Document filename: RA Policy Document			
Directorate / Programme	Operations & Technical Services – Spine 2 Programme	**Project**	Spine 2 – IAM Replacement project
Document Reference		<insert>	
Project Manager		**Status**	
Owner	John Winter	**Version**	V1.0
Author	Philip Gill	**Version issue date**	2 September 2014

Registration Authority Policy

Document Management

Revision History

Version	Date	Summary of Changes
V0.1	4 August 2014	Initial draft
V0.2	5 August	Revised draft
V0.3	8 August	Revised draft for discussion
V0.4	14 August	Revised following review comments
V1.0	2 September	Final approved version

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Access Control Team		August 2014	V0.4
IAM Team		August 2014	V0.4
National RA Team		August 2014	V0.4

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
John Winter		Senior Project Manager - Access Control	02/09/14	V1.0
Stephen Smith		Programme Head - Demographics & NHS Number, Access Control & National Registration	02/09/14	V1.0

Glossary of Terms

Term / Abbreviation	What it stands for

Document Control:

The controlled copy of this document is maintained in the HSCIC 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

1.1 Purpose of Document

As part of the IAM replacement Project RA policy requires updating to ensure it is clear and aligned with the Care Identity Services application. 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 DH Gateway document (reference number 6244) 'Registration Authorities: Governance Arrangements For NHS Organisations', the NHS Care Record Guarantee, the Data Protection Act 1998, and requirements contained in the HSCIC RA Process Guidance together with IG Toolkit requirements in relation to Registration Authorities.

1.2 Background

This document outlines:

1.2.1 The RA Hierarchy and the principle of delegated authority to local organisations to run their RA.

1.2.2 The requirements for creating a nationally verified digital identity.

1.2.3 The roles and responsibilities within organisations that run their own Registration Authority activity

1.2.4 Requirements in relation to Smartcards

1.2.5 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 (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 the minimum national requirements to provide such assurance: as such deviation from this 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 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/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 & Sponsors are appointed by the Board/EMT 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.

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 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

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

3 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:

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 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.

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.

4 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 new Registration Authority software, Care Identity Services, which is due to replace current software in the autumn of 2014, 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 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	❖ 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 ❖ 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

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. Local organisations must assure themselves that they have a robust and secure process in place to ensure that the Smartcard reaches all non RA end users for whom it is intended. This is of particular importance when issuing a Smartcard to someone at a different location from the RA operations. Failure to do so can result in an individual receiving a card and potentially gaining access to patient data when they are not the person entitled to do so.

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 an organisation 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.

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 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 HSCIC is notified of significant breaches to this policy it 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.

8 Appendix 1 – RA Manager Responsibilities

- RESPONSIBLE for running RA Governance in their organisation – 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 access rights, modifications to access and people 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
- Verifies user's ID to e-GIF level 3 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

9 Appendix 2 – RA Agent Responsibilities

- Verify users ID to e-GIF level 3 and NHS Employer standards
- 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 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, assignment of access rights, modifications to access and people and certificate renewal and card unlocking

10 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