NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE POLICY

IT01 Corporate Registration Authority

Policy Number:	**IT01**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint SIRO &Information Governance Committee**
Approving Committee:	**Executive Committee**
Date Ratified:	**September 2018**
Next Review Date (by):	**August 2021**
Version Number:	**August 2018 – Version 1.7**
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**Deputy Director of Informatics Systems Support Manager**

TRUST-WIDE POLICY

2018 – Version 1.7

Striving for perfect care for the people that we serve

NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE POLICY

IT01 Corporate Registration Authority

Further information about this document:

Document name	**Corporate Registration Authority Policy IT01**
Document summary	The Registration Authority (RA) process must have a controlled and secure method of implementation throughout its life cycle to ensure that patient and personnel information accessed through the national applications is kept as secure as possible
Author(s) Contact(s) for further information about this document	**Christine Cowell** **Head of Informatics and Systems** **Telephone: 0151-473-2982** **Email:christine.cowell@merseycare.nhs.uk** **Fiona Jones** **System Support Service Manager** **Telephone: 0151-296-7876** **Email: fiona.jones@imerseyside.nhs.uk**
Developed by consultation with	**Linda Yell** **Information Governance Manager** **Kathryn Saul** **Senior RA Technician**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Foundation Trust** **V7 Building** **Kings Business Park** **Prescot, Merseyside** **L34 1PJ** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	IT02 – IM & T policy, IT12 Information Governance policy, IT10 Confidentiality & Data Sharing policy, IT14 Data Protection policy.
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
IT01 Version 1	RA Manager & IT Systems Security Manager	March 2010
IT01 Version 1.1	RA Manager & IT Systems Security Manager	July 2013
IT01 Version 1.2	RA Manager & IT Systems Security Manager	December 2014
IT01 Version 1.3	Head of Informatics & Systems, System Support & Development Services Manager	August 2015
ITO1 Version 1.4	Head of Informatics & Systems, System Support & Development Services Manager	October 2015
IT01 Version 1.5	Head of Informatics & Systems, System Support & Development Services Manager	June 2016
IT01 Version 1.6	Deputy Director of Informatics, System Support & Development Services Manager	April 2017
IT01 Version 1.7	Deputy Director of Informatics, System Support Development Services Manager and presented to Policy Group Ratified by Executive Committee	August 2018 September 2018

SUPPORTING STATEMENTS – this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child / adult abuse and neglect through their observation of abuse, or by professional judgment made as a result of information gathered about the child / adult;
- knowing how to deal with a disclosure or allegation of child / adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child / adult concern;
- ensuring appropriate advice and support is accessed either from managers,
- *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

CONTENTS

1. INTRODUCTION

1.1 A Registration Authority (RA) manages Smartcards and the registration and access control processes. The role of the RA is to ensure all users of Smartcard Enabled applications are provided with the appropriate levels of access through the Smartcard system and have their identity rigorously checked. The RA comprises of the RA Manager, Agents and Sponsors and Local Smartcard Administrators.

1.2 For Healthcare Professionals to access NHS Digital applications, spine enabled clinical and administrative systems and the NHS Care Records Service (NCRS), they must be registered by the RA.

1.3 The registration process applies nationally and must meet the current Government requirements.

1.4 All the Smartcard Enabled applications use a common security and confidentiality approach. Access levels are identified in terms of organisation code(s), role code(s), and business function(s).

1.5 The method by which users will be able to access a National application is via a Smartcard issued during the Registration Process. The Informatics Merseyside Registration Authority manages the distribution and maintenance of Smartcards on behalf of the Trust.

1.6 Once an applicant has been successfully registered they will have a Unique User ID (UUID), Passcode and Smartcard – which will permit their access to the appropriate application (s) and information.

1.7 The use of the word staff in this document means people who are directly employed by, or contracted to provide service to, or are part of an agreement with the Trust.

2. STATEMENT OF INTENT / SCOPE OF THE POLICY

2.1 This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate.

2.2 This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non- compliance may also lead to criminal action being taken.

3. SUMMARY

3.1 This document describes procedures for the operation of the Registration Authority (RA) and Smartcards within Mersey Care Foundation Trust (hereafter known as the Trust).

3.2 The Registration Process is operated at a local level by a Registration Authority (RA) who is required to conform to the National Registration Policy and Practices identified below.

3.3 The Trust will comply fully with the latest published National Policies and Procedures identified in the following documents:

1. Registration Authority Policy v1.0 2 September 2014
2. NHS Employers Identity Checks (September 2017)
3. Registration Authorities Operational and Process Guidance V5.2 2016
4. The NHS Confidentiality Code of Practice (2003) (www.dh.gov.uk)
5. On-line Terms and Conditions or RA01 Terms and Conditions
6. NHS Operating Framework 2012/13
7. NHS Care Record Guarantee (2011)
8. NHS Code of Practice (Part 2- 2009)

These documents are available via https://www.digital.nhs.uk/Registration-Authorities-and-Smartcards

3.4 The procedures covered in this document are the local support procedures necessary to support the National Policies and Procedures.

4. DEFINITIONS

4.1 Smartcard Passcode

4.1.1 The Smartcard Passcode enables a user to authenticate to the NHS CRS. This Passcode must be 4-8 characters in length, alphanumeric and a mixture of upper/lower case.

