Tees, Esk and Wear Valleys
NHS Foundation Trust

Smartcards – Care Identity Service (CIS) Procedure

IT-0031-006-v2

Status: Approved
Document type: Procedure
Overarching Policy: Access to Information Systems Policy

Contents

1. Purpose

This document provides regulations and guidance for the specific access, security and use of the Care Identity Service (CIS) 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 race, gender, age, religion and belief, communication, sensory impairment, disability and sexuality.

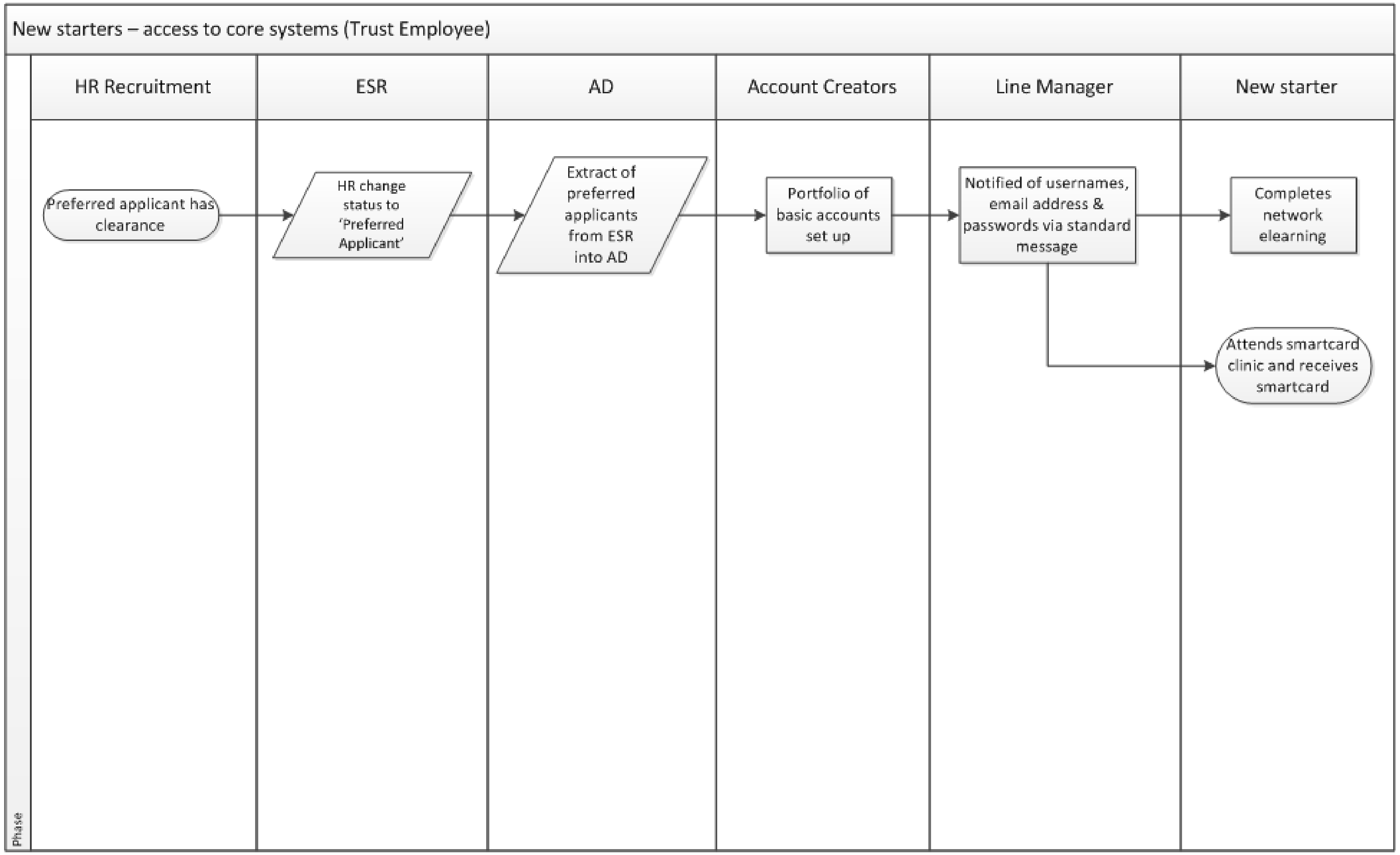
⚠ **Please note there are some services within the Trust that use alternative electronic systems. This document only relates to the use of CIS.**

2. Related documents

- Human Rights and Equality & Diversity policy, Equality Analysis Policy, Equality Analysis Guidance
- Disability, Race and Gender Equality Schemes
- Information Security policy
- Data Management Policy
- Access to information systems policy
- NHS Code of Confidentiality
- Confidentiality code of practice
- Minimum standards for record keeping
- CIS System Specific Policy
- Access to Systems Policy
- RA Operation and Policy Guide
- NHS Employers Identity Checks
- HSCIC Registration Authority Policy
- HSCIC Registration Authorities Operational Process and Guidance

3. Using the system

3.1. Access to CIS/Smartcard


New starters – access to core systems (Trust Employee)
HR Recruitment
ESR
AD
Account Creators
Line Manager
New starter
Preferred applicant has clearance
HR change status to 'Preferred Applicant'
Extract of preferred applicants from ESR into AD
Portfolio of basic accounts set up
Notified of usernames, email address & passwords via standard message
Completes network elearning
Attends smartcard clinic and receives smartcard
Phase

