Public – To be published on the Trust external website

SmartCards – Care Identity Management (CIM) Procedure

IT-0031-006-v4

Status: Approved
Document type: Procedure

Contents

1 Introduction

The use of the Care Identity Management (CIM), commonly known as SmartCards is national system operated by NHS Digital. NHSE 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.

The process of gaining access is called National Programme Registration and the primary method by which users are allowed to access a NHS Digital application is via a SmartCard, these are either Virtual or for Prison Service Staff a Physical SmartCard issued during the Registration Process.

This procedure aligns with and supports the delivery of Our Journey To Change: the next chapter.

2 Purpose

This document provides regulations and guidance for the specific access, security and use of the Care Identity Management (CIM) System in use within Tees, Esk and Wear Valleys NHS Foundation Trust. Misuse of your SmartCard can compromise the Trust's confidential information, staff information and otherwise adversely affect the Trust's interests and reputation.

This procedure when implemented should reflect anti-discriminatory practice. Any services, interventions or actions must take into account any needs arising from a person's protected characteristics.

Please note there are some services within the Trust that use alternative electronic systems. This document only relates to the use of CIM.

3 Who this procedure applies to

This procedure applies to all TEWV departments and staff.

4 Related documents

This procedure describes what you need to do to implement the Registration Authority Policy.

This procedure also refers to:-

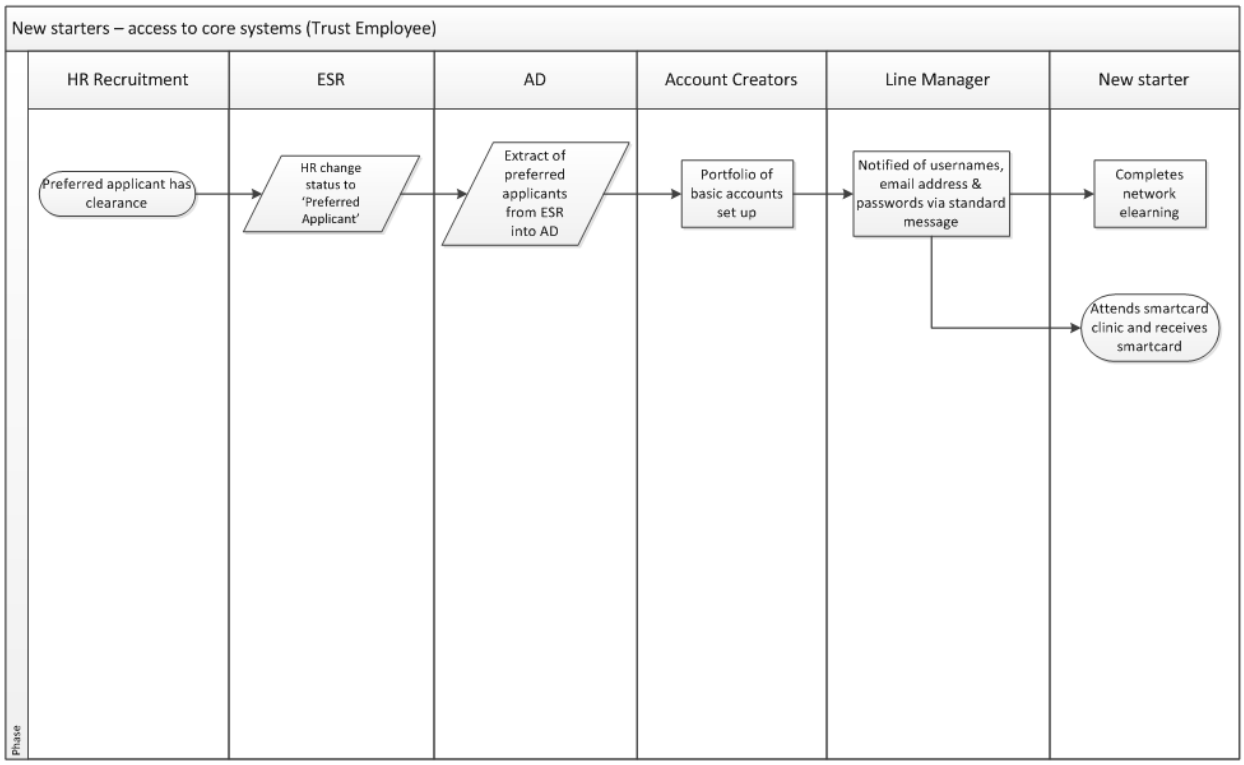
- Human Rights, Equality, Diversity & Inclusion policy.
- Disability, Race and Gender Equality Schemes
- Information Security & Risk policy
- Access to information systems policy
- Minimum standards for record keeping
- CIM System Specific Policy
- RA Operation and Policy Guide