4.2 NHS CRS and other Smartcard Applications

- 4.2.1 These following applications are currently used by Mersey Care Foundation Trust via NHS Smartcards:
  - Care Identity Service (CIS Registration Authority) – referred to as National RA System to avoid confusion locally with the Trust CIS Choose and Book (C&B) now known as E-Referral Service (ERS)
  - RiO
    EMIS
  - Summary Care Record (SCR) also known as Clinical Spine Application (CSA)
  - National Health Service Spine Portal
  - Secondary Users Service (SUS) Electronic Staff Record (ESR)
  - System1

4.3 RBAC / Job Roles

4.3.1 Role Based Access Control (RBAC) defines a national standard set of Job Roles and related activities which can be approved by a Sponsor and granted by the RA to a User. Each application, such as E-Referral System uses these definitions to enable access to specific functionality and information in their system.

4.4 PBAC / Positions

4.4.1 Position Based Access Control (PBAC) simplifies how access rights are granted to a user. PBAC builds on the existing Role Based Access Control (RBAC) security model, which provides access to NHS CRS compliant systems appropriate to the job that staff have been employed to do.

4.5 A Significant Incident

4.5.1 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.

5. ROLES & RESPONSIBILITIES

5.1 Executive Director of Finance

5.1.1 Overarching responsibility, Delegated by Chief Executive for ensuring systems and processes are in place to ensure compliance with registration authority requirements.

5.2 Registration Authority (RA) including RA Manager, Agents and Sponsors and Local Smartcard Administrators:

5.2.1 The Registration Authority (RA) is an official Team supplied by Informatics Merseyside with appropriate organisational authority and is responsible for ensuring that all aspects of registration services and operations are performed in accordance with National policies and procedures (See section 1).

5.2.2 The RA Team comprises of RA Managers and RA Agents, Sponsors and Local System Administrators are Mersey Care Trust staff and are not included in references to the Registration Authority.

5.2.3 There needs to be a Board level individual within the Trust who has overall accountability in the organisation for RA activity. The responsible individual must report annually to the organisation on this activity and must sign off on RA Data Security and Protection Toolkit submissions.

The named individual is currently:

Asim Patel
Interim Chief Information Officer
V7 Building, Kings Business Park Prescot L34 1PJ
Tel: 0151 473 2982 Email: asim.patel@merseycare.nhs.uk

5.2.4 The RA is responsible for providing arrangements that will ensure tight control over the issue and maintenance of electronic Smartcards, whilst providing an efficient and responsive service that meets the needs of the users and the Trusts patients.

5.2.5 The Registration Authority has the following responsibilities:

5.2.5.1 Ensuring that the National Registration processes are adhered to in full.

5.2.5.2 Ensure that Self Service functionality i.e. passcode changes / certificate renewal and un-locking is used where possible when this functionality becomes available.

5.2.5.3 Ensure that requests are correctly submitted and authorised on the Care Identity Service (CIS) system

5.2.5.4 Ensuring that requests are logged via the Service Desk as appropriate.

5.2.5.5 Ensuring that any forms, historically paper forms but currently CIS on-line forms, are used appropriately.

5.2.5.6 Ensuring that any local processes developed to support the National Registration processes are adhered to in full.

5.2.5.7 Ensure Sponsors are familiar with and understand User Registration - Sponsor Briefing (available via https://www.digital.nhs.uk/Registration-Authorities-and-Smartcards)

5.2.5.8 Ensuring Sponsors, Agents and Local Smartcard Administrators have completed appropriate training

5.2.6 They will be individuals capable of trust as they will be handling sensitive information covered by the Data Protection Act 2018 and European Directive: General Data Protection Regulation.

5.2.7 They will be key players in ensuring the NHS Code of Confidentiality and RA Terms and Conditions are followed.

5.2.8 The services available to RA Managers and Agents are:

5.2.8.1 New User registration

5.2.8.2 Re-open a User

5.2.8.3 Role profile and Position maintenance

5.2.8.4 Adding role profiles

5.2.8.5 Changing role profiles

5.2.8.6 Deactivating role profiles

5.2.8.7 Revocation and cancelling of Smartcards

5.2.8.8 Passcode resetting (changes/un-lock) – also available to Sponsors and Local Smartcard Administrators

5.2.8.9 Changes to account recovery settings, when this functionality becomes available

5.2.8.10 Smartcard renewal

5.2.8.11 Certificate renewal – also available to Sponsors and Local Smartcard Administrators

5.2.8.12 Certificates renewal for expired certificates.

5.2.8.13 Search for a position

5.2.8.14 Create a position
5.2.8.15 Modify multiple access profiles

5.2.9 The above arrangements cover all Trust RA requirements with the exception of those services and staff which formerly made up the Liverpool cohort of the former Liverpool Community Health (LCH). These services and staff receive RA services from the former LCH RA Team who work within the Human Resources Team. All responsibilities and references to RA Manage or RA Agents apply as appropriate to each Team.

5.3 Registration Authority Manager:

5.3.1 The RA Manager must ensure that all RA procedures are carried out in accordance with local and national policy.

5.3.2 Upon detection or notification of any issues relating to RA the RA managers would contact the IG Manager, or nominated deputy, in order for an adverse incident to be raised and further investigation.

