**Smartcard Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| v1.4 | 02/01/2024 | Sultan Mohamed | Nine Taylor |  |
|  | January 2026 |  |  | Next review |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 2](#_Toc142477999)

[1.1 Policy statement 2](#_Toc142478000)

[1.2 Status 2](#_Toc142478001)

[2 Smartcard governance 3](#_Toc142478101)

[2.1 Key personnel 3](#_Toc142478102)

[2.2 Roles and responsibilities of the RA manager 3](#_Toc142478103)

[2.3 Terms and conditions of smartcard usage 3](#_Toc142478104)

[2.4 Smartcard passcode 4](#_Toc142478105)

[3 Smartcard processes 4](#_Toc142478106)

[3.1 Registration 4](#_Toc142478107)

[3.2 Identity checks 4](#_Toc142478109)

[3.3 Issue a new smartcard 5](#_Toc142478111)

[3.4 Lost, stolen or damaged smartcards 5](#_Toc142478112)

[3.5 Smartcards for temporary staff and visitors 5](#_Toc142478150)

[3.6 Unlocking a smartcard 5](#_Toc142478152)

[3.7 Certificate renewal 5](#_Toc142478154)

[3.8 Repair card process 5](#_Toc142478171)

[3.9 Changing a passcode 6](#_Toc142478173)

[3.10 Assign user access 6](#_Toc142478174)

[3.11 Manage workflow requests 6](#_Toc142478175)

[3.12 Incident reporting 6](#_Toc142478179)

[3.13 Leaving the organisation 6](#_Toc142478185)

[3.14 Further help 7](#_Toc142478186)

[Annex A – Smartcard Agreement 8](#_Toc142478187)

# Introduction

## Policy statement

At Sheerwater Health Centre, for staff to access the NHS IT systems, a smartcard is required. NHS smartcards are similar to chip and PIN bank cards and enable healthcare professionals to access clinical and personal information appropriate to their role. Users are assigned an access profile which is aligned to their professional role within the organisation and staff are then able to access patient data, enabling them to deliver effective patient care.

Smartcards enable staff to access patient data; therefore, efficient access controls are vital to maintain the security of such data and it is imperative that these controls are used in the appropriate manner.

The following are mandatory requirements relating to smartcards:

* Local organisations must assure themselves that they have a robust and secure process in place to ensure that the smartcard reaches the end user for whom it is intended
* Only the end user of the smartcard should know the passcode for the smartcard. If anyone else knows the end user’s passcode, this breaches the smartcard terms and conditions of use and the [Computer Misuse Act 1990](https://www.legislation.gov.uk/ukpga/1990/18/contents)
* It is mandatory that users sign the Smartcard Agreement when provided with their smartcard. An agreement can be found both at [Annex A](#_Annex_A_–) or within the terms and conditions of smartcard use that are shown when first logging in
* When smartcard users leave an organisation, the end of their access assignment should be dated in that organisation

All staff must ensure that they conform to the guidance detailed in this document and the referenced material to ensure that clinical and personal information is only accessed by those personnel who have a valid reason to do so.

This policy is to be read in conjunction with the CQC’s [GP Mythbuster 41: Smartcards](https://www.cqc.org.uk/guidance-providers/gps/gp-mythbuster-41-smartcards) and NHS E [Care Identity Services Registration Authority guidance](https://digital.nhs.uk/services/care-identity-service/registration-authority-users#smartcards).

## Status

The organisation will aim to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

# Smartcard governance

## Key personnel

Contact details for Registration Authority (RA) primary care service providers can be found [here](https://digital.nhs.uk/Registration-Authorities-and-Smartcards/Service-provider-contact-details).

|  |  |
| --- | --- |
| **Role** | **Named provider** |
| RA primary care service provider | SCWCSU South, Central & West CSUScwcsu.smartcards@nhs.netTel 0300 561 0429 |
| RA Manager  | [Insert name/role] |
| ID Checker | [Insert name/role] |
| ID Checker | [Insert name/role] |
| Caldicott Guardian | Dr Munira Mohamed / GP |

These roles are detailed within the relevant job descriptions.

## Roles and responsibilities of the RA manager

To undertake the responsibilities delegated from NHS Digital in relation to RA activity, this organisation undertaking RA activity must ensure that the RA manager will:

* Be identified and have this role detailed within their job description
* Report to the CSU annually on RA activity and adhere to the requirements of the Data Security and Protection Toolkit (DSPT) submissions
* Be responsible for running the governance of RA in the organisation.
* Register RA staff at this organisation
* Be responsible for smartcard guidance and training to the ID checker and those receiving new smartcards

Further guidance on DSPT can be sought in the **Data Security and Protection Toolkit Handbook**.

## Terms and conditions of smartcard usage

The local RA process should reference that the user has electronically accepted the terms and conditions when they first log in with their smartcard. It is mandatory that users sign the terms and conditions of smartcard use (see Annex A).

NHS smartcards are to be retained by users at all times.

