Tees, Esk and Wear Valleys
NHS Foundation Trust

ⓘ **Public – To be published on the Trust external website**

Registration Authority Policy

Ref: IT-0011-v7

Status: Ratified
Document type: Policy

Contents

1 Introduction

The use of the Care Identity System (CIS), commonly known as Smartcards is national system operated by Health and Social Care Information Centre (HSCIC). HSCIC require all organisations that use smartcards to authenticate users identity follow strict policies and procedures to ensure the confidentiality and common security standards are maintained.

Virtual and Physical (utilised by Prison staff to access TEWV systems) smartcards are also used to gain access to systems such as CIS, ESR, SystmOne, summary care record, printers, and the Spine integration.

The process of gaining access is called National Programme Registration and the primary method by which users are allowed to access a Health and Social Care Information Centre (HSCIC) application is via a smartcard, these are either Virtual or for Prison Service Staff a Physical Smartcard issued during the Registration Process.

This policy is critical to the delivery of OJTC and our ambition to co-create safe and personalised care that improves the lives of people with mental health needs, a learning disability or autism. It helps us deliver our three strategic goals as follows:

This policy supports the trust to co- create a great experience for all patients, carers and families from its diverse population by ensuring access to the care is right for you, through staff accessing NHS information resources through the CIS.

This policy supports the trust to co-create a great experience for our colleagues by ensuring that staff requiring access are vetted correctly and ensuring that only staff that require access have that access to the CIS resource.

2 Why we need this policy

2.1 Purpose

With the use of Smartcards and to comply with National Registration Authority Policy we are required to maintain a Local Registration Authority Policy which identifies the roles and responsibilities as well as the access and identity verification controls that re in place in the Organisation.

2.2 Objectives

- Outline how access to smartcards is granted
- Outline how identities are verified by RA agents
- Outline the appropriate procedures and use of Smartcards

3 Scope

This Policy applies to all processes, procedures and activities carried out by the RA in relation to use of smartcards and CIS.

3.1 Who this policy applies to

This policy applies to all TEWV departments and staff.

3.2 Roles and responsibilities

Role	Responsibility
Board/Executive Directors Meeting Accountable individual	The Director of Finance and Information has the overall accountability for the implementation and operation of RA at TEWV. Responsibilities include; • Annual Reporting of RA activity to the trust
Registration Authority Manager (RAM)	At TEWV the RA Manager (currently the Corporate Systems Manager) is responsible for • Responsible for running RA Governance at TEWV • 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 guidelines • 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
Deputy Registration Authority Manager (DRAM)	At TEWV the Deputy RA Manager is responsible for deputising for the RA Manager when they are unavailable. The Corporate Systems Administrators (RAA Agent) act in to this role
Registration Authority Agent Advanced (RAA Agent)	At TEWV the RAA Agents are the Corporate System Administrators, they are responsible for: • Advanced configuration and batch uploads • Ensuring that the national and local processes are followed, • Registration Authority Agents and LSA's are appropriately trained and supported in their role

	• Responsible for ensuring users are compliant with the terms and conditions of Smartcard usage • Responsible for the security of (old) paper-based RA records • Ensure all service issues are raised appropriately locally and nationally
Registration Authority Agent (RA Agent)	At TEWV the RA Agents are limited to the Service Support Officers, Medical Staffing for clinical rotations only, and Temporary Staffing for Bank workers they are responsible for; • Creating and Cancelling Smartcards • Register users and provide them with NHS Smartcards and other registered devices • Renew NHS Smartcard certificates for users if self-service functionality not used • Advanced user actions and reports • Verify users ID to GPG45 Level 3 or 4 • Grant users access assignment • 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
Local Smartcard Administrators (LSA's)	At TEWV the LSA's are nominated by relevant business units to the RAA Agent by appointment, they are responsible for; • Unlocking and renewing certifications on smartcards

4 Policy

4.1.1 Gaining Access

How to acquire and gain access to smartcards will be contained the Smartcard (CIS) Procedure.