5.3.3 The Registration Authority Manager is responsible for running the governance of RA in Mersey Care. As such they must agree and sign off on local operational processes with the Trust and should assure themselves regularly that these processes are being adhered to. They are also responsible for:

5.3.3.1 Ensuring that there is sufficient availability of resource to operate the registration processes in a timely and efficient manner to meet organisational responsibilities
5.3.3.2 Ensuring that the RA Agents, Sponsors and Local Smartcard Administrators are adequately trained and familiar with the local and national RA policies, procedures and processes
5.3.3.3 Assign, sponsor and register RA Agents.
5.3.3.4 Register Sponsors and Local Smartcard Administrators as instructed by the Trust.
5.3.3.5 All completed forms and associated documents are kept secure in an area where the RA have access. This is in line with records management: NHS Code of Practice (Part 2- 2009) which stipulates retention periods for RA records.
5.3.3.6 Ensuring that an indexed and secure audit trail is maintained of applicant's registration information and profile changes.

5.3.3.7 Ensuring that there are sufficient Smartcards and Smartcard issuing/maintenance equipment for the organisation.

5.4 Registration Authority Agents:

5.4.1 Registration Agents are responsible to the RA Manager for ensuring that the national and local processes are followed and for the accurate input of information on the Care Identity Service (CIS).

5.4.2 Registration Agents will ensure that all inter-Trust agreements are followed and adhered to. All incidents, misuses, anomalies and problems will be reported to the RA Manager and via Datix Incident Reporting System.

5.5 Registration Sponsors:

5.5.1 Sponsors are appointed and entrusted to act on behalf of the Trust in determining who should have what access and maintaining the appropriateness of that access. This role carries a significant level of responsibility and cannot be delegated. Sponsors will have a line management or peer relationship for staff that they Sponsor.

5.5.2 Staff will be identified as Sponsors by the Trust on behalf of the Trust Executive as being suitable persons by virtue of their status and role. They will be staff with sufficient seniority to understand and accept the responsibility required and will be registered by the RA Manager or Agent on behalf of the Trust in accordance with instructions given by the Trust. Sponsors have two specific responsibilities:

5.5.2.1 Identification of the type of access to information a user or a position needs via an NCRS application – the organisation they belong to and their Role Profile.

5.5.2.2 Overseeing the appropriate use of the cards and ensure that any incidents or breaches are reported on Datix and to the RA Manager.

5.5.3 Sponsors are responsible for approving, on behalf of the Trust, who can have access to what information. They are responsible to the Trust to ensure only appropriate access to National applications is approved. They will be held accountable by the Trust for their actions.

5.5.4 Sponsors are responsible to the RA Manager for the accuracy of the information provided through the RA system.

5.5.5 All Sponsors are required to provide documentary evidence to prove their identity.

5.5.6 Sponsors / approvers are responsible for making sure that national application users are given the minimum appropriate level of access needed to perform their job.

5.5.7 The areas of responsibility with respect to national application user access should be clearly defined for each Sponsor Sponsors and Agents will report any RA related incidents, using the Datix Incident Reporting System, in line with the Trust Incident Reporting Procedure, and to the RA Manager.

5.5.8 Additionally, Sponsors and RA Agents will report any operational difficulties, especially where these have patient healthcare implications, to the RA Manager.

5.5.9 Sponsors are also able to change and unlock Passcodes – this must only be done when the Smartcard Holder is present in a face to face meeting and the

Smartcard Holder sets their own Passcode confidentially.

5.5.10 Sponsors also have the ability to assist in the renewal of Smartcard Certificates when the Smartcard Holder is present in a face to face meeting and the Smartcard Holder sets their own Passcode confidentially as part of the renewal process.

5.5.11 Local Smartcard Administrators (LSA's) have the ability to Unlock/Reset a Smartcard – this must only be done when the Smartcard Holder is present in a face to face meeting and the Smartcard Holder sets their own Passcode confidentially.

5.5.12 Local Smartcard Administrators also have the ability to assist in the renewal of Smartcard Certificates when the Smartcard Holder is present in a face to face meeting and the Smartcard Holder sets their own Passcode confidentially as part of the renewal process.

5.5.13 However staff should be encouraged to use the self-service portal, when available, to change their own passcodes, self- un-lock (where details have been provided) and renew their Smartcard certificates.

5.5.14 Sponsors must ensure that the RA Team are informed if a staff member leaves or changes roles, by making a request to end the access on the RA system and also log a request with the IT Service Desk.

5.5.15 Sponsors act as an intermediary between the RA and the users to disseminate information.

5.6 Board of Directors

5.6.1 RA Managers & Sponsors are appointed by the Trust and this appointment is confirmed in a letter of appointment which must be held by each individual appointed to these positions. Copies of these letters should also be held by the RA Manager so they are able to provide the necessary evidence to meet Data Security and Protection Toolkit requirements.

5.6.2 Notification of the creation and revocation of RA Managers (including their e-mail address) should be sent to accesscontrol@nhs.net

5.7 Responsibility for identifying Sponsors and Local Smartcard Administrators

5.7.1 The Trust delegates responsibility for identifying Sponsors and Local Smartcard Administrators to Operational Management Board, Corporate, Local, SLD and Secure.

5.9 Caldicott Guardian:

5.9.1 The Caldicott Guardian will consider incidents reported to them and decide whether Trust systems or working practices should be reviewed as a result.

5.10 Human Resources personnel:

5.10.1 Incidents involving breaches of security that demonstrate that a user may not be considered trustworthy should be reported to HR and the Caldicott Guardian by the RA Manager so that any disciplinary measures required may be taken.HR will decide which other members of staff need to be involved (e.g. line manager).

