Smartcard and Identity Card (ID) Policy

Document Reference:	IG23
Document Purpose:	The purpose of this document is to provide guidance to all CCG staff on Smartcard & Identity Card usage.
Date Approved:	December 2015
Approving Committee:	NHS South Lincolnshire Clinical Commissioning Group Risk and Governance Committee
Date Ratified:	December 2015
Ratified by:	NHS South Lincolnshire Clinical Commissioning Group Governing Body
Version Number:	2.1
Status:	Final
Next Revision Due:	December 2016
Developed by:	Registration Authority Department, Arden & Greater East Midlands Commissioning Support Unit (Arden & GEMCSU)
Policy Sponsor:	Gary Thompson, Chief Officer, Senior Information Risk Owner, NHS South Lincolnshire Clinical Commissioning Group
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to members, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit
Distributed via:	Intranet & Internet

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/Amended by
1.0		Adoption of NHS Lincolnshire policy (CG001), adapted for CCG	January 2013	
2.0		Updated to reflect NHS Arden & GEM CSU & CCG. Replaced IDFO1(page 16) with updated version	January 2015	Barbara Huxtable, IG Officer, NHS Arden & GEM CSU
2.1		Updated Policy Statement on Page 5 to reflect new user identify management system in place.	December 2015	June Emptage, IG Compliance Manager, NHS Arden & GEMCSU

Contents

Section **Page**

Appendices

Policy Statement

Background	The implementation and use of smartcard technology is a key component of all National Programme applications.
Statement	This policy will apply to all procedures and activities in relation to Smartcards and Identity Cards (ID) processed on behalf of the CCG. It is anticipated the current User Identity Manager will be taken down on 19th February 2015 and the new service, Care Identity Service will be up and running on 24th February 2015 (Ref: HSCIC - National Access Control, January 19th 2015).
Responsibilities	All staff must abide by the Terms & Conditions for smartcards ***Appendix 3*** *refers* and identity cards (IDF01) issued by the RA department on behalf of the CCG.
Training	Training will be facilitated by the Clinical Systems Training department.
Dissemination	This policy will be published on the CCG's website.
Resource implication	None.

Introduction

The Registration Authority acts on behalf of the CCG, and has organisational authority for ensuring that all aspects of registration and identity card services are performed in accordance with local and national policies and procedures. It is responsible for providing arrangements that will ensure tight control over the issue and maintenance of smartcards and identity cards, whilst providing an efficient and responsive service that meets the needs of the organisation.

Roles and Responsibilities

Registration Authority Manager (RAM)

The lead for the development and service provision for NPfIT Registration Authorities (smartcards) across the CCG as well as Lincolnshire Community Health Services, Lincolnshire Partnership Foundation Trust, GP Practices, Pharmacists, and other NHS and non-NHS organisations including private and public sector organisations.

The RAM is the lead in relation to all Registration Authority (RA), Role Based Access Control (RBAC) and Person Based Accessed Control (PBAC) matters and all associated programmes of work assuming overall responsibility and delegating authorities to staff as appropriate.

Registration Authority Officers

Registration Authority Officers work with the RAM in providing day-to-day support across the full range of RA duties.

Registration Authority Responsibilities

- Ensuring that the National and Local Registration processes are adhered to
- Process all smartcard and identity card applications
- Ensuring that all RA forms are appropriately used
- Ensuring that there is sufficient availability of resources to operate the registration process and identity card process in a timely and efficient manner to meet the organisational responsibilities
- Ensuring that the RA team members are adequately trained and familiar with local and national RA procedures
- Ensuring that an indexed and secure audit trail is maintained of applicants' registration information and profile changes
- All completed application forms and associated documents are kept in a secure area where access is limited
- Ensuring that all RA documentation held, meets the CCGs retention and destruction guidelines
- Ensuring sufficient Sponsors and Local Agents have been appointed to meet organisational needs, they have been adequately trained, and have access to relevant guidance to carry out their role

1. Smartcards

1.1. Smartcards Overview

A smartcard is a security device incorporating chip and PIN security which permits an authorised user to gain access according to their requirements. This is based upon the person's organisation/s, job role/s, areas of work and business functions/activities referred to as Position Based Access Control (PBAC). This is a key component for all National Programmes for IT (NPfIT) systems. As new systems are deployed, staff will be identified, their roles and access requirements agreed, and arrangements made for them to be issued with an NHS smartcard. This process is known as the 'registration process' and is managed through the Registration Authority Department.