5 Using the System

All trust staff employees are set up in the Electronic Staff Record (ESR) system, which automatically integrates with CIM. They can be issued with a SmartCard, either virtual or a Physical SmartCard for Prison Service staff which can enable access to the following integrated applications dependent on the relevant permissions being associated to their account:

- Secondary Uses Service (SUS)
- ESR
- Choose and Book/NHS e-Referral Service
- Batch Tracing
- SystemOne
- Summary Care Record - Demographics
- Summary Care Record – Clinical

5.1 Access to CIM/SmartCard



5.2 Obtaining a SmartCard

For new members of staff, the new members of staff individual's line manager or the user should contact a SmartCard administrator to request a SmartCard. A list of administrators can be found on the SmartCard page of the Trust intranet. Prior to a card being issued the new starter must have successfully completed network training.

The SmartCard system, CIM is a national system allowing access to secure information systems which contain staff and patient identifiable information. SmartCards can be used across NHS organizations, and as such have stringent verification protocols which must be adhered to when being issued.

If you are attending an appointment for a new SmartCard, it is mandatory to bring the following ID to the appointment:

> ⚠ 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.

If you do not bring the required evidence your card may not be able to be issued.

- Photographic identity: Passport and/or Full Driving Licence (inc. paper counterpart)
- 2 documents with name and address within the last 3 months, i.e. utility bills, council tax, photo driving licence (if using passport as photo ID), financial statement, tenancy agreement
- If you require access to Summary Care Records (SCR), please ensure that you have completed your SCR training prior to booking an appointment

Once issued with a physical SmartCard it is YOUR responsibility to keep it safe and secure and report if it is lost or stolen promptly.

5.3 Becoming a Local SmartCard Administrator

Local Administrators are SmartCard users, with elevated permissions. They can assist users with resetting pin numbers or unblocking SmartCards.

To become a local system administrator the line manager should Log a SmartCard Request on the Service Desk Portal and nominate a staff member from their team to be a local administrator. The nomination is then reviewed by the Corporate Systems team and approved if deemed a business need, guidance will be sent by email.

A list of local SmartCard administrators is available on the intranet.

5.4 Leaving TEWV/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 managers and destroyed. The manager should then log a call with the Digital & Data Service Desk saying that the card has been destroyed.

Access via the SmartCards is removed as part TEWV's leavers process.

5.5 Passcode/Pin Numbers

A SmartCard requires users to use a passcode to authenticate at each use. The passcode is determined by the individual at the point the SmartCard is created/unblocked.

You can change your Pin Number at any time by accessing the CIM on the NHS Spine Portal and accessing the 'My Profile' option.

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

5.6 Security

It is essential alongside all existing Information System Policies that you adhere to the following SmartCard security principles:

- Do not allow other users to utilise your SmartCard
- Never share your SmartCard passcode.
- Do not leave your SmartCard in the reader unattended - even if your workstation is locked

Line managers are responsible for ensuring that staff members have undertaken and passed relevant mandatory and statutory training and are aware of the organisations policies and procedures, especially related to information security. This will ensure they understand the Trusts data governance, legal and ethical requirements for protecting and accessing personal information. Trust terms and conditions of employment include adherence to Information governance standards, information security requirements, code of confidentiality and common law of confidentiality.

5.7 Lost, stolen or damaged cards

If a SmartCard has been lost, stolen or damaged:

- Log a call with the Service Desk ASAP stating what has happened to your card
- Raise an incident on Inphase
- Your card will be cancelled as a matter of urgency if it has been lost or stolen

Failure to raise an Inphase incident when a card has been lost or stolen is a disciplinary offence.