5.11 All Users of the RA Service:

5.11.1 It is the responsibility of all users to comply fully with the latest published National Policies and Procedures identified under section 3, and to adhere to local policies and procedures and undertake Information Governance/Information Security training.

5.11.2 Users are required to accept the RA terms and conditions.

5.11.3 Lost or stolen Smartcards must be reported as soon as possible to the RA and on the Datix Incident Reporting System. The RA will cancel the lost/stolen card and arrange a re-issue.

5.11.4 A user must not use a Smartcard to prove NHS identity.

5.11.5 All Smartcard users must ensure the security of their cards, and not share the physical Smartcard or the confidential Passcode with anyone, nor are they to leave their card unattended at any time.

5.11.6 Smartcards should always be kept in a safe and secure place when not in use e.g. a locked drawer or secure locker and never to be left logged in.

5.11.7 It is the responsibility of the user to ensure that they have their card available in work. It is recognised that some users work at multiple bases and may need to take their cards home.

5.11.8 If the user forgets their card it is their responsibility to make alternative arrangements. It is recommended that the user returns home to retrieve their card and make the hours up at a later date. If this is not possible the user should take alternative tasks that do not require a Smartcard.

5.11.9 A user taking an extended period of absence, i.e. longer than 3 months, will have their access removed until they return.

5.12 Joint SIRO & Information Governance Committee:

5.12.1 The Joint SIRO & Information Governance Committee is a formal working group to oversee and coordinate the technical and organisational security measures that need to be place for all the key Information assets. This ensures the confidentiality, integrity and availability of information and complies with the ISO 27001 Information Security Standard.

5.12.2 The group will consider incidents reported to them and decide whether Trust systems or working practices should be reviewed as a result. The group will

escalate incidents through the Risk Management Structure where appropriate.

5.12.3 The Information Governance Manager will oversee all reports of incidents reported, escalating as appropriate.

5.13 All Trust Managers:

5.13.1 All managers are directly responsible for implementing the policies and procedures within their business areas.

5.14 All Trust Staff:

5.14.1 It is the responsibility of each employee to adhere to the policies and procedures and undertake Information Governance/Information Security training.

5.14.2 It is the responsibility of all staff to inform the Information Governance Manager of any information security related incident which has occurred in their area.

6. THE POLICY

6.1 Incident Reporting

6.1.1 Incidents may be reported by any member of staff where they feel that there is a risk to patient health, confidentiality or Trust reputation. Incidents should be reported, using the Datix Incident Reporting System, in line with the Trust Incident Reporting Procedure, Corporate Policy & Procedure for The Reporting, Management and Review of Adverse Incidents (including serious untoward incidents and near misses) SA03, and to the RA Manager.

Examples of incidents include but are not limited to:

- Smartcard or application misuse.
- Smartcard loss or theft.
- Inappropriate levels of access
- Non-compliance of local or national NHS RA policy.
- Any unauthorised access of national applications.
- Any unauthorised alteration of data.

6.1.2 The RA Manager will consider all incidents reported to them. Any incidents considered significant will be escalated through the risk management structure and to HR and/or the Trust Caldicott Guardian depending on the nature of the incident.

6.1.3 A major breach of security / significant incident will also be reported by the RA Manager to the System Supplier and NHS Digitalto ensure that any risks resulting from the event can be taken into account and mitigated against.

6.1.4 Security incidents reported directly onto Datix Risk Management System are

reviewed by each Division. The Information Governance Manager is made aware and the incidents are reviewed formally at the Joint SIRO & Information Governance Committee.

6.1.5 Information Security incident reports via Datix will also be reviewed at the Information Governance Committee to identify whether any further action is required, in addition to any actions taken at the time of the incident or by the risk coordinator/governance lead. In the event that an NCRS application becomes unavailable due to a technical failure, this will need to be reported immediately to the Service Desk and will be escalated to the NHS Digital National Service Desk for resolution, as appropriate.

6.1.6 Monitoring of the RA process any associated risks or incidents will be overseen by the Joint SIRO & Information Governance Committee.

6.1.7 Departments will need to invoke local contingency plans, as appropriate, to minimise any disruption to services during the period of unavailability.

6.2 Processes

6.2.1 The Trust will ensure that processes supporting the identification, registration and management of staff will be integrated with other Trust processes as appropriate, e.g. recruitment process, starters and leavers, disciplinary policy, use of agency/locum/bank staff etc.

6.3 Starters

As part of normal induction processes new staff required to use NCRS applications will be:

- Introduced to the relevant Sponsor who will identify the appropriate RA access position for the user and take them through the Trust RA processes required.
- Trained on the aspects of national application use relevant to their role(s).
- Made aware of the National and Trust RA processes.
- Where full registration is required; the applicant will be required to bring suitable forms of identification with them.
- Where staff are recruited to a role which requires access to National Applications it is important that the following points are considered:

    - Checks on an applicant's ID are made during recruitment to ensure e-Gif Level 3 identification requirements can be met
    - Offers of employment are dependent on the applicant's ability to meet and continue to meet all requirements for national application access
    - Induction processes include the issuing of Smartcards (where the applicant is not an existing Smartcard holder) and adding of the appropriate access position(s)
    - Staff should be trained sufficiently prior to the use of Smartcards and/or national applications
    - Staff must digitally sign to accept the NHS Care Records Service

Smartcard Terms and Conditions at issuance of the smartcard once this functionality is available.

- All national application users must have sufficient training to carry out their tasks without risk.