⚠ **How to acquire a smartcard is outlined in the Smartcard (CIS) Procedure which is available on Trust Intranet**

4.1.2 Removing Access

When leaving TEWV, most employees should retain their Smartcards, this includes people moving NHS organisations, leaving the NHS and retiring. Smartcards can be utilised at other NHS organisations and the possibilities of employees later returning to the NHS and returning from retirement.

Only in rare circumstances should the smartcard be returned i.e., Death in Service. In these circumstances, smartcards should be returned to the line managers and destroyed in confidential waste. The manager should then log a call with the Information Service Centre saying that the card has been destroyed.

4.1.3 Identity Verification

The 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 GPG45 Levels 3 and 4 which provides assurance that the identity is valid across any organisation an individual works within.

Trust staff who have the protected characteristic of ‘Gender Reassignment’ where their identification doesn’t match their current name can contact Rebekah Stamp or Theresa Roberts who can confidentially review their identification, process their applications and issue their card.

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, RA Advanced Agents or 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/your-workforce/recruit/employment-checks/nhs-employment-check-standards/identity-checks

4. NO other documents are approved for verification of identity, including those contained within other NHS Employers standards.
   a. 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.

4.1.4 Smartcard Delivery by Post

Following the printing of a smartcard, it's permissible for a locked smartcard to be issued and posted to the requestor. The requestor must subsequently visit an LSA to unlock the card.

Under no circumstances should unlocked smartcards be posted to users.

⚠ **The list of Local Smartcard Administrators is available on the Trust Intranet.** Smartcards | TEWV Intranet

4.1.5 Pin Code

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.

⚠ **Under no circumstances should you allow anyone else to access the system using your Smartcard and pincode. Disclosure of passcodes to others could lead to disciplinary action**

4.1.6 Leaving / End Date

All smartcards will be disassociated from TEWV automatically when the employment end date is populated in ESR by managers. This will revoke access to all TEWV associated systems.

4.1.7 Failure to comply with this policy

This policy has been developed from National RA Policy, failure to comply would require the HSCIS to be informed to consider the situation and take appropriate remedial action. This could include discussions with the Organisation and with other regulatory or professional v bodies by HSCIC.

The trusts Disciplinary Procedure should be used where staff have failed to adhere to this procedure.

5 Definitions

Term	Definition
Registration Authority	An individual or team that is responsible for managing the registration and access control processes required to ensure that individuals who need to access the NHS Care Records Service or other NHS Digital services have had their identity checked and are assigned appropriate access.
Smart Cards	A smart card is the size of a credit card, that incorporates a Chip, holding the users profile details. Smartcards are needed to use the NHS Care Record Service and other National Programme for IT (NPfit) services whilst protecting the security and confidentiality of patient's healthcare information.
Role Based Access Control (RBAC)	Use of pre-defined roles as an intermediary between an individual and the system. Permissions are assigned to

	roles which are in turn assigned to individuals and extended to include other related attributes such as; Area of Work and Business Function/Activities.

6 Related documents

- Managing concerns of potential conduct procedure (Disciplinary Procedure)
- Records Management Policy
- Minimum standards for corporate record keeping procedure
- Information Security and Risk Policy
- Smartcards (CIS) SSP
- Smartcards (CIS) Procedure

7 How this policy will be implemented

- This policy will be published on the Trust's intranet and Trust website
- Circulated to all RA Agents and included in inductions

7.1 Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
Publish policy to the Trust intranet and website	Making the most up to date version available	As soon as policy is approved	Corporate Systems Team	Once published, ensure the policy can be opened
Send link to new policy	RA Agents have the most up to date policy	As soon as policy is published	RA Manager	Ask all RA Agents to confirm they have read the updated policy

7.2 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
ID-Checkers	ID Checker E-Learning	1 hour	Once
RA Agent	RA Authority E-Learning	1 Hour	Every 3 years

8 How the implementation of this policy will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	All ID checkers have completed ID checker e-learning training	Ad Hoc on application for ID checker status/ESR check/Corporate Systems Officer	Corporate Systems Huddle
2	RA Authority E-Learning	Every 3 years/e-learning/RA Agents	Compliance is monitored via reporting in ESR