5.8 Passcode resets, forgotten pins and blocked cards

You can change your Passcode at any time but it is essential to do this if you think it has been compromised Access the CIM on the NHS Spine Portal and selection the 'My Profile'

option and follow the on screen instructions to change your PIN. Further guidance on how to do this is available on the intranet.

If you have forgotten, your pin or your card has been blocked when exceeding three invalid login attempts you will need to visit a local SmartCard administrator. A list of Local SmartCard Administrators across the trust is available on the intranet.

5.9 Certificate Expiry and Renewal

Every two years the CIM system needs to revalidate and certify that users are still at the Trust. This process is called certification and can be carried out by the user who self-certifies that they are still an employee at the Trust and require a SmartCard. When a user is approaching 90 days to the renewal period, a notification will be displayed. At 60 days before the user can self-certify by following the on-screen prompt. This process will take several minutes.

If a SmartCard has not been used for a significant amount of a time or the user fails to self-certify within the 60-day period, the certificates will expire. In these cases, the user is required to log a support call to request a replacement card following the process in section 3.1.2.

A user can only recertify twice and after 6 years, a face-to-face certification with a Local SmartCard Administrator is required to verify you still work at TEWV.

6 Managing the CIM System

6.1 Planned downtime

There are clear service standards to monitor planned downtime for the CIM system to enable maintenance. In the main, this will be planned well in advance and notice given to system users to make alternative arrangements as defined by service business continuity plans. The system will generally be available 24 hours per day from trust-networked sites.

6.2 Emergency downtime

There could be rare occasions where the system is unavailable and it is impossible to give prior notice. On these occasions, users should inform the Information Service Centre and you should invoke your Business Continuity Plan.

These plans should cover the eventuality that a user is unable to authenticate to any of the associated CIM. These may include, but not be limited to, the use of other trust locations to access systems, use of reciprocal agreements with other trusts or use of manual paper systems in the interim period prior to fault resolution being achieved. All operational areas should hold signed, up to date business continuity plans.

7 CIM System Monitoring

The CIM system is fully auditable and access is monitored.

Staff records for the use of CIM authentications are restricted to those who are defined as the individuals 'line manager' and can provided on request.

8 Audit

SmartCard use is continuously audited and the types of audits will include;

- Auditing staff who have not been issued with a SmartCard
- Authentications, failed authentications and overall SmartCard usage
- Auditing of users with multiple cards.
- Any other audit to check the system is being used appropriately and securely may be conducted.

9 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 NHS Digital services whilst protecting the security and confidentiality of patient's healthcare information.

10 How this procedure will be implemented

- This procedure will be published on the Trusts intranet and Trust website and will be circulated to all RA Agents and included in inductions

10.1 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

11 How the implementation of this procedure 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

12 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 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
- NHS Code of Confidentiality
- NHS Employers Identity Checks
- NHS Digital Registration Authority Policy
- NHS Digital Registration Authorities Operational Process and Guidance

13 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	10 November 2025
Next review date	10 November 2028
This document replaces	IT-0031-006-v3
This document was approved by	DPAG
This document was approved	10 November 2025
This document was ratified by	n/a
This document was ratified	n/a
An equality analysis was completed on this policy on	21 October 2025
Document type	Public
FOI Clause (Private documents only)	N/A

Change record

Version	Date	Amendment details	Status
v3	01/06/2022	Full review with amendments, includes:- • transferred to new template • re-wording throughout • Addition of confidential process to support staff with protected characteristic of gender reassignment	Withdrawn
v4	10 Nov 2025	Full review • Updated CIS (Care Identity Service) to CIM (Care Identity Management) • Updated Policies and links	Approved

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	SmartCards – Care Identity Management (CIM) Procedure
Type	Procedure
Geographical area covered	Trust Wide
Aims and objectives	Provide information and appropriate use and access to SmartCards / CIM.
Start date of Equality Analysis Screening	21/10/2025
End date of Equality Analysis Screening	21/10/2025

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, Heterosexual, Pansexual and Asexual 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 policy will be reviewed by DPAG
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	Corporate manager
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	SSP Registration Authority Policy
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	Approved by E&D team 02 Dec 2025 (ah)
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	DPAG
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	