All the above processes will be integrated into the standard employment processes of the Trust, as much as possible to prevent duplication.

6.4 Leavers and Revocation

6.4.1 When staff leave the Trust, the following points must be considered:

- All Trust access positions/role profiles in the RA System pertaining to the employee must be removed as soon as is practical.
- If the user if transferring to another NHS related location e.g. GP practice, CSU, or Acute Trust etc. the user is allowed to retain the Smartcard but their Trust profile in this Organisation is removed. If the new employer should request, in writing, a user's RA documentation, a copy may be provided to them if essential
- Staff permanently leaving the healthcare environment should have their user registration closed and the Smartcard issued to them should be destroyed (Examples of permanently leaving would include retirement, leaving for employment in a non-NHS job or taking up full-time education etc.).

The required actions must be taken as soon as possible.

6.4.2 In the event of a member of staff leaving with immediate effect, it is the responsibility of the line manager to ensure that the Smartcard is recovered before the member of staff leaves the premises, a job needs to be logged via the IT Service Desk for the Smartcard to be collected by hand by a member of the RA Team – the card will then be revoked, destroyed and securely disposed of. In addition the RA Manager will receive an alert on dismissal of a member of staff.

6.4.3 During the leaving process HR and/or the Sponsor will establish whether the User is leaving the NHS permanently (retirement, education or a non-NHS job) or joining another NHS organisation.

6.4.4 Where the user is moving to another NHS organisation, HR and/or the Sponsor will notify the RA Manager who will arrange for any access associated with Mersey Care NHS Foundation Trust to be removed.

6.4.5 There are other occasions when it is necessary to deactivate a Smartcard by revoking the Smartcard certificate or cancelling the card.

Reasons for this include:

- The Smartcard is lost or stolen

- There has been some other security breach associated with the Smartcard, Smartcard certificate and/or the Smartcard Passcode.

6.4.6 Revocation tasks can only be carried out by RA Team Members.

6.4.7 Where the revocation is needed due to a staff member leaving the Trust, the line manager will log a request via Service Desk and the Sponsor will raise a request in the RA CIS System. As an extra precaution, HR will inform the RA of any leavers, by means of a monthly leaver's reports.

6.4.8 Where the revocation has been requested by HR because of security related events the RA Manager will authorise the appropriate action and inform the following staff as appropriate:

- The HR Manager
- The relevant Sponsor(s)
- Revocation renders the Smartcard useless.
- Revocation can only be carried out by Registration Managers and Agents.

6.4.9 Where a card has a secondary use, e.g. for door access, it is the responsibility of the department issuing access to remove access, they must link in with the HR and resourcing department to link in with the leavers process.

6.5 Appropriate Identity Documentation

6.5.1 To ensure compliance with the current Registration Authorities Operational Processes and Guidance and the NHS Employers - Verification of Identity Checks, the Registration Authority must follow nationally agreed processes as detailed in section 6.2, including that all Smartcard users/applicants must provide either:

1. Two forms of personal photo ID and one active in the community document or
2. One form of personal photo ID and two active in the community documents. National Insurance Number should also be available at registration.

6.6 Acceptable Photo Personal Identity Documents

- Current UK passport or EU/other nationalities passport.
- Passport of non-EU nationals, containing UK stamps, a visa or a UK residence permit showing
- the immigration status of the holder in the UK
- A current UK or EU/other nationalities photo-card driving licence
- A national ID card and/or other valid documentation relating to immigration status and permission to work.

Any document NOT listed above is not acceptable.

6.7 Acceptable Proof of Address 'Active in the Community' Documents

6.7.1 To confirm address, various documents are acceptable as detailed in NHS

Employers Identity Check.
* The date on any documents presented should be within the last six months (unless there is a good reason for it not to be, e.g.: clear evidence the user has not lived in the UK for six months or more) and all the documents must contain the name and address of the applicant.

6.8 Active in the Community Documents

6.8.1 Active-in-the-community documents shall have all the following properties:

1. Documents must be issued by a trusted source;
2. Each document must be an original or notarised document, not a photocopy or printed from the internet;
3. The document must be valid at the time it is used (it must be current)
4. The document must contain the individual's name;
5. The document must contain the individual's address;
6. The document must be difficult to forge.

6.9 No acceptable photographic documentation available:

6.9.1 If the applicant is unable to provide acceptable photographic personal identification, two forms of non-photographic personal identification and two documents confirming the address must be provided. All four documents must be from different sources. To confirm personal identification, various documents are acceptable as detailed in NHS Digital Guidance.

6.9.2 **In addition** the applicant will need to provide a passport sized photograph, endorsed on the back with a signature of a 'person of standing' in the community who has known them for at least two years.

6.9.3 A 'person of standing' could be a magistrate, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager or civil servant. A full list is available in Appendix One of the Employers Identity Checks.

6.9.4 The photograph should be accompanied by a signed statement from the person of standing, indicating the period of time that they have known the applicant. The statement also needs to contain a legible name, address and telephone number of the person of standing.

6.9.5 Where the User is unable to provide appropriate identification they will not be given a Smartcard and will not be allowed access to national applications.

6.10 Non Trust Employees e.g. Contractors, Students, Locums, Agency and Bank Personnel

6.10.1 Temporary staff filling roles may need access to NHS Digital records as part of their role. The following points should be considered:

- Staff working as part of a team may not need a Smartcard to fill the role if

they are not accessing systems

- Some temporary staff could already be registered and will only require access added temporary staff who are Smartcard holders may not have sufficient training in the use of the particular NHS Digital application needed to be accessed.