3.1.1. Who can be issued with a Smartcard?

All trust staff employees are set up in the Electronic Staff Record (ESR) system, which automatically integrates with CIS. They can be issued with a smartcard, which can enable access the following integrated applications dependent on the relevant permissions being associated to their account;

- Secondary Uses Service (SUS)
- ESR
- Choose and Book
- Batch Tracing
- SystmOne
- Summary Care Record - Demographics
- Summary Care Record – Clinical

3.1.2. Obtaining a Smartcard

For new members of staff, the new members of staff individual's line manager or the user books directly onto the new starter onto a Smartcard clinic on InTouch. Prior to the appointment new starter must have successfully completed network training.

The smartcard system, CIS 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 strident 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: 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 Smartcard it is YOUR responsibility to keep it safe and secure and report if it is lost or stolen promptly.**

3.1.3. 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 an LSA 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 InTouch.

3.1.4. 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 utilized 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 Information Service Desk saying that the card has been destroyed.

Access via the smartcards is removed as part of the organisations leavers' process.

3.2. 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 CIS 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**

4. 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 utilize 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 organizations 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.

4.1. 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 Datix
- Your card will be cancelled as a matter of urgency if it has been lost or stolen

⚠ **Failure to raise a Datix incident when a card has been lost or stolen is a disciplinary offence.**

4.2. 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 CIS 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 InTouch.

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 InTouch.

4.3. Certificate Expiry and Renewal

Every two years the CIS 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 from Supporting Users.

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.

5. Managing the CIS System

5.1. Planned downtime

There are clear service standards to monitor planned downtime for the CIS 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.

5.2. 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 CIS. 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.

6. CIS System Monitoring

The CIS system is fully auditable and access is monitored.

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

7. Audit

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

- Auditing staff who have not being 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.

8. Document control

Date of approval:	07 November 2018	
Next review date:	07 May 2022	
This document replaces:	None	
Lead:	Name	Title
	Niall Evans	Systems Manager (Corporate)
Members of working party:	Name	Title
	Kendra Smith Dom Prest	System Administrator (Corporate) System Administrator (Corporate)
This document has been agreed and accepted by: (Director)	Name	Title
	Patrick McGahon	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Digital Safety and Information Governance Board	07 November 2018
An equality analysis was completed on this document on:	01 November 2018	

Change record

Version	Date	Amendment details	Status
1	Sep 2015	Initial Draft	Published
2	Nov 2018	Reviewed and updated	Approved
	Jul 2020	Review date extended 6 months	

9. Equality Analysis Screening Form

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc	Information					
Name of responsible person and job title	Niall Evans – System Manager (Corporate)					
Name of working party, to include any other individuals, agencies or groups involved in this analysis	N/A					
Title	CIS / Smartcard Procedure					
Is the area being assessed a	Policy/Strategy	X	Service/Business plan		Project	
	Procedure/Guidance				Code of practice	
	Other – Please state					
Geographical area	Trust Wide					
Aims and objectives	Provide information and appropriate use and access to Smartcards / CIS.					
Start date of Equality Analysis Screening	01/11/2018					
End date of Equality Analysis Screening	01/11/2018					

Please read the Equality Analysis Procedure for further information

You must contact the E&D team if you identify a negative impact. If you require further advice and support please ring Sarah Jay on 0191 3336267/3542

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?
All System Users, Information Department
2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?

Race (including Gypsy and Traveller)	No	**Disability** (includes physical and mental impairment)	No	**Sex** (Men and women)	No
Gender reassignment (Transgender and gender identity)	No	**Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual)	No	**Age** (includes, young people, older people – people of all ages)	No
Religion or Belief (includes faith groups, atheism and some other non religious beliefs)	No	**Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave)	No	**Marriage and Civil Partnership** (includes opposite sex and same sex couples who are either married or civil partners)	No

Yes – Please describe the anticipated negative impact **No – Please describe any positive outcomes**

3. Have you considered any codes of practice, guidance, project or business plan benefit? **If 'No', why not?**	**Yes**	**X**	**No**	

Sources of Information may include:

- Feedback from equality bodies, e.g. Care Quality Commission, Disability Rights Commission, etc
- Investigation findings
- Trust Strategic Direction
- Data collection/Analysis
- Staff grievances
- Media
- Community Consultation/Consultation Groups
- Internal Consultation
- Other (Please state below)

4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Gender, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership

Yes – Please describe the engagement and involvement that has taken place
Consultation has taken place in part of the Corporate Products team, Staff Domain and ISSG.

No – Please describe future plans that you may have to engage and involve people from different groups

5. As part of this equality analysis have any training needs/service needs been identified?

No	Please describe the identified training needs/service needs below

A training need has been identified for

Trust staff	No	Service users	No	Contractors or other outside agencies	No

Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so

The completed EA has been signed off by: You the Policy owner/manager: Type name: Kendra Smith	Date: **01/11/2018**
Your reporting manager: Type name: Niall Evans	Date: 01/11/2018
Please forward this form by email to: tewv.policies@nhs.net **Please Telephone: 0191 3336267/6542 for further advice and information on equality analysis**	