HBL ICT Registration Authority Policy

Author: Waseem Khan (RA Manager)

Version: 4.0.1

Hertfordshire, Bedfordshire, and Luton ICT Shared Services is hosted by Hertfordshire and West Essex Integrated Care Board

Copyright

Document Control

Document Owner	Phil Turnock (Managing Director HBL ICT)	**Approved by**	
Document Author(s)	Waseem Khan (RA Manager)	**Date of Approval**	
Version	4.0.1	**Date for Review**	12 months

Version Control

Version	Status	Commentary	Date	Author
V0.01	Live		Oct 2015	Mark Peedle
1	Live		Feb 2016	Mark Peedle
1.1a	Live	Scheduled Review	Jan 2018	Mark Peedle
1.1.1	Draft	Review: Moved into updated template Updated in line with national policy 2.4	July 2020	Alex McLaren
2	Draft	• Scheduled review • Updated in line with National Policy 2.4 • Equality Impact Assessment updated • DPIA updated • HBL ICT Services' Partners and Customers Privacy Impact Assessment *outstanding*	Aug 2020	Circe Teasdale Waseem Khan
2.0.1	Draft	○ Update to Implementation plan replacing IG Toolkit with DSPT	Oct 2020	Alex McLaren
3.0.0	Live	○ Authorized by ENHCCG IG Forum	9 Dec 2020	Alex McLaren
3.1.0	Draft	Annual review – Authorized by HBL ICT SMT Update RA Manager details, ○ removal of Appendices – DPIA/EIA, Organisations (actioned separately)	16 Nov 2021	Alex McLaren Waseem Khan

3.2.0	Draft	Additional reference to RPA & FIDO Review following release of National Policy v2.5, clarification of sponsor role EIA and DPIA issued	Feb 2022	Waseem Khan Philip Taylor
4.0.0	Live	Authorized by ENHCCG IG Forum held 16/3/2022.	Mar 2022	A McLaren
4.0.1	Draft	Document template/format updated CCG references updated to ICB External legislation –GDPR changed to UKGDPR As requested by Mike Partridge (National RA Manager) have inserted section pertaining to the issuing of RPA Smartcards. EIA approval HBL ICT SMT approval	Jan and Feb 2023	Waseem Khan
5.0.0	PROPOSED	Authorised by HWE ICB IG Forum – In-progress		

Terms and Acronyms

Term	Definition
"Authentication Token"	Refers to Physical Smartcards, Virtual Smartcards, Authorised Devices and iPad Devices which enable healthcare professionals to access clinical and personal information appropriate to their role and the type of Identity Solution. Note – the Authentication Token is not the HBL ICT provided RAS or Nebula access Token solution
"Authorised Devices"	Means an alternative to smartcards, a device as approved by FIDO 2 Consortium that provides Assured Level 3 Authentication2.
"Data Protection Laws"	Is the applicable legislation protecting the fundamental rights and freedoms of individuals, in respect of their right to privacy and the processing of their personal data, as amended from time to time, including Regulation (EU) 2016/679, 'the General Data Protection Regulation' ("GDPR") and the Data Protection Act 2018) and the Privacy and Electronic Communications Regulations 2003, together with decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, data protection authorities and other applicable Government authorities;
"Physical Smartcards"	This is an approved physical card. Physical Smartcards are supplied by the authorised supplier(s) of cards to NHS Digital and are similar to chip and PIN bank cards.
"RA Agent ID Checker"	An individual who has undertaken appropriate training who is authorised to undertake identity verification and identity creation.
"RA Agent"	An individual who has undertaken appropriate training who is authorised to undertake identity verification, identity creation, creation and assignment of authorisation tokens and assign access rights to a user. In addition, they can perform a range of administrative tasks to maintain good RA records and processes

"RA Manager"	An individual appointed by the Executive Management Team of an organisation to set up and run the organisations Registration Authority processes and procedures. In addition, they are responsible for ensuring good governance and report annually to the organisation's EMT on RA activity. In addition, they are required to undertake appropriate training to discharge these responsibilities and arrange training for all other RA team members. They are also authorised to undertake identity verification, identity creation, creation and assignment of authorisation tokens and assign access rights to a user.
"Registration Authority (RA)"	Means NHS Digital as the single national Registration Authority and all other organisations that run a local Registration Authority on a delegated authority basis from NHS Digital.
"Spine"'	The NHS central 'Spine' is the digital central point allowing key NHS online services and allowing the exchange of information across local and national NHS systems.
"Virtual Smartcards"	Is a solution that provides access functionality, but the card itself may be stored on a device, approved for use by NHS Digital and or its partners.
RPA	Robot Process Automation
CIS	Care Identity Service
EMT	Executive Management Team
ESR	Electronic Staff Records
FIDO	Fast Identity Online
HBLICT	Hertfordshire Bedfordshire and Luton information and Communication Technology
ICT	Information and Communications Technology
ID	Identity
IIM	Integrated identify management
IM&T	Information Management and Technology
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
Sponsor	Refers to an individual appointed by the Executive Management Team of an organisation who is authorised to request and approve that digital identities be created and appropriate and specific access assigned to staff within the organisation

