Hull Teaching Primary Care Trust

REGISTRATION AUTHORITY POLICY

06.02.08

CONTENTS

1. INTRODUCTION

Hull Teaching PCT has responsibilities as a Registration Authority (RA), enabling users to gain secure and appropriate access to the National Care Records (NCRS) applications. This policy sets out the approach it has taken to ensure compliance with the Registration Authority National Policies and Procedures.

With the introduction of the NCRS it is vital that patients are confident that their medical records are secure and confidential and accessed appropriately. The registration process consists of three distinct activities:

- Registration of identity (a user is sponsored to be issued with a Smartcard and has their identity checked). A personal details record is created in the Spine User Directory by the RA Agent.

- Choosing appropriate access, which may change if staff move into other roles or other organisations, or with the development of roles. A profile requires a sponsor's approval and their access rights are granted by the RA Agent.

- Creating a card that links the user to their access profile(s) and therefore allowing access to the NCRS.

The above mentioned process is based upon the employee's organisation(s), role(s), area(s) or work and activities which make up their access profile. Access profiles give staff access to patient information and software functions that they need to perform their role within the organisation.

Hull Teaching PCT must ensure that staff have appropriate access to NCRS applications in accordance with their role.

2. SCOPE

2.1 This policy applies to all PCT employees, independent contract staff and partner organisations (GP, Pharmacists, other NHS organisations, contractors etc) irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner and reasonable adjustments will be made where appropriate (e.g. interpreter or signing provision, access arrangements, induction loop, etc.).

3. ROLES AND RESPONSIBILITIES

3.1 RA Manager

3.1.1 The RA Manager is responsible for ensuring adherence to the RA Policy and RA governance arrangements. The RA Manager is also responsible for the efficient day to day operation and capacity planning of the RA function. The RA Manager responsibilities include the following:

- Manage the day-to-day operation of the PCT's RA function
- Ensure the national RA processes for card issue/revocation and profile modification are adhered to
- Establish and ensure compliance with the RA Policy in support of national processes
- Ensure RA forms are appropriately used
- Identify, sponsor and register RA Agents
- Ensure RA Agents / Sponsors are sufficiently responsible and trained to operate the National RA processes, equipment and applications
- Ensure there is sufficient capacity in the RA function to meet the operational and clinical needs in the PCT
- Escalate process, hardware and application problems to the SHA
- Provide support to the RA Agent(s) and Sponsors
- Ensure all RA forms and any other material which supports the issue/revocation of a Smartcard and the role profiles associated with the card are kept in a secure area to which the RA Agent and HR team have access
- Champion the importance of all Smartcard users adherence to security standards imposed by access control.
- Responsible for managing the audit / disciplinary process for breaches in access control.

3.2 RA Agent

3.2.1 The RA Agent is responsible for ensuring RA services are delivered in accordance with the policy and governance requirements to users of RA services. RA Agents are appointed by the RA Manager and are accountable to the RA Manager. The RA Agent responsibilities include the following:

- Responsible for the day-to-day operation of the local Registration Authority, ensuring that national requirements are met at a local level and appropriate, safe systems are in place and adhered to
- Ensure RA forms have been completed with valid information
- Enter this information accurately onto the Spine User Directory
- Issue Smartcards to users who have been sponsored and who have suitably proven identities in accordance with the national processes
- Update user's Smartcard profiles in accordance with the sponsor's requirements
- Revoke certificates when required by sponsors, or in the instance of a breach of security
- Ensure National RA processes are adhered to within the PCT
- Escalate process, hardware and application problems to the SHA

- Provide support to Sponsors on process, hardware and application problems (escalating to other experts such as the IT Department where appropriate)
- Ensure all RA forms and any other material which supports the issue/revocation of a Smartcard and the role profiles associated with the card are retained in accordance with the National RA processes
- Monitor registration of users assigned to or employed by the PCT
- Keep a record of authorised sponsors with their signatures and scope of authority
- Ensure there are sufficient numbers of Smartcards and Smartcard issuing and maintenance equipment for the PCT
- Ensure Sponsors are appropriately briefed on their role
- Support the training of newly allocated Smartcard users the importance of adherence to security standards imposed by access control.
- Undertake regular audit of access control ensuring all breaches are identified and reported to the RA Manager to support security requirements.
- Support the sponsor in the identification of the appropriate roles as set out in the 'Role Based Access Control' standards.

3.3 Sponsor

3.3.1 Sponsors are responsible for approving, where appropriate, the registration and profiles to be granted for users. Additionally they are responsible for the appropriate issue of Fallback Smartcards, passcode resetting and vouching for the identity of users (all within the policy, governance arrangements and national processes). The following staff roles may act as sponsors for staff under their supervision:
- GPs
- Assistant Directors
- Primary Care Support Managers
- Practice Managers
- Pharmacy Advisors

The above list is not exhaustive.

