Smart Card Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
001	July 2020	Claire Laing/ Margaret McHugh		

Table of contents

1 Introduction

1.1 Policy statement

In order for NICS staff to access the NHS IT systems, a smartcard is required. Users are assigned an access profile which is aligned to their professional role within NICS; staff are then able to access patient data, enabling them to deliver effective patient care. This policy relates to all NICS staff in both Improved Access and Urgent Treatment Centre.

1.2 Principles

Smartcards enable staff to access patient data; therefore, it is vital that they are issued and used in the appropriate manner. The following are mandatory requirements relating to smartcards:[1]

- 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, it breaches the smartcard terms and conditions of use and the Computer Misuse Act 1990
- When smartcard users leave an organisation, they should have the end of their access assignment dated in that organisation
- It is mandatory that users sign the terms and conditions of smartcard use shown when the user first logs in

1.3 Status

NICS aims 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. Consideration has been given to the impact this policy might have in regard to 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This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time.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.

1.4 Training and support

NICS will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

[1] NHS Digital Registration Authority Policy

2 Scope

2.1 Who it applies to

This document applies to all employees and directors of NICS. Other individuals performing functions in relation to NICS, such as agency workers, locums and contractors, are encouraged to use it.

2.2 Why and how it applies to them

Smartcard users have access to sensitive patient data and efficient access controls are vital to maintain the security of such data. 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.

3 Definition of terms

3.1 Registration authorities

A Registration Authority (RA)[2] is a function that carries out the identity check of prospective smartcard users and assigns an appropriate access profile to the health professional's role, as approved by the employing organisation.

3.2 Care Identity Service

The Care Identity Service (CIS) is an electronic system for registering and issuing smartcards and the subsequent management of smartcards.

3.3 Smartcards

NHS smartcards enable healthcare professionals to access clinical and personal information appropriate to their role. A smartcard is used in conjunction with a passcode, known only to the holder, and gives secure and auditable access to national and local Spine-enabled health record systems.

3.4 NHS Digital

Formerly known as the Health and Social Care Information Centre or HSIC, NHS Digital is the national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care.

3.5 Local smartcard administrator

[2] Registration Authorities and smartcards NHS Digital

A Local Smartcard Administrator (LSA) is an individual who has additional abilities[3] to enable them to unlock or unblock smartcards and assist cardholders in changing their PIN, should they wish to do so. Smartcard administrators may also be asked to:

- Check, renew and re-issue certificates
- Assist users in locating smartcard expiry dates
- View the expiry data of a smartcard
-

Smart card administrators for NICS both Improved Access and UTC

Claire Laing	RA sponsor and Privacy Officer NICS IA and UTC	Claire.laing@nhs.net
Laura Sutton	RA Sponsor IA	Nics.admin@nhs.net
Sharon Green	Card unlocker IA	Nicsadmin.sharon@nhs.net
Fran Rawlings	RA Sponsor UTC	f.rawlings@nhs.net
Jenni Bailey	Card Unlocker UTC	Jennifer.bailey10@nhs.net
Margaret McHugh	RA Sponsor ST Peters -UTC	m.mchugh@nhs.net

4 Protecting information

4.1 Legislation

The NHS Care Record Guarantee for England details how patient information is used by NHS staff and what controls patients have over this information. All staff at NICS must comply with the Guarantee at all times.

5 Smartcards

5.1 RA contact details

Contact details for Registration Authority organisations which support primary care organisations can be found here.

5.2 Registration process

The user registration process is undertaken using the CIS application and is formed of three stages:

1. The user is identified for an NHS smartcard
2. Access to the relevant Spine is permitted
3. An NHS smartcard is created, linking the user to the Spine, with the appropriate level of access

Registration for an NHS smartcard must take place in a face-to-face meeting with either a RA manager, agent or approved ID checker. The CIS enables organisations

[3] CIS Smartcard Administrator Guide V1

to have nominated ID checkers to facilitate registrations, meaning that new applicants do not need to visit the RA. The local ID checker is Claire Laing

5.3 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 check standards. Verifying the identity of an individual is essential and is the most significant of all the pre-employment requirements.