Under no circumstances can NHS smartcards:

* Be issued with the organisation name
* Be issued without the user’s unique user identifier and a true likeness of the user’s photograph displayed
* Be shared, including the passcode
* Be shared by any other user other than the user on the smartcard
* Remain in the smartcard reader when the workstation is left unattended

RA Manager responsibilities can be found within the appendices to the [Registration Authority Policy](https://digital.nhs.uk/services/care-identity-service/registration-authority-users/registration-authority-help/registration-authority-policy#appendix-1-ra-manager-responsibilities).

## Smartcard passcode

Only the user should know their smartcard passcode. If anyone else knows the passcode, this breaches the smartcard terms and conditions and the [Computer Misuse Act 1990](https://www.legislation.gov.uk/ukpga/1990/18/contents).

The passcode is:

* Set by the user during the registration meeting
* Entered by the user when using their NHS smartcard

Passcodes are never to be shared or disclosed to anyone else.

# Smartcard processes

## Registration

The registration process for a new user is undertaken by the NHS E process [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/cis-application-ra-user-guides/register-a-new-user-and-verify-their-identity). Guidance for RA, including key documents and forms, can be found [here](https://digital.nhs.uk/services/care-identity-service/registration-authority-users#smartcards).

Further advice and guidance can be found within the NHS Digital's [Registration Authority Policy](https://digital.nhs.uk/services/care-identity-service/registration-authority-users/registration-authority-help/registration-authority-policy).

Special revised guidance was issued by NHS Digital in relation to the smartcard registration process during the COVID-19 pandemic when face-to-face identity checks were not possible. This emergency registration process ended on 31 May 2023 as detailed [here](https://digital.nhs.uk/services/care-identity-service/latest-news/emergency-registration-has-ended).

## Identity checks

Prior to an individual being issued with an NHS smartcard, they must have their identity verified in accordance with the [NHS Employers’ identity checks standard](https://www.nhsemployers.org/publications/identity-checks-standard)

Guidance for verifying a new user’s identity can be found [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/cis-application-ra-user-guides/register-a-new-user-and-verify-their-identity).

As obtaining a smartcard involves rigorous identity checks, and is therefore an essential aspect of the pre-employment requirements, the CQC’s [GP Mythbuster 41](https://www.cqc.org.uk/guidance-providers/gps/gp-mythbusters/gp-mythbuster-41-smartcards) details that having a smartcard will be acceptable as evidence that fit and proper principles have been applied during the recruiting process.

## Issue a new smartcard

The process to issue a new smartcard can be found [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/cis-application-ra-user-guides/issue-a-new-smartcard).

## Lost, stolen or damaged smartcards

Should a user lose, damage or have their smartcard stolen, they are to report this to the RA. The RA will then cancel the smartcard and replace it.

Further information on this process can be found [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/cis-application-ra-user-guides/destroy-or-cancel-a-smartcard).

## Smartcards for temporary staff and visitors

Refer to the NHS Digital guidance that supports this subject [here](https://digital.nhs.uk/services/care-identity-service/registration-authority-users/registration-authority-help/smartcards-for-temporary-staff-and-visitors).

Should there be a local arrangement or requirement from the CSU citing that additional governance arrangements are required, then the CSU should ordinarily provide the process and subsequent guidance. This is to support how temporary staff can gain access when employed at short notice.

## Unlocking a smartcard

When a smartcard is initially issued, the RA will also register the new user for the [self-service smartcard unlock](https://digital.nhs.uk/services/care-identity-service/smartcard-and-authentication-users/register-for-self-service-smartcard-unlock).

Should the smartcard not be registered for self-service smartcard unlock, then the card will have to be unlocked by the RA. Further reading can be found on the [How to unlock your smartcard](https://digital.nhs.uk/services/care-identity-service/smartcard-and-authentication-users/how-to-unlock-your-smartcard) webpage.

## Certificate renewal

Smartcard certificates are valid for two years. If a certificate is due to expire within the next 90 days, then the user will receive a smartcard expiry alert each time they log in. This will continue until the certificate is renewed.

Further reading can be found at [renew your smartcard certificates before they expire](https://digital.nhs.uk/services/care-identity-service/smartcard-and-authentication-users/self-renewal-nhs-smartcard-service).

If the certificates have expired, then the smartcard user will need to have their certificates renewed via the RA. This process known as 'repairing' the smartcard and must be done in person. Further reading on this process can be found [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/cis-application-ra-user-guides/repair-smartcard-certificates).

## Repair card process

The repair card process applies to those smartcards that appear faulty but are not physically damaged, e.g., the user is unable to log in. The repair card process will remove all associated certificates and passcodes before reissuing the certificate and prompting the user to set a new passcode. It is advisable for users to use a passcode that has not been previously used.

## Changing a passcode

Smartcard users can change their passcode at any time using the ‘Change Passcode’ function in the CIS application. This process does not require the support of the RA.