Implementation Plan

Development and Consultation	IG within Partner organisations Hertfordshire, Bedfordshire and Luton ICT Shared Services (HBL ICT) is committed to the fair treatment of all, regardless of age, colour, disability, ethnicity, gender, gender reassignment, nationality, race, religion or belief, responsibility for dependents, sexual orientation, trade union membership or non-membership, working patterns or any other personal characteristic This policy / procedure will be implemented consistently regardless of any such factors and all will be treated with dignity and respect. To this end, an equality impact assessment has been completed on this policy.
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. This policy will be included in the ICBs Publication Scheme in compliance with the Freedom of Information Act (FOI) 2000
Training	Staff Awareness sessions, Registration Authority Position holders, Sponsors in those HBL Partner(s) to who HBL ICT provide Registration Authority (RA) services
Monitoring	3rd Party Audit, DSP Toolkit, spot check
Review	The policy will be reviewed annually or when National Policy updates requires
Equality, Diversity and Privacy	Completed Separately

References

External : Legislation, Guidance and Standards	• NHS Digital National Registration Authority Policy v2.5 • NHS Digital Registration Authorities Operational and Process Guidance v5.2 • DH Gateway Document (reference number 6244) 'Registration Authorities: Governance arrangements For NHS Organisations' • NHS Care Record Guarantee, • The Data Protection Act 2018 and UK GDPR • DSPT (Data Security and Protection Toolkit) • Additionally, the policy now reflects current best practice around Identity & Access Management as informed by the National Cyber Security Centre which covers what needs to be considered in identity verification and security requirements in relation to authentication to clinical systems and other systems which hold personal information. In particular this includes: ○ Good Practice Guide 43 – Requirements for Secure Delivery of Online Public Services https://www.ncsc.gov.uk/guidance/requirements-secure-deliveryonline-public-services-good-practice-guide-43 ○ Good Practice Guide 44 – Authentication and Credentials for use with HMG Online Services https://www.ncsc.gov.uk/guidance/authentication-and-credentialsuse-hmg-online-services-gpg-44 ○ Good Practice Guide 45 – Identity Proofing and Verification of an Individual https://www.ncsc.gov.uk/guidance/identity-proofing-andverification-individual-gpg-45
Internal : Related Documentation	• Acceptable Use Policy • Information Governance Policy • Mobile Device Policy • Confidentiality Policy • Information Security Policy
Enclosures	None

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.

1.1 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.

1.2 What is the Care Identity Service (CIS)?

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.

1.3 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.

1.4 What is the User Registration Process?

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

- 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.
- 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.

- 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.

1.5 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.

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 National Registration Authority Policy v2.4.

2.1 Background

This document outlines:

- The RA Hierarchy and the principle of delegated authority from NHS Digital 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, authentication methods for the different Authentication Tokens

3 Registration Authority Hierarchy

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

As NHS Digital 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 the minimum national requirements to provide such assurance: as such deviation from this policy document due to a local preference is not permitted. In addition, HBLICT RA Managers are required to read and comply with RA operational guidance available at https://digital.nhs.uk/services/registration-authorities-and-smartcards

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 and/or be a Registration Authority, for both their own users and users in other local organisations.

This policy document outlines the full range of mandatory requirements that HBL ICT services adheres 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/Executive Management Team (EMT) level individual who has overall accountability in the organisation for RA activity. The responsible individual must report annually to the organisation on this activity. This only relates to RA.

2. RA Managers are appointed by the Board/EMT and this appointment is confirmed in an official document (e.g. minute, letter of appointment, email from SRO etc.) which must be held by each individual appointed to these positions, and be made available for inspection when required (see Appendix C).

3. RA Managers are accountable for the running of RA service in HBL ICT within the Partner and Customer organisations *under binding agreement.* RA Managers are 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).**

4. RA Managers and 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 registered users (The Spine User Directory).

5. RA Managers have a line of professional accountability to uphold good RA practice to NHS Digital.

6. The Registration Authority and, where different, employing organisation must:

    - have sufficient governance, processes and oversight in place to comply with the Data Protection Laws, including (but not limited to) providing fair processing information to all users, the NHS Code of Practice on confidential information, as amended from time to time, and the Care Record Guarantee; and
    - be registered for the latest Data Security Protection Toolkit (currently this is V4 21-22) and have a current latest status rating of at least ‘standards met’.