1.2. Why you need one

Smartcards are primarily used for access to spine connected clinical systems, for example Choose & Book, SystmOne, PDS (Patient Demographic Service).
All staff will require a smartcard for access to the Electronic Staff Record (ESR). This will give staff access to online mandatory training and enable them to view/update their staff details.
Version 5 (V5) smartcards can also be programmed for use with some of the proximity swipe buildings access systems used within Lincolnshire.

1.3. How to Apply

A smartcard cannot be used as an identity card, should a user need a separate identity card these can be applied for via the process in section 2.

Smartcard applications are via User Identity Manager (UIM) access via:
https://portal.national.ncrs.nhs.uk

Only approved Sponsors have access to UIM and are capable of making smartcard requests. Guidance is available from NHS ARDEN & GEM CSU.

1.4. 3rd Party Provision

Smartcard provision for 3rd party providers i.e. pharmacists, social services, St Barnabas will be through CCG approved service level agreements.

1.5. Training

All RA managers, RA officers, Local Agents and Sponsors need to complete the Information Governance e-learning training modules appropriate for their job role on an annual basis. In addition to training, all individuals with RA responsibilities should have access to up to date guidance and web-based materials.

Clinical systems training will be provided by the Clinical Systems Training Department (CST). They can be contacted on Clinicalsystems.support@gemcsu.nhs.uk

Access should not be requested for SystmOne or C&B until the user has been trained by CST or is booked onto training.

1.6. Timescales

All smartcard applications and amendments are subject to a 5 day turnaround period (excluding postal delays), this should be considered when setting up new users or where additional access is required.

Revocations will be actioned within 24 hours; revocations for security reasons will be actioned immediately by the RA dept.

1.7. Duties

Title	Responsibilities
Registration Authority Agent	Ensure all forms are processed within agreed timescales. Record all access to local or national systems where required.
Sponsor	Responsible for approving, where appropriate, the registration and profiles to be granted to users. Informing the RA Department of user requirements/changes in a timely manner. Ensuring all ID checks comply with EGif3 standards as part of the registration process. Comply to the procedures set out in the Sponsor Guide Ensuring all actions comply with Information Governance practices & policies.
Local Agent	Assist other smartcard users with duties documented in the Local Agent Guide. Comply with the procedures set out in the Local Agent Guide. Ensuring all actions comply with Information Governance practices & policies.

1.8. Leaving/Changing Job

A smartcard is designed to stay with an individual for as long as they need it, as such should they leave a position or a CCG they should *keep* their card provided they are going to another role within the NHS or outside the NHS but using a smartcard; access must however be removed via a 'Modify Person' request where applicable.

If your new employment does not require a smartcard then your smartcard should be given to your manager before leaving for secure destruction by the RA.

It is the responsibility of the Sponsor to ensure that users who leave or take an agreed period of leave from the organisation have their status recorded by the RA Office. The RA Department will process leavers/absentees in line with locally developed procedures, either suspending or revoking access. It is then the Sponsor's responsibility to notify the RA office of any users who require their smartcard to be re-activated.

Suspension of smartcards is appropriate for members of staff who will not be in a position to use the smartcard for a short period of time e.g. sickness absence, short career break. Ideally suspension should not cover a period greater than 3 months, although the Sponsor has the discretion to request suspension for longer periods, depending on the circumstances.

It is the responsibility of the RA office to keep records of all cards that have been returned and destroyed. Records must include details of the member of staff's name, UUID number and smartcard number. In order to ensure that all leavers are being captured by the RA team, a list of leavers will be supplied to the RA team by Employee Services on a regular basis.

2. Identity Cards

2.1. ID Cards Overview

ID cards must be visibly worn at all times whilst at work, whether on NHS premises or in the community; they should not be worn outside of working hours. ID cards must conform to current layouts and specifications, see Appendix 1. Any that do not match should be updated immediately.

The image on the cards must always be an accurate likeness of the individual, should this change a new card should be applied for and an updated picture supplied.

For users concerned about having their full name on their card, i.e. receptionists and secure unit employees cards can be double sided to allow for one face to omit their surname.

2.2. Why you need one

ID cards must be worn at all times when on duty to enhance the safety of staff and patients.
Failure to wear a valid ID card may result in staff members not being able to access some sites for security reasons.
It is the responsibility of all managers should ensure that their staff have a valid ID card at all times.

2.3. Lapel Badges

Only cards with the users' full name (Forename and Surname) and photo are acceptable, as such lapel badges etc are not considered acceptable on their own and can only be worn together with a CCG issued identity card.

2.4. How to Apply

ID card applications and changes are all applied for via gemcsu.idcards@nhs.net they can be posted in, however emailed applications are preferred. Applications must be made by each staff member's manager.