To change a passcode:

* [Log in to the Spine Portal](https://portal.national.ncrs.nhs.uk/portal/) (needs HSCN connection)
* Select ‘Care Identity Service’
* Select 'My profile'
* In the 'Smartcard Details' section, find the smartcard for which you want to change the passcode and select 'Service'
* Select 'Change passcode'
* Complete the current and new passcode boxes and confirm

A detailed version of this process including screenshots is [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/change-your-passcode).

It is recommended that smartcard users change their passcodes at regular intervals.

## Assign user access

Guidance on how to add access positions to a profile in the Care Identity Service application can be found [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/cis-application-ra-user-guides/assign-user-access-or-submit-a-request).

## Manage workflow requests

Guidance on how to manage workflow requests in the Care Identity Service application can be found [here](https://digital.nhs.uk/services/care-identity-service/applications-and-services/care-identity-service-application/cis-application-ra-user-guides/manage-requests).

## Incident reporting

Should a member of staff at this organisation become aware of an incident involving a smartcard, such as theft or misuse, they are to contact the Practice Manager who will report the matter immediately to the Caldicott Guardian for full investigation. Ordinarily a significant event would be raised for such an incident.

When NHS Digital is notified of significant breaches to the Registration Authority Policy, it will consider the situation and take appropriate remedial action. This will include discussing the situation with this organisation but may result in discussions with regulatory or professional bodies depending upon the seriousness of the situation.

Further reading can be found in NHS Digital’s [Registration Authority Policy](https://digital.nhs.uk/services/care-identity-service/registration-authority-users/registration-authority-help/registration-authority-policy) and this organisation’s **Significant Event Policy**.

Contact details for NHS Digital can be found at [Section 3.14](#_Further_help).

## Leaving the organisation

Should a member of staff move to a different healthcare organisation then they can retain their smartcard. Access will be removed and the new organisation will apply for access to the existing smartcard. If a member of the organisation is leaving the healthcare industry, then they are to return their smartcard to either their line manager or the RA.

Further reading on this subject and also for those on extended leave or parental leave can be found in the NHS E document titled [Smartcards and access controls](https://www.england.nhs.uk/long-read/smartcards-and-access-controls/).

## Further help

Further guidance for RA Managers and ID checkers can be found [here](https://digital.nhs.uk/services/care-identity-service/care-identity-service-guidance-leaflets/guidance-for-registration-authority-managers-agents-and-id-checkers). Useful contact details for NHS Digital can be found [here](https://digital.nhs.uk/about-nhs-digital/contact-us).

# Annex A – Smartcard Agreement

**SMARTCARD AGREEMENT**

**STAFF OBLIGATIONS**

* I consent to the collection and use of personal data and agree to provide any additional information and documentation required by the Registration Authority in order to verify my identity.
* I confirm that the information provided by myself on the smartcard application is accurate. I agree to notify my local Registration Authority immediately of any changes to this information.
* I agree that the smartcard issued to me is the property of the NHS and I agree to use it only in the normal course of my employment or contract arrangement.
* I agree that I will check the operation of my smartcard promptly after I receive it. This will ensure that I have been granted the correct access profiles. I also agree to notify my local Registration Authority promptly if I become aware of any problem with my smartcard or my access profiles.
* I acknowledge that I will keep my smartcard private and secure and that I will not permit anybody else to use it or any session established with the NHS Care Records Service applications. I will not share my passcodes with any other user. I will not make any electronic or written copies of my passcodes (this includes function keys). I will take all reasonable steps to ensure that I always leave my workstation secure when I am not using it by removing my smartcard. If I lose my smartcard or if I suspect that it has been stolen or used by a third party, I will report this to my local Registration Authority as soon as possible.
* I agree that I will only use my smartcard, the NHS Care Records Service applications and all patient data in accordance with the [NHS Confidentiality Code of Practice](https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice) and (where applicable) in accordance with my contract of employment or contract of provision for service (whichever is appropriate) and with any instructions relating to the NHS Care Records Service applications which are notified to me.
* I agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate my smartcard, NHS Care Records Service applications components or any access profiles given to me.
* I agree not to deliberately corrupt, invalidate, deface, damage or otherwise misuse any NHS Care Records Service applications or information stored by them. This includes but is not limited to the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality.
* I acknowledge that my smartcard may be revoked, or my access profiles changed at any time without notice if I breach this Agreement; if I breach any guidance or instructions notified to me for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. I acknowledge that if I breach this Agreement this may be brought to the attention of my employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution).
* I agree that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of smartcards for the NHS Care Records Service applications. The Registration Authority is not responsible for the availability of the NHS Care Records Service applications or the accuracy of any patient data.
* I acknowledge that I, or my employer, shall notify my local Registration Authority at any time should either wish to terminate this Agreement and to have my smartcard revoked e.g., on cessation of my employment or contractual arrangement with healthcare organisations or other relevant change in my job role.
* I acknowledge that these terms and conditions form a binding agreement between myself and those organisations who have sponsored my role(s). I agree that this Agreement is governed by English law and that the English courts shall settle any dispute under this Agreement.

|  |  |
| --- | --- |
| **Name** |  |
| **Signature** |  |
| **Date** |  |