### Registration Authority Policy

<table>
<thead>
<tr>
<th>Document filename:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Directorate / Programme</td>
<td>Interoperability &amp; Architecture</td>
</tr>
<tr>
<td>Document Reference</td>
<td></td>
</tr>
<tr>
<td>Programme / Project Manager</td>
<td>Philip Gill</td>
</tr>
<tr>
<td>Owner</td>
<td></td>
</tr>
<tr>
<td>Author</td>
<td>Philip Gill</td>
</tr>
<tr>
<td>Issue date</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Document Management

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3</td>
<td>01/03/2019</td>
<td>Includes new identity verification standards and policy approval for additional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>authentication methods that meet approved standards</td>
</tr>
<tr>
<td>2.31</td>
<td>05/03/2019</td>
<td>Amended link to GPG45 document (WB/PG)</td>
</tr>
</tbody>
</table>

Reviewers

This document has been sent to for review and/or reviewed by the following people (please include nil returns):

<table>
<thead>
<tr>
<th>Reviewer Name</th>
<th>Title / Role / Directorate</th>
<th>Version</th>
<th>Date Sent to Reviewer</th>
<th>Date Feedback Received</th>
<th>Feedback Actioned (Y/N ?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anthony Wilson</td>
<td>Technical Product Manager Identity &amp; Access Services</td>
<td>2.0</td>
<td>01/12/2018</td>
<td>21/12/2018</td>
<td>Y</td>
</tr>
<tr>
<td>Hazel Randall</td>
<td>Head of Legal</td>
<td>2.1</td>
<td>08/01/2019</td>
<td>08/01/2019</td>
<td>Y</td>
</tr>
<tr>
<td>Mike Partridge</td>
<td>National RA Manager</td>
<td>2.3</td>
<td>23/01/2019</td>
<td>28/01/2019</td>
<td>Y</td>
</tr>
<tr>
<td>Andy Smith</td>
<td>Principal Security Specialist</td>
<td>2.3</td>
<td>31/01/2019</td>
<td>01/02/2019</td>
<td>Y</td>
</tr>
</tbody>
</table>

*This document must be quality assured by the Directorate PMO before approval by the SRO and NHS Digital Executive Portfolio Director before submission to the NHS Investment Sub-Group.

Approved by

This document has been approved by the following people:

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Title</th>
<th>Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gareth Thomas</td>
<td></td>
<td>Senior Responsible Owner (SRO)*</td>
<td>17/01/2019</td>
<td>2.3</td>
</tr>
<tr>
<td>Andrew Meyer</td>
<td></td>
<td>Executive Portfolio Director*</td>
<td>17/01/2019</td>
<td>2.3</td>
</tr>
<tr>
<td>Mike Walker</td>
<td></td>
<td>Programme Head</td>
<td>17/01/2019</td>
<td>2.3</td>
</tr>
<tr>
<td>Philip Gill</td>
<td></td>
<td>Portfolio Item Manager</td>
<td>17/01/2019</td>
<td>2.3</td>
</tr>
<tr>
<td>Integrating Care</td>
<td></td>
<td></td>
<td>17/01/2019</td>
<td>2.3</td>
</tr>
<tr>
<td>Programme Board</td>
<td></td>
<td></td>
<td>17/01/2019</td>
<td>2.3</td>
</tr>
</tbody>
</table>

*This document must be approved by the SRO and relevant NHS Digital Executive Portfolio Director.

Glossary of Terms

<table>
<thead>
<tr>
<th>Term / Abbreviation</th>
<th>What it stands for</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>AAL</td>
<td>Authentication Assurance Level</td>
</tr>
<tr>
<td>NHS Identity</td>
<td>Strategic Identity Service for health &amp; social care created as part of NIB 2020</td>
</tr>
<tr>
<td>FIDO</td>
<td>Fast Identity Online</td>
</tr>
</tbody>
</table>

Document Control:
The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.
# Contents

1 Introduction 5  
   1.1 Purpose of Document 5  
   1.2 Background 5  
2 Registration Authority Hierarchy 6  
3 Creation of a national digital identity 7  
4 Roles & Responsibilities 8  
5 Requirements in relation to Smartcards and other approved devices and authentication methods 9  
6 Local RA Policy 10  
7 Failure to comply with policy requirements 11  
   Appendix 1 – RA Manager Responsibilities 12  
   Appendix 2 – RA Agent Responsibilities 13  
   Appendix 3 – Sponsor Responsibilities 14
1 Introduction

1.1 Purpose of Document

National IT systems for health need to ensure that users of these systems are identified correctly and are given appropriate access. This is achieved by identity verification and creating a national digital identity for each user. The process to doing doing this uses local ‘Registration Authorities’ which consist of people and processes who are trained to create identities and grant access. This policy covers these services.

This policy replaces the Registration Authority Policy issued on 2 September 2014.

As part of the NHS Identity Project, Registration Authority (RA) policy requires updating to ensure that it supports the modern delivery of health and social care across boundaries and in multiple locations whilst ensuring staff have access to appropriate, up to date, clinical information at the point of need. Details of the project aims and developments can be found at https://digital.nhs.uk/services/nhs-identity. The key elements of the policy that have been updated relate to:

- The use of a new, more modern identity verification standard, GPG45, to replace e-Gif Level 3.
- The ability to use other authentication methods alongside NHS Digital issued Smartcards, the only approved physical Smartcard (to meet technical requirements for production of card and authentication). Other authentication methods will be allowed provided they meet the National Institute of Systems and Technology (NIST SP800 – 63 Digital Identity Guidelines, available at https://pages.nist.gov/800-63-3/), and are approved by the FIDO alliance as a FIDO2 approved authentication method (see section 5 for further detail).