2.5. Timescales

ID applications will be processed by the RA department within 5 days of a correctly completed and authorised form being received into the department.

ID card applications for new employees should be submitted before the individual starts work, to ensure a valid ID has been produced and available on the start date.

ID card renewals should be submitted 30 days before the current card expired to allow for sufficient time for the new card to reach the individual before their current card expires.

2.6. Expired Cards

Once a card has expired, i.e. its two year life has been reached; the card should be securely destroyed on site or returned to the RA for destruction. To prevent any staff member not having a valid ID card at all times a replacement card must be requested via an IDF01 prior to the expiry date being reached.

2.7. Leaving / Changing Job

If a cardholder changes name or their job title they need to apply for a new ID card. Once they have received the new ID card, the old one will need to be destroyed securely. Alternatively, return it to the RA department for secure destruction.

Once a user has left the position or CCG the ID card that applies to that position must be handed in to the person's manager for them to either securely destroy on-site or return to the Registration Authority Department along with an IDF01 for secure destruction.

Should a staff member be dismissed, any ID cards they have must be retained by the manager and returned to the RA department for destruction.

3. Lost or Stolen Cards

An IR1 should be completed for all lost or stolen cards. The user should inform both their line manager/manager and the RA department immediately. An IDF01 (for ID cards), will then need to be completed and/or a UIM Re-Issue smartcard request (for smartcards) and submitted to the RA department so a replacement card can be provided as soon as possible.

All smartcard losses should be reported immediately to the Registration Authority Team to avoid misuse.

4. Incident Reporting

All members of staff are encouraged to report incidents involving the use and abuse of smartcards and identity cards. These should be reported in line with the CCGs Incident Reporting or Whistleblowing Policies.

Examples of incidents are:

- Smartcard or application misuse.
- Theft of a smartcard
- Non-compliance of local or national RA policy

- Any unauthorised access of CfH applications
- Any unauthorised alteration/viewing of patient data

The Manager, or equivalent, or the Sponsor will consider all incidents reported to them. Any incidents considered significant will be escalated to the Caldicott Guardian, and the Human Resources department depending on the nature of the incident. A significant incident is an isolated incident or a series of less significant incidents that could lead to a serious degradation of healthcare or information security. The RA Manager and Caldicott Guardian will consider incidents reported to them and make recommendations as to whether CCG systems or working practices should be reviewed as a result.

A major breach of security will also be reported by the RA Manager to the local service provider and Connecting for Health to ensure that any risks resulting from the event can be taken into account and mitigated against.

Incidents involving breaches of security must also be reported to HR and the Caldicott Guardian by the RA Manager so that any disciplinary measures required may be taken. The HR department will contact the relevant Manager, or equivalent, who will be responsible for ensuring an appropriate and timely investigation is undertaken in line with the CCG's Disciplinary Policy.

5. Confidentiality

All users issued with a smartcard or identity card must adhere to the smartcard terms and conditions, NHS Confidentiality Code of Practice (November 2003) and the Data Protection Act (1998) and any CCG policies on Confidentiality, Information Security and the Disclosure of Confidential Information. Any breaches of confidentiality or misuse of the smartcard or identity card may result in disciplinary action being taken up to and including dismissal, in line with the CCG's Disciplinary Policy.

6. Security

It is the responsibility of the RA team to ensure the secure storage of RA equipment and consumables, these areas are secured by passcode security locks or swipe card entry.

All manual files will be stored in a secure area, only accessible by passcode security locks, and accessible only by those members of staff who have been given permission.

All precautions should be taken to secure all RA mobile equipment. Please refer to the CCGs mobile policy. All loses should be reported to the Registration Authority Manager and an IR1 should be completed. Please refer to the CCGs Incident Reporting Policy.

All actions taken by a user logged in with their smartcard are recorded, and are traceable back to that smartcard and the audit trail can be reviewed by the CCG Information Security Manager. This audit trail can be used to identify misuse of the smartcard from which disciplinary measures can be taken.

The Information Security Manager reserves the right to carry out random checks on smartcard audit trails as well as specific checks after reported incidents. The RA team may also undertake 'spot checks'.

Appendix 1 ID Card Images:

LPfT:

Lincolnshire Community Health Services:

CCG:

Appendix 2: Smartcard Images:

Version 4:

Version 5:

Version of card can be determined by second digit on reverse of card.