3.3.2 Sponsors may only sponsor users who do not fall within their own area of supervision if they are either locum/out of hours/staff sub-contracted and the sponsor has a responsibility for supervising their practice in relation to their PCT work; GP practices may nominate sponsors who are Deputy Practice Managers and/or Senior Reception Staff whose only RA responsibility is to reset PINs in the absence of the Practice Manager; Locum GPs/Pharmacists will be sponsored by the Practice Manager and must provide documentation (e.g. GMC registration for GPs). Sponsor responsibilities include:

- Ensuring that they are familiar with the extent of the functionality and information access that the roles relevant to their work area confer
- Ensuring that they are familiar with the access needs of the staff under their supervision
- Ensuring the system roles and any additional business functions assigned to staff under their supervision are not excessive and are appropriate to their job roles
- Escalating role profile problems to the RA Agent
- Completing appropriate parts of the RA forms and any other material which supports the issue/revocation of a Smartcard and the role profiles associated with the card in a timely manner
- Ensuring the accuracy of the information on the RA forms
- Where they are confident they can substantiate knowing an individual for at least two years (they must have been providing clinically related or support services for the organisation continuously for two years) they can vouch for the identity of staff. If they can't, the suitability of the user should be confirmed in writing by the HR Department. If neither the HR Department nor the sponsor can vouch for the individual's identity the individual must produce full documentary evidence, as per national requirements and processes.
- Understand the latest version of the IG RBAC Control Names and Codes and any application based RBAC material. Sponsors must understand the implications of approving job roles and activities
- Work with the RA Agent to maintain appropriate access to the NCRS, ensuring that access is consistent with the NHS Code of Confidentiality and national requirements
- Ensuring user profiles are reviewed as job roles change
- Ensuring certificates are revoked when users leave (e.g. sponsors must complete an RA02 form and forward it to the RA Agent at the earliest opportunity)
- Ensure staff have attended appropriate training in applications and modules before access is granted
- Unlock Smartcards, reset logon passwords and perform certificate updates

3.4   Users

3.4.1 Users are allowed a Smartcard/job profile when they have been sponsored by a sponsor and set-up by the RA Agent.   User responsibilities include:
- Ensuring they keep their PIN codes or pass codes confidential
- Ensuring they keep their Smartcard secure and that they only have one card (e.g. if they lose a card and are issued with another one they must return the old one to the RA Agent immediately if it is found subsequently)
- Ensuring that no-one else uses/has access to their card or account

- Reporting any loss, theft or suspected misuse to the RA Agent immediately
- Ensuring that they comply with the terms and conditions that are outlined on the RA01 form
- Ensuring that they have attended formal training before accessing the appropriate applications and modules

4. SMARTCARD MISUSE

If a member of staff is suspected of Smartcard misuse the incident must be reported via the Trust's Incident Reporting Mechanism within the organisation and to the RA Agent immediately. Depending on the circumstances the Smartcard may be suspended or revoked. Smartcard misuse within the PCT may result in disciplinary action as per the PCT's Disciplinary Policy. Allowing someone else access to a Smartcard would be viewed as serious Smartcard misuse.

5. REGISTRATION PROCEDURES

The PCT will adhere to national procedures located on the NHS Connecting for Health website. The RA Agent will regularly check the website to ensure that any changes or amendments of national processes are adhered to within the PCT.

6. CONFIDENTIALITY

All personal data held by the Registration Authority relating to registration processes are considered to be sensitive information and must be protected in accordance with the national processes, set within the Data Protection Act framework. The PCT will ensure that systems are established and maintained to ensure information is retained confidentially which will include the following:

Documentation will be stored in a locked, secure cabinet within the HR Department. Access will be limited to members of the HR team.

The information stored will only be used in relation to the registration process.

The RA Agent will ensure that relevant information including evidence that has been used to verify the individual (such as passport number, driving licence number, via the RA01 form) is logged appropriately.

SUPPORTING POLICIES AND GUIDANCE

The following policies and guidance will support the Registration Authority Policy:

Confidentiality:NHS Code of Conduct
Data Protection Act 1998
The Data Protection (Processing of Sensitive Personal Data) Order 2000
Human Right Act 1998
Computer Misuse Act 1990
Caldicott Principles
Records Management Policy
Information Security Policy

7. REVIEW

7.1   This policy will be reviewed in partnership with the recognised trade union partners within 2 years of the date of implementation.

Author: Lisa Pipes
Title: HR Business Partner
Date: 17th October, 2007

Approved by: Date:

Reviewed by: Date: