smartcard to access NHS Computer Systems. ▪ HBL Clients who purchase Registration Authority Services from HBL ICT Services.
Training	Staff Awareness sessions, Registration Authority Position holders, Sponsors in those HBL Partner(s) to who HBL ICT provide Registration Authority (RA) services
Monitoring	In Line with HSCIC IG Toolkit annual submissions the implementation, staff awareness and adherence is monitored by regular staff survey and awareness sessions.
Equality, Diversity and Privacy	▪ Privacy: Appendix 1
Associated Documents	▪ HSCIC Registration Authority Policy v1.0 ▪ HSCIC Registration Authorities Operational and Process Guidance v5.1

Contents

1 Introduction

It is of paramount importance that patients are confident that their medical records are kept safe, secure and confidential in line with The Care Record Guarantee for England. To achieve this objective all healthcare professionals/worker requiring access to Spine enabled systems must be registered with a national digital identity, issued a NHS Smartcard and assigned an appropriate access control position according to their healthcare role.

What are NHS 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 roles 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.

What is the Care Identity Service?
The Care Identity Service is the new Smartcard registration application available to all organisations to perform Registration Authority activities. As an integrated application, it enables an automated 'workflow' approach that provides greater levels of governance, accountability, auditability and enables more efficient ways of working.

What is the ESR Interface to Care Identity Service?
The ESR Interface to CIS, also known as Integrated Identity Management (IIM) 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. This allows for greater efficiency when controlling access to records on computer systems linked to the Spine.

What is the user registration process?
The user registration process operates locally and broadly consists of the following three stages:

1. A user is identified for a NHS Smartcard – this can be via
   - an individual (sponsor) explicitly requesting the individual be registered in CIS or other means such as employment into a role or requirements of a job changing
   - The user provides appropriate identification as per NHS Employers Identity Check standards to ensure their identity is verified and recorded to e-GIF Level 3.

2. Access to the relevant Spine enabled application is permitted on assignment of an Access Control Position. The RA Manager or the Advanced RA Agent directly assigns the user to the Access Control Position or grants the assignment where the request has been approved by the Sponsor.
3. A NHS Smartcard is created that links the user to their record on the Spine and the required level of access. Access to the Spine enabled applications is then established.

What security and confidentiality measures are implemented?
All Spine enabled applications use a common security and confidentiality approach. This is based upon the healthcare professional's/worker's organisations, 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 healthcare professionals/workers with the access to patient information required to perform their role within the organisation, satisfying both clinical and Information Governance needs.

Reference and Standard Documents
This document references job roles and activities in the National RBAC database which can be found in the following location:
http://nww.hscic.gov.uk/rasmartcards/docs

2 Purpose of this Document

This document lays out the RA Policy requirements that HBL ICT Services Registration Authority adheres to.

It is based on the original DH Gateway Document (reference number 6244) 'Registration Authorities: Governance arrangements For NHS Organisations', the national Registration Authority Guideline, the NHS Care Record Guarantee, The Data Protection Act 1998, and requirements contained in the HSCIC RA Process Guidance together with the IG Toolkit requirements in relation to Registration Authorities.

2.1 Background

This document outlines:

- The RA Hierarchy and the principle of delegated authority from the HSCIC to us to run the RA on behalf of our partners and customers.
- The requirements for creating a nationally verified digital identity.
- The roles and responsibilities with HBL ICT services, our Partner organisations and customers.
- Requirements in relation to Smartcards

3 Registration Authority Hierarchy

In Public Key Infrastructure (PKI) terms there is a single Registration Authority (HSCIC). All organisations that run a local Registration Authority do so on a delegated authority basis from HSCIC.

As HSCIC is the single Registration Authority it needs to assure itself that organisations are operating appropriately and discharging their duties in an effective and consistent fashion. This policy outlines HBL ICT Services assurance that it is meeting minimum national requirements; deviation from the HSCIC National Registration Authority Policy document due to a local preference is not permitted.

The original DH Gateway document (DH 6244) 'Registration Authorities: Governance Arrangements for NHS Organisations' outlines some of the requirements for delegated authority to local organisations to run their own RA activities.

This policy document outlines the full range of mandatory requirements that HBL ICT services adheres with to carry out this activity. The mandatory requirements in relation to organisational set up and appropriate governance oversight are:

1. There needs to be a Board/EMT level individual who has overall accountability in each organisation for RA activity. The responsible individual must report annually to the organisation on this activity.

2. The RA Manager & Sponsors are appointed by the Board and this appointment is confirmed in a letter of appointment which must be held by each individual appointed to these positions. Copies of these letters should also be held by the RA Manager so they are able to provide the necessary evidence to meet IG Toolkit requirements. Each of the Partner and Customer organisations who receive RA services from HBL ICT are required to acknowledge that the appointed HBL ICT RA Manager is responsible for the provision of RA services supplied by HBL ICT Services (Appendix 3).

3. Partner and Customer organisation may appoint local RA Managers if this is appropriate, however delegated responsibility to HBL ICT services must be made clear so that lines of accountability are maintained.

4. The RA Manager is accountable for the running of RA service in HBL ICT Services within the Partner and Customer organisations under binding agreement, these organisations are listed in Appendix 4. The RA manager is required to set up the systems and processes that ensure that the policy requirements contained in this document are met and local processes meet these requirements and cater for local organisational circumstances (NOTE: deviation from the national policy requirements due to a local preference is not permitted).

5. The RA Manager and appointed Agents need to keep up to date with national policy requirements, initiatives and changes. In order to do this it is mandatory that their email address is entered as part of their personal details held within the database of Smartcard users. They are also required to subscribe to the national

email address list by sending an email with their details to ramanagers.agents@hscic.gov.uk

6. The RA Manager has a line of professional accountability to uphold good RA practice to HSCIC.

4 Creation of a national digital identity

HSCIC as the single Registration Authority needs to be assured that users who have a digital identity created are subject to the same standards of identity verification, to prove identity beyond reasonable doubt, irrespective of which local organisation creates the identity. This is vital as the identity created is a national identity and must be trusted by each organisation where an individual is required to access the National Spine to access data. To achieve this, identity is required to be verified to the previous inter-governmental standard known as eGIF Level 3 This provides assurance that the identity is valid across any organisation an individual works within.

In order to ensure this the following requirements in creating a digital identity are mandatory and are adhered to by HBL ICT Services Registration Authority.

1. 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.

2. The person verifying the identity is trained to do so. In Registration Authority terms this means that individuals holding the roles of RA Managers and RA Agents must perform these checks at face to face meetings since part of their responsibilities and requirements are that they are trained to carry out this activity. The RA Manager is responsible for training all other RA staff who will conduct ID checking to ensure that appropriate standards exist and they can evidence good ID checking as part of the IG Toolkit requirements.

3. 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/case-studies-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.

4. 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 a person holding an RA role and provide appropriate documentary evidence.

5. Smartcards can only be issued to individuals who have a national verified digital identity. This is also the case for processes that are used to issue temporary access to an individual – they need to have a verified identity first.

5 Policy Roles & Responsibilities

In order to discharge the responsibilities delegated from HSCIC in relation to Registration Authority activity there are requirements each organisation must meet in relation to roles and responsibilities within the local organisation. These are as follows:

1. The Board/EMT person accountable for RA activity within the organisation must be overtly identified and named. Part of this ensures that the RA Manager knows who to raise issues with.

2. The Board/EMT individual must report to the Board/EMT annually on RA activity and must sign off on RA IG Toolkit submissions.

3. The RA Manager is responsible for running the governance of RA in the organisation. As such they must agree and sign off on local operational processes and should assure themselves regularly that these processes are being adhered to (NOTE: local processes cannot contradict this national policy document). They are also responsible for registering RA staff in their own organisations and any RA Managers in child organisations. They are also responsible for ensuring the effective training of RA Agents and Sponsors within their organisation.

4. New roles have been created in the Registration Authority software, Care Identity Services, to allow the RA Manager to delegate certain aspects of RA activity. These include Advanced RA Agents, RA Agents (ID checking only) and Local Smartcard Administrators. However these delegated permissions do not extend to any of the areas covered in point 3 above. This is explained in the following table.

RA Manager CANNOT delegate	**RA Manager CAN delegate**
❖ Responsibility for running RA Governance in their organisation ❖ Responsibility for ensuring local processes are in place that meet policy and guidance for the creation of digital identities, production of smartcards, assignment of access rights, modifications to access and people and certificate renewal and card unlocking ❖ Assignment of RA Agents and sponsors and the registration of RA Agents and Sponsors ❖ The training of RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process. A RA Hosting organisation parenting another RA Hosting organisation is responsible in providing training to the RA Manager	❖Creation of local processes that meet policy and guidance for the creation of digital identities, production of smartcards, assignment of access rights, modifications to access and people and certificate renewal and card unlocking ❖ Operation of core RA processes of registering a user, the approval and granting of access, the modification of personal details and the modification of access rights ❖ The implementation of the local auditing process ❖ Ensuring users accept terms & conditions of Smartcard use when registering them ❖ Operational security of (old) paper based RA records

in the next level down ❖ Facilitation of the process for agreeing the organisation's access control positions ❖ Responsibility for ensuring that appropriate auditing is carried out ❖ Responsibility for ensuring users are compliant with the terms and conditions of Smartcard usage ❖ Verification of user's ID to e-GIF level 3 when they register users ❖ Responsibility for ensuring the security of (old) paper based RA records ❖ Responsibility for ensuring all service issues are raised appropriately locally and nationally	❖ Raising service issues as appropriate and through the correct channels

5. Identity checking must be carried out by those holding an RA role – RA Managers RA Agent and RA ID Checker Roles roles.

5.1 Sponsors

Sponsors are appointed and entrusted to act on behalf each partner and customer organisation in determining who should have what access and maintaining the appropriateness of that access. Their roles is primarily identification of the type of access to information a user's needs via a National application – the organisation they belong to, their Position(s) and Workgroup(s).

Sponsors are responsible for granting on behalf of each partner and customer organisation, who can access what healthcare information. Sponsors will be held accountable by each partner and customer organisation Board for their actions. Sponsors are responsible to each partner and customer organisation Board to ensure only appropriate access to National Applications is granted.

Sponsors will be identified by the RA Manager as being suitable persons by virtue of their status and role. Sponsors will be registered by the RA Manager on behalf of each partner and customer organisation in accordance with guidance. Sponsors will be staff with sufficient seniority to understand and accept the responsibility required. Registration Sponsors are responsible to the RA Manager for the accuracy of the information on the RA01, RA02 and RA03 forms in the current system, and for using the CIS system for 'self-service' activities in relation to Position Based Access Control when this is fully implemented.

The Registration Authority Office will maintain the list of sponsors.

All Sponsors are required to provide documentary evidence to prove their identity. RA forms may be scanned and transmitted by fax or e-mail and sent to the Registration Authority Office for processing. The original RA form must be sent to the Registration Authority Office within three working days. Registration Sponsors are responsible for making sure that National application users are given the minimum appropriate level of

access needed to perform their job. The areas of responsibility with respect to National application user access should be clearly defined for each Sponsor.

Registration Sponsors and Registration Authority Office Staff will report any RA related incidents, using the HBL ICT incident reporting procedure to the RA Manager. Additionally Sponsors and Registration Authority Office staff will report any operational difficulties especially where these have patient healthcare implications to the RA Manager. Some circumstances will require a report to be made to the appropriate organisation's Caldicott Guardian

6 Requirements in relation to Smartcards

Smartcards enable an individual to access sensitive patient data and therefore how they are issued and ensuring safe receipt and appropriate use are of vital importance. As a result the following are mandatory requirements in relation to Smartcards.

1. Smartcards issued to anyone holding RA roles (RA Manager, Advanced RA Agent, RA Agent and RA Agent – ID Checking) must be handed over to that individual in a face to face encounter. This is because RA staff have significant powers in relation to the system and they are entrusted with much of the delegated responsibilities from HSCIC – therefore it is vital that risks are minimised in the process of the Smartcard getting to the right person. It is also a Public Key Infrastructure requirement for these reasons.

2. HBL ICT Services has a robust and secure process in place to ensure that the Smartcard reaches all non RA end users for whom it is intended. In the event that it is not possible to hand the card over in a face to face encounter when performing the identity check, the card is produced in a 'locked' state and stored in the fire safe in the secure RA office, the card is then handed over at the next available face to face encounter, where the card is unlocked and the card user sets their own passcode.

3. Only the end user for whom the Smartcard is intended should know their passcode for their Smartcard, no-one else should, including RA staff. If anyone else knows the end users passcode it breaches the Smartcard terms and conditions of use and the Computer Misuse Act 1990.

4. When Smartcard users leave one of HBL ICT's partner or Customer organisations they should have their access assignment end dated in that organisation. However unless it can be reasonably foreseen that they will not require access in another organisation in the future, leavers should retain their Smartcard.

5. It is mandatory that users sign the Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.

6. RA staff (RA Managers, Advanced RA Agents and RA Agents) are reminded that it is their responsibility to ensure that users comply with these terms and conditions.

Appendix 1 – Privacy Impact Assessment Stage 1 Screening

1. Policy	PIA Completion Details
Title: Registration Authority Procedures Policy ☒ Proposed Date of Completion: 08/03/2011 ☐ Existing Review Date: March 2014	Names & Titles of staff involved in completing the PIA: Mark Peedle

2. Details of the Policy. Who is likely to be affected by this policy?

☒ Staff ☐ Patients ☐ Public

	Yes	No	Please explain your answers
Technology Does the policy apply new or additional information technologies that have the potential for privacy intrusion? (*Example: use of smartcards*)	☒	☐	**For security purposes.**
Identity By adhering to the policy content does it involve the use or re-use of existing identifiers, intrusive identification or authentication? (*Example: digital signatures, presentation of identity documents, biometrics etc.)*	☒	☐	**Under controlled conditions.**
By adhering to the policy content is there a risk of denying anonymity and de-identification or converting previously anonymous or de-identified data into identifiable formats?	☐	☒	
Multiple Organisations Does the policy affect multiple organisations? (*Example: joint working initiatives with other government departments or private sector organisations*)	☒	☐	**RA Service is provided to third party organisations with appropriate security measures.**
Data By adhering to the policy is there likelihood that the data handling processes are changed? *(Example: this would include a more intensive processing of data than that which was originally expected)*	☐	☒	
If Yes to any of the above have the risks been assessed, can they be evidenced, has the policy content and its implications been understood and approved by the department?	**See comments above.**		

Appendix 2 – Template for acknowledgement of responsibility for provision of RA service.

HBL ICT Services
Charter House
Parkway
Welwyn Garden City
AL8 6JL

FAO: Phil Turnock

I confirm on behalf of NHS Bedfordshire CCG that we acknowledge that the appointed HBL ICT RA Manager is responsible for the provision of RA services supplied by HBL ICT Services.

At the time of writing, I confirm the following roles are allocated within this organisation as below:

Role	**Allocated To**
Privacy Officer	
Caldicott Guardian	
Board Member Responsible for RA	
Sponsors	

Yours sincerely

A N Other

Appendix 3 – HBL ICT services Partners and Customers as at policy creator or revision.

HBL Partner(s) to who HBL ICT provide Registration Authority (RA) services who are currently:

- NHS Bedfordshire CCG (06F) and the CCG's constituent GP Practices (0CG).
- NHS Luton CCG (06P) and the CCG's Constituent GP Practices (0CG)
- NHS Herts Valley CCG (06N) and the CCG's Constituent Practices (0CG)
- NHS East and North Herts CCG (06K) and the CCG's Constituent GP Practices (0CG)
- Hertfordshire Community NHS Trust (RY4)

External Clients to who HBL ICT provide Registration Authority (RA) services who are currently:

- NHS England; RA services to Pharmacies throughout Bedfordshire and Hertfordshire (CCG Codes)
- Hospices in Bedfordshire and Hertfordshire (under 0CG)
- Cambridgeshire Community Services (Luton Community Services) (RYV)
- The Gynaecology Partnership Limited (NW4)
- Direct Local Health (NXG)
- Herts County Council (VJC)
- RX Systems (YGM19)
- (Haverstock) Cheshunt Minor Injuries Unit (Y02864)
- Northgate Information Solutions (NWY)