5.4 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. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode to others.[4]

5.5 Smartcard requirements

NHS smartcards are to be retained by the user at all times. Under **no** circumstances can NHS smartcards be:[4]

- Issued with the organisation name
- Issued without the user's unique user identifier (UUID) and a true likeness of the user's photograph displayed
- Shared, including the passcode
- Shared by any other user other than the user on the smartcard
- Remain in the smartcard reader when the workstation is left unattended
- Removed from the user when they leave an NHS organisation if they intend or there is a possibility that they will work for the NHS in the future

5.6 Smartcard passcode

Only the user should know their smartcard passcode. If anyone else knows the passcode, it breaches the smartcard terms and conditions and the Computer Misuse Act 1990. The passcode is:

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

Under no circumstances are passcodes to be shared or disclosed to anyone else.

5.7 Lost, stolen or damaged smartcards

[4] RA Operations and Process Guidance

Should a user lose, damage or have their card stolen, they are to report it to the local RA. The RA will follow protocols to ensure that the lost, damaged or stolen card is cancelled and a replacement card issued.

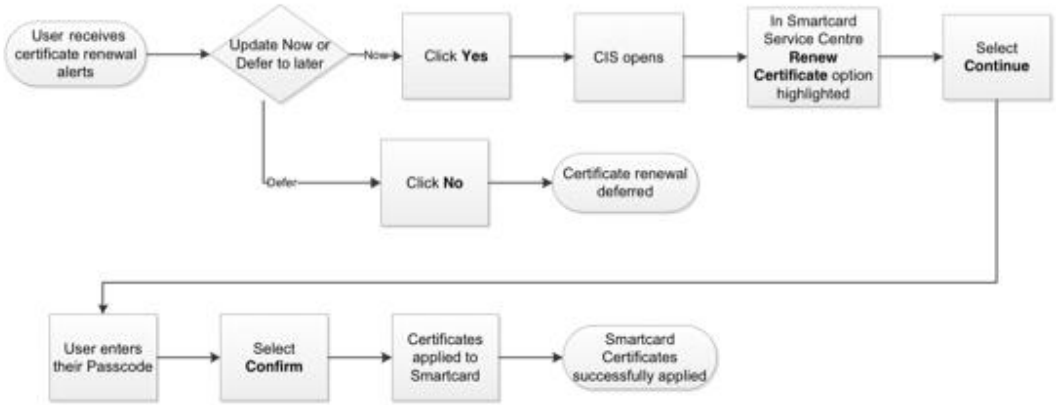
5.8 Unlocking a smartcard

LSAs are able to unlock smartcards and should follow the guidance detailed in the CIS guidance leaflet for Unlocking a smartcard.

5.9 Certificate renewal

NHS smartcards have certificates assigned to them which need to be renewed every two years. Users can self-renew the certificate on two separate occasions; however, for the third renewal, the RA must be involved. RA representatives will verify the user and provide assurance of likeness before renewing the certificates.

The process of self-renewal follows and was extracted from the RA operations and process guidance document.



5.10 Expired certificates

If a certificate expires, the smartcard can only be reissued by the following personnel:

- RA manager
- Advanced RA agent
- RA agent
- RA agent ID checkers

The above individuals will reissue certificates using the Issue Card Process detailed on page 34 of the RA operations and process guidance document.

5.11 Repair card process

The repair card process applies to those cards 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. Any queries relating to the repair card process are to be directed to the local RA organisation.

5.12 Changing a passcode

Smartcard users can change their passcode at any time using the 'Change Passcode' function in the Care Identity Service (CIS) application. This process does not require the support of the RA, sponsor or LSA.

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

5.13 Incident reporting

Should a member of staff at NICS become aware of an incident involving a smartcard, such as theft or misuse, they are to contact the Service Manager who in turn will report the matter immediately to the St Peter's Hospital or South central CSU submitting an incident report form.

5.14 Smartcard user profiles

Smartcard users are able to update certain aspects of their profile on the CIS database in the 'my profile' section. A user guide illustrating this process can be found here.

6 Summary

It is the responsibility of all staff at NICS to ensure that they adhere to the terms and conditions relating to the use of their smartcards. Staff must also comply with the information detailed in this policy and associated reference material in order to safeguard the sensitive patient data to which they have access.

Information required for issuing a Smart card.

Name:	
DoB:	
National Insurance No:	
Passport Number & expiry date	
Driving License No and start date	
Proof of address x2 Not mobile phone Bank Statement < 3 months old TV License	
Photograph head and shoulders in jpeg format	
Do you already have a smart card? Smart card No:	Yes/No
During Covid-19 pandemic if no face to face confirmation, there will be a video meeting for ID verification.	