- Staff will be required to sign an acceptance of policy and confidentiality agreement prior to being given Smartcard access at the Trust.

6.10.2 The Trust will ensure all non-Trust employees who need to use the national applications are bound to the Data Protection Act and The NHS Confidentiality Code of Practice. This will include the process to be taken in cases of a breach and liability issues.

6.11 Management and use of RA Equipment

The RA Manager, on behalf of the Trust, will be responsible for ensuring that adequate resources are available for the issuance and maintenance of Smartcards. This includes the ordering of Smartcards through the NHS Digital website, the registration of smartcard printers with NHS Digital and contacting Data card (Data Card Printers/SCC (Magi card Printers) directly by email to arrange on site visits for Smartcard printer repairs.

6.11.1 The Trust will ensure that there is sufficient computer equipment to support all users of national applications.

6.12 Management of National Application Users

6.12.1 All Trust RA Team members will receive Training on the use of the National RA System and all relevant RA processes.

6.12.2 Requests for access to the NCRS or national applications should be '**submitted'** on-line using the National RA system and also raised as a request via the IT Service Desk

6.12.3 Requests must be submitted by a registered Smartcard user who has been trained and authorised to submit and/or Sponsor requests. Sponsors should electronically "**Raise Requests"** requests by logging in to the National RA system. Requests can them be *"Granted"* by an RA Agent or Manager.

6.12.4 On-line requests for users in RA system include:

- Create a New User
- Modify a User
- Close User
- Re-Open a User
- User Terms and Conditions

6.13 Record retention

6.13.1 RA01, RA02, Bulk RA02, RA03, RA04, RA05, RA06, RA07, RA08 and RA09 forms are no longer used but, along with any signed photographs and accompanying letters need to be retained in accordance with The NHS England Corporate Records Retention and Disposal Schedule February 2014 or its successor code of practice on records management…."6 years after subject of file leaves service or until subject's 79th birthday whichever is the later". Further detail available here: https://digital.nhs.uk/article/311/Registration-Authorities-and-Smartcards

6.14 Smartcards

6.14.1 Smartcards should be treated with care and protected to prevent loss or damage. They should be kept secure and also in a Smartcard Holder with a Lanyard or Clip.

6.15 Trust name on Smartcards

6.15.1 There will be no Trust name printed on Smartcards issued due to the varied nature of agreements and that staff may retain their Smartcards when transferring to other NHS organisations.

6.16 Lost, Stolen and Broken Smartcards

6.16.1 Lost and damaged Smartcards should be reported to the RA Team as soon as is practical. Once notified of a lost or damaged Smartcard the RA Team will arrange to have the lost / damaged Smartcard cancelled and replaced (see below) as soon as possible.

6.16.2 In the case of loss or theft, the RA Manager must be informed so that checks may be made to ensure that the Smartcard has not been misused.

6.16.3 Loss or theft should be reported immediately via IT Service Desk and logged as a breach in Datix.

6.16.4 When an issued Smartcard becomes unusable, or it is lost or stolen, the Smartcard certificate must be cancelled, see section 6.4.5 Leavers and Revocation. Cancellation renders the Smartcard useless.

6.16.5 The Smartcard holder's identity must be verified at a face to face meeting for a new Smartcard to be issued. In exceptional circumstances a replacement Smartcard may be left with a Sponsor to do the face to face checking and then arrange for the Smartcard Passcode to be confidentially be reset – where the Smartcard Holder inputs the Smartcard Passcode to the replacement Smartcard. Should a lost card be found, a job must be logged with the IT Service Desk and a member of the RA Team will arrange to collect the Smartcard by hand then arrange for the secure disposal of the Smartcard.

6.17 Passcode Unlocking/Changing

6.17.1 Users who have forgotten their Smartcard Passcode, suspect it may be

known by another or who have been locked out of NHS Digital Applications because of three failed login attempts, should report the problem to their Sponsor, Local Smartcard Administrator or the RA Team as soon as possible.

6.17.2 If the user is unable to resolve the issue with their Sponsor (usually their line manager) or Local Smartcard Administrator the RA Team will arrange a time within working hours for the user to have the Passcode unlocked or reset. This task must be carried out face to face by a Registration Agent, Sponsor, or Local Smartcard Administrator. The Smartcard holder must be present and confidentially set their own Smartcard Passcode

6.17.3 Users are also able to change their own Passcode if they have registerd for Self Service Smartcard.

6.18 Renewal of Certificates

6.18.1 Smartcard certificates will expire two years after issue of the card and users should use the 'Self Service Portal' to re-new their own certificates. If the 90 day notifications are ignored the user will need to Log a job via the IT Service Desk for the RA team to have the certificates renewed in an arranged meeting in working hours – the meeting must be face to face and the Smartcard Holder confidentially inputs their Smartcard Passcode during this process.

6.19 Smartcard Misuse

6.19.1 A staff member must report suspected Smartcard misuse in line with Trust incident reporting policy and procedure. Depending on the severity of the allegation an investigation maybe required.

6.19.2 If it is suspected that a Smartcard is being misused then it should be reported to the RA Manager and Information Governance Manager/Information Governance Authority Group who may request that the certificate associated with the Smartcard should be suspended or revoked as appropriate and the user's line manager informed.