9 References

- The Data Protection Act 1998
- The Computer Misuse Act 1990
- E Communications Act 2003
- Electronic Signatures Regulations 2002
- NHS Confidentiality Code of Practice
- The Records Management NHS Code of Practice
- The Freedom of Information Act 2000
- The NHS Care Record Guarantee for England (PDF, 128.2kB)
- The Code of Practice for the Management of Confidential Information

- Verification of Identity Checks - http://www.nhsemployers.org/your-workforce/recruit/employment-checks/nhs-employment-check-standards/identity-checks
- National RA policy: http://nww.hscic.gov.uk/rasmartcards/docs/rapolicyv1sep14.pdf
- National Smartcard policy and strategy: Registration authorities and smartcards - NHS Digital
- Registration Authorities Governance Registration Authority governance - NHS Digital
- *NHS Confidentiality Code of Practice* Confidentiality: NHS Code of Practice - GOV.UK (www.gov.uk)
- *Registration Authorities Operational Process and Guidance* Registration authorities and smartcards - NHS Digital

10 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	14 December 2022
Next review date	14 December 2025
This document replaces	IT-0011-v6.1
This document was approved by	DPAG
This document was approved	05 October 2022
This document was ratified by	Executive Directors Meeting
This document was ratified	14 December 2022
An equality analysis was completed on this policy on	13 May 2022
Document type	Public
FOI Clause (Private documents only)	N/A

Change record

Version	Date	Amendment details	Status
7	14 Dec 2022	Full review with changes including:- • added to new template • Clarified roles and responsibilities	Ratified

		- Addition of confidential process to support staff with protected characteristic of gender reassignment	

Appendix 1 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	**Scope**
Name of service area/directorate/department	Digital and Data Services
Title	Registration Authority Policy
Type	Policy
Geographical area covered	Trust Wide
Aims and objectives	To comply with National Registration Authority Policy
Start date of Equality Analysis Screening	13/04/2022
End date of Equality Analysis Screening	13/05/2022

Section 2	**Impacts**
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	All Trust staff and patients
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO** • **Gender reassignment** (Transgender and gender identity) **Yes** • **Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO**

	- **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** - **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** - **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** - **Veterans** (includes serving armed forces personnel, reservists, veterans and their families) **NO**
Describe any negative impacts	A staff member who is transgender but has not legally changed name/gender would have to provide their legal identity documentation which means that they will have to out themselves. This has been identified as a possible negative impact for staff who have the protected characteristic of 'Gender Reassignment'. Currently there is no alternative process that trans staff can access. There are 2 service desk staff members that have been identified and can be sign posted to, Theresa Roberts and Rebekah Stamp to ensure that there is a confidential process for staff to follow and to ensure that access to this information is only available to those staff members that need access to it which will be a limited number of staff.
Describe any positive impacts	Any staff member who is transgender but has not legally changed name/gender can have a smartcard issued with a 'known as' name which means that the staff members preferred name would be shown on the card only alongside a current photo of themselves.

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of	See Reference section

practice, best practice, nice guidelines, CQC reports or feedback etc.)	
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	Previous versions of this policy have been consulted across all Trust staff. This current version has had a full six-week Trust wide consultation. This policy will be reviewed by IMM, DPAG, MG (or ED)
If you answered No above, describe future plans that you may have to engage and involve people from different groups	N/A

Section 4	**Training needs**
As part of this equality analysis have any training needs/service needs been identified?	no
Describe any training needs for Trust staff	no
Describe any training needs for patients	N/A
Describe any training needs for contractors or other outside agencies	N/A

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	**Yes / No / Not applicable**	**Comments**
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	System administrator/Corporate manager
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	Historic consultation + sent out for full six week trustwide consultation
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	SSP
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	

	Title of document being reviewed:	Yes / No / Not applicable	Comments
7.	**Implementation and monitoring**		
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	IMM, DPAG, MG (or ED)
10.	**Publication**		
	Has the policy been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	Public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	N/A	