This document lays out the RA Policy requirements which every organisation that has a Registration Authority needs to adhere to. It is based on the original Department of Health (DH) Gateway document (reference number 6244) ‘Registration Authorities: Governance Arrangements For NHS Organisations’, the NHS Care Record Guarantee, GDPR requirements, and RA good practice guidance. 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:


1.2 Background

This document outlines:

- The RA Hierarchy and the principle of delegated authority to local organisations to run their RA.
• The requirements for creating a nationally verified digital identity.
• The roles and responsibilities within organisations that run their own Registration Authority activity
• Requirements in relation to authentication, and authentication methods including Smartcards and other approved devices
• The requirement to develop and implement a local RA Policy.

2 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 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.

This policy document outlines the full range of mandatory requirements for an organisation 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.

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.

3. RA Managers within organisations running their own RA activity are accountable for the running of RA activity in their organisation. They need 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 these 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.
3 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 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 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:

1. 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.

2. 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 IG 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/your-workforce/recruit/employment-checks/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.

3. 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.

4. Smartcards (or other AAL3 (Authenticator Assurance Levels) mechanisms) 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. GPG 45 outlines four levels of identity assurance. NHS Identity will support these four levels of identity assurance. In practice NHS Identity 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.

4 Roles & Responsibilities

In order to discharge the responsibilities delegated from NHS Digital 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 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.

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.

<table>
<thead>
<tr>
<th>RA Manager CANNOT delegate</th>
<th>RA Manager CAN delegate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Responsibility for running RA Governance in their organisation</td>
<td>• 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</td>
</tr>
<tr>
<td>• 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</td>
<td>• 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</td>
</tr>
<tr>
<td>• Assignment of RA Agents and sponsors and the registration of RA Agents and Sponsors</td>
<td>• The implementation of the local auditing process</td>
</tr>
<tr>
<td>• Training of RA Agents and Sponsors and ensuring they are competent to carry out their roles and adhere to policy and process</td>
<td></td>
</tr>
<tr>
<td>• The training of RA Agents and Sponsors and ensuring they are</td>
<td></td>
</tr>
</tbody>
</table>
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

| 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 |

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

A full list of RA policy responsibilities for RA Managers, RA Agents and Sponsors is contained at Appendices 1-3 of this document

5 Requirements in relation to Smartcards and other approved devices and authentication methods

NHS Digital will allow a range of identity tokens in addition to centrally issued 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/](https://pages.nist.gov/800-63-3/)), this describes the cryptographic strength of authentication methods that is required to access sensitive data. In addition, devices and authentication methods need to meet FIDO 2 standards for how devices utilise the required cryptography (available at [https://fidoalliance.org/](https://fidoalliance.org/)) and must be accredited by the FIDO alliance. Any 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.

Smartcards and other approved devices and authentication methods 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:

1. Smartcard, device or other approved authentication method 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 Smartcard/Security Key getting to or a device being linked to the right person. It is also a Public Key Infrastructure requirement for these reasons.

2. Local organisations must assure themselves that they have a robust and secure process in place to ensure that the Smartcard, device or other approved authentication method reaches all non RA end users for whom it is intended. This is important to avoid individuals potentially gaining access to patient data when they are not the person entitled to do so.


4. Only the end user for whom the Smartcard, device or other approved authentication method is intended should know their passcode for their Smartcard/Device, no-one else should, including RA staff. If anyone else knows the end users passcode it breaches the Smartcard/Authorised Device terms and conditions of use and the Computer Misuse Act 1990.

5. When Smartcards and other approved devices and authentication methods 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 Smartcard. Users of other authentication devices or methods will return these devices to their organisation before they leave.

6. It is mandatory that users sign the Terms & Conditions of Smartcard/Authorised Device 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.

7. 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. 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 Local RA Policy**

It is a mandatory requirement that organisations that run local RA activity have a local policy outlining their approach. The following are mandatory requirements within the local organisation’s policy.
1. The name of the Board/EMT accountable person and the RA Manager within the organisation must be named within the policy. The policy needs to outline the governance requirements placed upon these individuals. The local organisation’s policy must be updated to reflect any changes to the named individuals.

2. The policy must describe how access rights will be granted and revoked in a timely way, ensuring that requirements for staff to be able to access electronic records in a timely way can be met and that individuals do not retain access within an organisation once they have left that organisation.

3. The policy must not contradict the mandatory requirements contained within this national RA policy document. At a minimum the policy must cover:
   i. Governance arrangements
   ii. A demonstration of the adherence to this policy document requirements in relation to the verification of identity
   iii. Roles & responsibilities
   iv. Smartcard and other approved devices use

4. The policy must be formally signed off by the organisation at an appropriately senior level, e.g. the EMT, the IG Committee on a delegated authority basis, etc.

7 Failure to comply with policy requirements

Where NHS Digital is notified of significant breaches to this policy they will consider the situation and take appropriate remedial action. This will include discussing the situation with the organisation, but may result in discussions with regulatory or professional bodies depending upon the seriousness of the situation.
Appendix 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 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 RA Policy and RA Processes locally adhering to national guidance's

- 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
Appendix 2 – RA Agent Responsibilities

• Verify users ID to GPG45 Level 3 or 4
• Register users and provide them with Smartcards and other registered devices
• 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 terms and conditions of Smartcard/Authorized Security Device usage
• 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 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
Appendix 3 – Sponsor Responsibilities

- Can raise requests for new users
- Approve users assignment to access control positions, or,
- Directly assign users under position management
- Unlock Smartcards and renew smartcard certificates for non-RA staff
- DO NOT verify users ID