6.19.3 If Smartcard misuse by a Trust staff member is discovered the appropriate disciplinary measures must be taken. The RA Manager will consult with HR and the matter must proceed using Trust Disciplinary Processes.

6.20 Positions

6.20.1 What a user is able to access is based on the information built in to the access position. These Positions will be agreed by the Trust and any new or amended Positions should be reviewed and agreed by The Clinical Reference Group

6.20.2 Whenever there is a change in the way a person works, a review of their Smartcard access must be carried out by the Trust. If there are significant

changes to the staff member's role the relevant Position must be added–

- a RA CIS request must be raised by the Sponsor and a job must be logged via the IT Service Desk
- When a user's role in the organisation comes to an end the Assigned RA Position must be scheduled or end dated as soon as possible.
- Where the user is leaving the NHS please refer to section 6.4 Leavers and Revocation.

6.21 Local support processes for National Application users

6.21.1 Users needing support with National Applications should contact the IT Service Desk

6.22 System Supplier Access

6.22.1 As a consequence of RA restrictions in 2008 and in agreement with the Access Control Team (NHS Digital), RA Agents will allow or remove access for supplier system administrators for upgrade, testing purposes, projects or resolution of service calls when the following process is followed:-

1. The access request is received in writing from the supplier.
2. The authorisation of sponsorship is made by Mersey Care Foundation Trust Sponsors via National RA System. The Trust will not devolve RA Agent status to supplier.

Note: The authorisation must contain name, UUID, access required, duration of access and Trust.

7. CONSULTATION AND IMPLEMENTATION

7.1 The responsibility of implementing this document, including RA training and other RA needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

7.2 Line managers must ensure that departmental systems are in place to enable staff including agency staff to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

7.3 This policy has been developed through guidelines from national and local policies and implementation guides for the implementation of Registration Authority.

7.4 This policy has been reviewed and updated after consultation between RA Managers and Head of Informatics.

Christine Cowell	Head of Informatics and Systems	Mersey Care NHS Foundation Trust
Fiona Jones	System Support Manager	Informatics Merseyside
Linda Yell	Information Governance Manager	Mersey Care NHS Foundation Trust
Kathryn Saul	Senior RA Technician	Informatics Merseyside

8. Training and Support

8.1 Registration Authority Training Needs Analysis

8.1.1 All RA Members will have sufficient training to carry out their RA tasks in accordance with Local and National Policies and Procedures.

8.1.2 Training Needs Analysis for all RA Managers, Agents, and Sponsors and Local Smartcard Administrators:-

1. Trust Data Security Awareness Training
2. RA Specific Training (provided by the RA Team on ad-hoc basis)
3. RA modular training.

9. GLOSSARY OF TERMS

9.1 The following glossary has been taken from the Registration Policy and Practices for Level 3 Authentications (NPFIT-NCR-DES- 0294 06) which contains all the Acronyms and terminology within the scope of the national Registration Authority process.

Term	Description
Activation Data	Data values, other than keys, required to operate cryptographic modules that protect private keys. An example of activation data is a PIN or pass phrase. [IETF RFC 2527]
Authority	Authority means the Secretary of State for Health and any party of the Authority such as; contractors, directors, officers, employees and sub- contractors for the purposes of the Project of the Authority, whether employed directly by the Authority or any Authority sanctioned supplier.
ARL	Authority Revocation List – a list of revoked CA certificates (normal reason - CA's signing key was compromised).
BS 7799	A standard on security practices issued by the British Standards Institute and subsequently adopted in 2000 by the International Standards Organisation (ISO). See also ISO 17799-1:2000.

Certificate	See Public Key Certificate.
CA	Certification Authority – the umbrella term given to a range of certification services. In this instance of service provision, the certificate signing functionality is provided by the National Application Service Provider (the Certificate Manufacturer) for the Issuing Authority (IssA); the National Programme for IT.
Certificate Applicant	One who is in the process of registering to become a Certificate Holder (see below), but has not yet been issued the certificate.
Certificate Holder	Digital certificates may be issued to individuals (regulated and non- regulated health professionals, administrators, and support staff) and computer applications, or devices. Each Certificate Holder has been registered to receive a certificate prior to its issuance. In the case of certificates for applications or devices, the Certificate Holder is the individual who is responsible for the use of the certificate by the application or device.
Certificate Holder Agreement	Certificate Applicants and Certificate Holders must agree to protect their private decryption key(s). They must also indicate that they understand the consequences of misuse and agree to accept responsibility for those consequences (including any legal liability if they act negligently). In view of the legal responsibilities involved, Certificate Applicants and Certificate Holders must therefore sign an agreement (sometimes called a "Subscriber Agreement") before they can be issued an encryption certificate. This agreement describes the obligations of each Certificate Applicant/Certificate Holder and is part of the *User Registration*
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the digital signing of information to the level of non-repudiation. [IETF 2527 – framework for CP development]