Appendix 3

NHS Care Records Service Smartcard Terms and Conditions V1.0b 1st January 2010

1.1.1 Notice to applicants on the collection of personal data

In accordance with the requirements of Department of Health, the personal data (as defined in the Data Protection Act 1998) that the applicant provided as part of the application process to access NHS CRS together with any personal data processed in relation to the applicant in support of their application is collected for the purpose of identifying the applicant and processing this application and evaluating the applicant for suitability as an authorised user; if accepted, to generate a personalised certificate and Smartcard for the authorised user and for the purpose of managing the applicant's use of any NHS Care Records Service applications or applications that utilise NHS Care Records Service authentication.

In particular, this personal data will be used to validate and verify the applicant's identity to ensure that the applicant is correctly identified and appropriately authorised for access. The personal data in relation to the applicant will be processed by local Registration Authority/Authorities and may be shared with other Registration Authorities for the purpose of processing this application, in accordance with the requirements of the Data Protection Act 1998 as amended and supplemented from time to time. This personal data may also be used to ensure that accurate information can be recorded regarding the applicant's use of systems.

In accordance with the Data Protection Act 1998, this personal data will neither be used nor disclosed for any other purpose other than where required by law, and will be retained in accordance with the Registration Authority's data retention policy. It is the applicant's responsibility to ensure that their registered name is accurate and kept up-to-date. The applicant may contact their local Registration Authority or Sponsor in relation to any queries they may have in connection with this application.

By signing this declaration I, the applicant:

1. consent to the use of my personal data in the manner described in the "Notice to applicants on the collection of personal data" above. I also agree to provide any additional information and documentation required by the Registration Authority in order to verify my identity;
2. confirm that the information which I provide in the process of my application is accurate. I agree to notify my local Registration Authority immediately of any changes to this information;
3. 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;
4. 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;
5. 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;

6. 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 (www.dh.gov.uk site) and (where applicable) in accordance with my contract of employment or contract of provision for service (which ever is appropriate) and with any instructions relating to the NHS Care Records Service applications which are notified to me;
7. 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;
8. 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;
9. 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);
10. 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 applications which use NHS Care Records Service authentication or the accuracy of any patient data;
11. 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 health care organisations or other relevant change in my job role; and
12. 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.

Appendix 4

IDF01

ID Card Application

For a manager to request or return an ID Card for a staff member.

This is not a Smartcard request: If a Smartcard is also required please complete a request in UIM.

For new starters please attach photo here.

When submitted by email a digital image must be attached to the email along with this form.

For renewals please submit new photo where current image no longer reflects a true likeness.

Arden&GEM Arden and Greater East Midlands Commissioning Support Unit

NHS

Card Created	Initials/Date:
Database	Initials/Date:
Posted	Initials/Date:
Comments	

* For official use only

This form should *not* be used by staff at Francis Crick House & Sherwood Place who should see reception.

.....Please submit this form by email wherever possible.....

	Please complete the following details: (Please use BLOCK CAPITALS and complete ALL fields)			
User Details	Reason for application: (New User, Name/Job Title/Organisation/Picture Change, Lost Card, Expiry Date Nearing, Left Position, Left Organisation, etc.)			
	Card holder required: (Neck Lanyard / Clip, Card Holder, None required)			
	Organisation: i.e. GEM CSU, LCHS, LPT, Other Lincs CCG (E/WS/BA), Derby CCG (N/S/H), Leics CCG (EL&R/WL/LC), Notts CCG (R/M&A/N&B), NHSPS		Employee Number: (8 Digit number from ESR)	
	Title (e.g. Dr, Mr, Mrs, Miss, etc):		Middle Name(s):	
	First Name(s):		Family Name (Surname):	
	Preferred Full Name: (To be shown on card)		Previous Name: (For name change requests)	
	National Insurance No.:		Date of Birth (dd/mm/yy):	
	Post Title (Job): (To be shown on card)	(Max 41 Characters)		
	Workplace Name:		Department / Ward:	
	Workplace Address: (Inc. Post Code)			
	Work Phone Number: (Inc. STD Code)		Mobile Phone Number:	
	Email Address:			
Manager Details	Print Full Name:		Work Phone Number:	
	Post Title (Job):			
	Email Address:			
	By signing below or using my personal work email address to submit this application I, the manager named above, approve this application and request the applicant specified above be issued with an ID Card. I confirm that I have carried out the necessary identity checks and satisfied myself the above individual meets the government eGIF level 3 standards.			
	Manager's Signature:		Date:	

Please email completed form to: GEMCSU.IDCards@nhs.net (including digital photo for new applications)
Alternatively post to: Registration Authority Dept., Cross O'Cliff Court, Bracebridge Heath, Lincoln, LN4 2HN
Tel: 01522 515362

This application will be stored electronically by the Registration Authority. IDF01 Version 2.07 Updated 14/01/2015