Accountable Board/EMT Member:

Simon Carey – Associate Director

RA Managers:

Waseem Khan

4 Creation of a National Digital Identity

NHS Digital's strategic aim is to create a single, non-repudiated, trusted, digital identity for healthcare workers. This will be pivotal to enabling national access to health information in a secure way.

NHS Digital, as the single Registration Authority for health and social care, needs to be assured that users who have a digital identity created are subject to the same minimum standards of identity verification, to prove the individual has ownership of the identity irrespective of which local Registration Authority 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 National Cyber

Security Centre Good Practice Guide 45 – 'Identity Proofing and Verification of an Individual'. 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:

- Identity must be verified in a face-to-face meeting. It must be done by examining original identification evidence documents and seeing that identity relates to the individual who presents themselves at the meeting. The person verifying the identity must be 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 Data Security Protection Toolkit requirements.

- The documents that can be used to verify an identity have been jointly determined by NHS Digital and NHS Employers and the list is contained in the NHS Employers 'Verification of Identity Checks' standard which can currently be found at https://www.nhsemployers.org/publications/identity-checks.

  However GPG 45 processes and NHS Employers guidance, around managed risk, allow for additional documents to be considered provided they meet the GPG45 evidence category requirements.

- 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.

- Use of Authorised Devices and iPad Devices must be subject to HBLICTs Registration Authority's and, where different, employing organisation's device management policies (which should include additional relevant provisions where users are allowed to use their own personal devices for work purposes), and checks that the Authorised Device meets the minimum required solution specification.

- Authentication Tokens 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.

- Different types of Authentication Tokens meet different levels of security classification. For further information see https://digital.nhs.uk/services/registration-authorities-andsmartcards#registration-authorities. The local Registration Authority and, where different, employing organisation must ensure that the Authentication Token provided to a user is appropriate for that user's role.

- GPG 45 outlines four levels of identity assurance. Authentication Tokens will support these four levels of identity assurance. In practice Authentication Tokens will combine the level 3 and level 4 identity requirements. Level 4 being a level 3 identity with the addition of a biometric indicator. A level 3 or level 4 identity is required in order to access clinical, sensitive and person identifiable information. Level 1 and 2 identities will be able to be registered but are aimed at people who do not need access to the types of information that requires a level 3 or 4 identity.

- Users must be able to easily access support and report and receive assistance with any operational issues, thefts, losses or unauthorised uses of Authentication Tokens, requirements for PIN/password resets, and terminations of Authentication Tokens.

5 Roles and Responsibilities

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

- 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.

- The Board/EMT individual must report to the Board/EMT annually on RA activity and must sign off on RA Data Security and Protection Toolkit submissions.

- RA Managers are responsible for running the governance of RA in the organisation. As such they must agree and sign off on local operational processes and guidance and should assure themselves regularly that these processes are being adhered to (NOTE: local processes must comply with this national policy process and guidance set out by NHS Digital). 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.

- 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 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 GPG45 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	• Creation of local processes that meet the Registration Authority Policy and guidance for the creation of digital identities, production of NHS Digital smartcards, allocation of other approved devices 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 • Raising service issues as appropriate and through the correct channels

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

5.1 RA Manager Responsibilities

- Responsible for running RA Governance in their organisation – RA Managers CANNOT DELEGATE THIS
- Responsible for the development of local processes that meet policy and guidance for the creation of Authentication Tokens, digital identities, production of smartcards, assignment of security device, assignment of access rights, modifications to access and people, removal of access rights in a timely fashion where there is no business justification for the rights to be retained and certificate renewal and card unlocking
- Implements local RA policy and RA processes adhering to national guidance and this policy
- Assign, sponsor and register RA Agents and Sponsors
- Train RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process – If an RA hosting organisation with a child hosting organisation – need to train RA Manager at next level down
- Facilitate the process for agreeing the organisations access control positions
- Responsible for auditing
- Responsible for ensuring users are compliant with the terms and conditions of Smartcard usage and other registered devices
- Verifies user's ID to GPG45 Level 3 or 4, when they register users
- Ensuring leavers from an organisation have their access rights removed in a timely way
- Responsible for the security of (old) paper-based RA records
- Ensure all service issues are raised appropriately locally and nationally

5.2 RA Agent Responsibilities

- Verify users ID to GPG45 Level 3 or 4
- Register users and provide them with Authentication Tokens
- Grant users access assignment
- Renew Smartcard certificates for users if self-service functionality not used
- Responsible for ensuring users at the time of registration or assigned a role in the organisation comply with the individual terms and conditions applicable to access to the NHS Care Records Service Ensuring leavers from an organisation have their access rights removed in a timely way
- Adhere to local processes that meet policy and guidance for the creation of Authentication Tokens, digital identities, production of smartcards, allocation and registration of other approved devices, assignment of access rights, modifications to access and people and certificate renewal and card unlocking

5.3 Sponsors

Sponsors are appointed and entrusted to act on behalf of 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 needs via a National application.

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 information requests provided to the Registration Authority Office, 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 post or e-mail and sent to the Registration Authority Office for processing. 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 Authentication Token

NHS Digital will allow Authorised Devices and iPad Devices in addition to centrally issued Virtual Smartcards and Physical Smartcards. These methods will include approved mobiles, approved tablets, approved devices/operating systems and other approved peripherals and authentication methods. These additional authentication methods must meet the National Institute of Systems and Technology (NIST SP800 – 63 Digital Identity Guidelines for a Authentication Assurance Level 3 authentication, available at https://pages.nist.gov/800-63-3/, this describes the cryptographic strength of authentication methods that is required to access sensitive data. In addition Authorised Devices and authentication methods need to meet FIDO 2 standards for how devices utilise the required cryptography (available at https://fidoalliance.org/) and must be accredited by the FIDO alliance. Any Authorised Device or authentication method that meets both of these standards will be acceptable for authenticating to national clinical systems and the choice of device that meets these standards is down to the local organisation. iPad devices must authenticate using the NHS Digital created authentication app which follows the FIDO patterns of cryptographic exchange.

Authentication Tokens 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 for Registration Authorities and employing organisations making use of RA activity provided by a local Registration Authority:

- Authentication Tokens 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 NHS Digital – therefore it is vital that risks are minimised in the process of the Identity Solution getting to or a device being linked to the right person. It is also a Public Key Infrastructure requirement for these reasons.

- HBL ICT has a robust and secure process in place to ensure the Authentication Tokens reach all non-RA users for whom they are intended. This is important to avoid individuals potentially gaining access to patient data when they are not the person entitled to do so. 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.

- Organisations should ensure that their infrastructure is secure, in particular ensuring they meet the Warranted Environment Specification issued by NHS Digital available at https://digital.nhs.uk/services/spine/spine-technical-information-warranted-environment-specification-wes

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

- Robot Process Automation (RPA) solutions requiring Smartcards for nonperson specific use, form an exception to policy so the security and risks need to be assessed on a case-by-case basis. All requests for an RPA Smartcard must be submitted to the Registration Authority Manager.

- When Identity Solution users leave an organisation 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 Physical Smartcard or Virtual Smartcard if this is stored on their personal mobile phone. Users of other Authorised Devices or iPad Devices will return these devices to their organisation before they leave.

- It is mandatory that users sign the Terms & Conditions applicable to access to the NHS Care Records Service detailed at https://digital.nhs.uk/services/registration-authorities-andsmartcards#registration-authorities. This reminds them of their responsibilities and obligations, including not sharing their Identity Solution, and not disclosing their passcode to others.

- 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 A. Template for acknowledgement of responsibility for provision of RA service

HBL ICT Services

Charter House

Parkway

Welwyn Garden City

AL8 6JL

FAO: Simon Carey

I confirm on behalf of ***Insert Organisation Name*** 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 B. Comment Form

As part of HBL ICT Services Department continuous improvement regime, would you please complete this form. Any comments or feedback on this document should be addressed to the Owner. Please provide your name and contact details in case clarification is required.

Name Click here to enter text.

Address Click here to enter text.

Click here to enter text.

Phone Click here to enter text.

Email Click here to enter text.

Please return to:

HBL ICT Services

Charter House

Welwyn Garden City

Hertfordshire, AL8 6JL

Please confirm the document you want to give response to as:

HBL ICT Policy/Procedure: Click here to enter text.

Please rate the document using the topics and criteria indicated below:

	Very Good	Good	Average	Fair	Poor
Format and Layout	☐	☐	☐	☐	☐
Accuracy	☐	☐	☐	☐	☐
Clarity	☐	☐	☐	☐	☐
Illustrations (tables, figures etc.)	☐	☐	☐	☐	☐

When using the document, what were you looking for?

Click here to enter text.

How could the document be improved?

Click here to enter text.

How often do you use the document?

Click here to enter text.

If you have additional comments, please include them below:

Click here to enter text.

Thank you for your time.