Smartcard Policy

Author	Alyson Hope
Responsible Director	Medical Director
Ratified By	Quality and Safety Committee
Ratified Date	October 2012
Review Date	December 2015
Version	1.1
Policy Consultation Period	21.01.2015 – 20.02.2015

Related Policies & Guidelines:

- Information Governance Policy

Contents

Amendment History

Version	Status	Date	Reason for Change	Authorised
1.0		October 2012	Initial Policy	
1.1		December 2014	Review and formatting	Q&SC

1. Scope

The PRS applies to INWL for all RA01 related issues.

The RA Lead at INWL is currently Craig Thomas (craig.thomas@inwl.nhs.uk). If he is unavailable, please contact either the IT service desk 0207 350 4050.

2. Issue of Smartcards for New Users

Approval for a request for a staff member to be issued with a smartcard and the access rights associated with it must come from the Access Control Lead (RA) at INWL.

New staff will be sponsored by Quality Co-Ordinator (Monika Truszczynska) or relevant Service Delivery Manager for their smartcards. Their RA01 forms should be sent by fax to the RA Lead at INWL. On receipt of the relevant forms, the RA Lead will arrange an appointment with the new user. New staff will be required to collect their Smartcard from INWL in person. They will need to provide proof of ID (either a valid passport or driving licence), proof of address (recent utility bill/bank statement or formal letter), and proof of National Insurance Number.

New Staff will be made aware of their responsibilities in relation to this as part of their induction and again, upon issue of the RA01 forms and Smartcard.

3. Leavers

Sponsors must ascertain whether a user is leaving the NHS or joining another NHS organisation. The sponsor must then complete an RA03 form and send it to the RA Lead at INWL, whereby the Smartcard will be cancelled. If the user in leaving the NHS, the Smartcard must be cancelled, destroyed, and returned to the RA Lead at INWL. If the user is staying within the NHS, they may take their Smartcard with them to their new employing organisation however access must still be cancelled. For additional guidance, see ID Rules for Smartcard Issuance document in CLH\PRS Operations\PRS Service Management/Registration Authority\RA Forms folder.

The Line Manager of exiting staff members has a duty to ensure the above procedure is followed.

4. Use of Smartcards

- Smartcards are issued to an individual on a named basis and are for the use of that person only.

- The access level relating to an individual is personal and must not be shared or otherwise made accessible to another member of staff.
- The Smartcard is to be kept under the personal control of the individual to whom it has been issued at all times and must not be left inserted into a smartcard reader when the individual is not present.
- On leaving a terminal for any length of time the Smartcard is to be removed. All staff should lock their screen when leaving their computer for a prolonged period of time (i.e. for lunch or meetings etc).
- Staff members must not share Smartcards.
- If a staff member is absent then their Smartcard must not be used.
- Smartcards should not be left in readers, on desktops or in any other insecure place overnight.
- Routine Smartcard spot checks will be carried out at regular intervals. Staff found not to be observing the Smartcard policy will be required to repeat their IG training modules.

5. Lost, stolen or Broken Smartcards

Staff members must report the loss, breakage or theft of a Smartcard to their line manager, or sponsor, as soon as it is known that the card is missing. They will in turn report it to:
- Craig Thomas at INWL so that it can be revoked and replaced as soon as possible.
- CLH Analyst in order for CLH's Incident Reporting Database to be updated where necessary.

6. PIN/Pass-code Unlocking/Changing

Users who have forgotten their PIN/pass-code or suspect that it may be known by another, or who have been locked out of Choose and Book because of three failed log-in attempts should report the problem to Monika Truszczynska at CLH. If she is unavailable, they should contact the INWL Service Desk (number at beginning of policy).

7. Incident Reporting

Incidents may be reported by any member of staff where they feel that there is a risk to patient health, patient confidentiality, or the reputation of CLH. Incidents should be reported to your Line Manager and the Head of Performance and Information. Examples of incidents are:

- Smartcard or application misuse
- Smartcard theft
- Non-compliance of local or national RA policy
- Unauthorised access of applications

- Unauthorised alteration of patient data

The Head of Performance and Information and relevant Service Delivery Manager together with the Analyst will consider all incidents reported. Any incidents considered significant will be escalated to the IG Manager or Caldicott Guardian. A significant incident is an isolated incident or series of less significant incidents that could lead to a serious degradation of healthcare or information security. The IG Manager or Caldicott Guardian will consider incidents reported to them and decide whether CLH systems or working practices should be reviewed as a result.

Incidents involving breaches of security or demonstrating that a user may not be considered trustworthy should also be report to the Head of Performance and Information, who may request that the certificate associated with the Smartcard should be suspended or revoked as appropriate. If Smartcard misuse is discovered, appropriate disciplinary action will be taken.

8. Reviewing this Policy

This policy will be subject to review when any of the following occur:

- The adoption of its standards highlights errors and omissions in its content
- When other standards/guidance issued by INWL conflict with the information contained
- Where good practice evolves to the extent that revision would bring about improvements
- One year's elapse after approval of the current version