Certificate Revocation	Act of removing any reliable link between a certificate and its related owner (or security subject owner), because the certificate is not Trusted any more even though it is still unexpired. [ISO 17090] Certificates will also be revoked when they are no longer required for the use against which they were issued; e.g. change of job role does not warrant use of a certificate, though the certificate is still within its validity period.
Content Commitment	Digital signatures which are intended to convey to relying parties, that the signer is committed to the content being signed. Backed by content commitment services in PKI (Public Key Infrastructure), which require both technical and human elements to reach a decision as to whether an action can be repudiated. ***Formerly referred to as non-repudiation***
CPS	Certification Practice Statement – a statement of the practices which a certification authority employs in issuing certificates [RFC2527 – framework for CPs development].
CRL	Certificate Revocation List – a list of revoked certificates created and signed by the issuing CA.
Digital Signature	Extra data appended to a message or data which identifies and authenticates the originator and the data using public key encryption so a recipient can determine: 1. whether the transformation was created using the signer's key; and 2. whether the message has been altered since the transformation was made.
DN	Distinguished Name – a globally unique identifier representing an individual's identity. [INFOSEC-99]. Distinguished Names (DNs) are printable strings that uniquely identify a person, organisation, organisational unit, device, or application and that have a syntax that complies with the X.500 directory standard. According to this standard, the distinguished name of each entry in a directory consists of the entry's relative distinguished name (RDN; see below) and the RDNs of each of the entries that lie directly between the entry and the root of the directory tree. In certificates issued by a Certification Authority, DNs are used to identify the entity that owns the certificate (e.g. an individual health professional or an organisation).
Directory	A special type of hierarchal database that can be used to store encryption certificates in such a way that Relying Parties who want to send an encrypted email or file to recipient can quickly locate the recipient's encryption certificate. Such directory systems conform to the X.500 reference model.
Domain	A domain can be a single organisation or a group of organisations operating a RA under a shared service
ESR	Electronic Staff Record

Encryption	The cryptographic transformation of data so that it's true meaning is rendered totally worthless without the mechanisms to reverse the transformed data. The reverse process is called decryption.
End-Entity	Refers to the entity to which a certificate has been assigned, either an individual or a computer application/device. For certificates assigned to computer devices/applications, the certificate holder must be an authorised responsible member of staff of the organisation owning the computer application\device.
ISO	International Standards Organisation – an international standards- setting body in which the UK actively participates.
ISO 17090	A technical specification from the International Standards Organisation (ISO) on the use of encryption certificates and/or digital signature certificates in health care.

ISO 17799	A standard on security practices originally issued by the British Standards Institute and subsequently adopted in 2000 by the International Standards Organisation (ISO). See also BS 7799.
IssA	**Iss**uing **A**uthority – the authority responsible for the registration policies and procedures that govern the verification of an end entities identity through to the issuance of certificates and their management.
NCRS	**National Care Records Service**
OCSP	On-line Certificate Status Protocol – an on-line method of checking the revocation status of a certificate.
OID	Object Identifier – a unique identifier, consisting of a series of integers separated by dots, assigned to a specific object or class of objects. OIDs are hierarchical in nature and are registered with ISO and with national and organisational registration authorities to ensure that each OID is unique.
PMA	Policy Management Authority – a body responsible for setting, implementing and overseeing the administration of the Certificate Policy and Certification Practices Statement. When this policy has been adapted to support a local implementation of digital certificates, the empanelling of the PMA resides with those responsible for oversight of this local implementation. In addition, the Authority will periodically review and revise all of its guidance documents on encryption and digital signatures, including this one. A committee within the Authority is responsible for this periodic review.

Private Decryption Key	A secret key belonging to the Certificate Holder (and that only the Certificate Holder can access) that is mathematically associated with the public encryption key in the Certificate Holder's certificate. The Certificate Holder uses the private decryption key when decrypting a document, file or message.
Private Signing Key	A secret key belonging to the Certificate Holder (and that only the Certificate Holder can access) that is mathematically associated with the public signature verification key in the Certificate Holder's certificate. The Certificate Holder uses the private signing key when creating a digital signature for a document, file or message.
Public Key Encryption	An encryption scheme, introduced by Diffie and Hellman in 1976, where each person gets a pair of keys, called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his private key. This is often used in conjunction with a digital signature.
Public Encryption Key	A key contained in the Certificate Holder's public key certificate that is mathematically associated with his/her private decryption key. The public encryption key is used by Relying Parties to encrypt information that only the Certificate Holder will then be able to decrypt.
Public Key Certificate	An X.509 public key certificate binds an identity and a public key. The public key together with the identity and related information are digitally signed with the private signing key of the Certification Authority that issues the certificate. The format of the certificate is in accordance with ITU-T Recommendation X.509.
Public Signature Verification Key	A key contained in the Certificate Holder's certificate that is mathematically associated with his/her private signing key. The public signature verification key is used to confirm the authenticity of a digital signature.
RA	Registration Authority – An individual or team that is responsible for identification and authentication of Certificate Applicants and which submits certificates for signing and issuance and certificates for revocation by the CA. Registration Authorities are hierarchical and are referred to as Superior and Subordinate. Subordinate RAs will be accountable to a Superior RA.
RBAC	Role Based Access Control – Use of pre-defined roles as an intermediary between an individual and the resource. Permissions are assigned to roles which are in turn assigned to individuals and extended to include other related attributes such as; Area of Work and Business Function/Activities.

RDN	Relative Distinguished Name – the set of attribute types and values (such as common name, organisation, etc.) that uniquely identify a directory entry among its siblings in the directory hierarchy. Every entry in a directory has a Distinguished Name which is made up of a sequence of RDNs, separated by commas or semi-colons. There can be more than one identical RDN in a directory, but they must be in different branches of the directory tree.
Relying Party	A relying party is an individual who: 1) uses an encryption certificate's public encryption key to send the owner of the certificate (the Certificate Holder, q.v.) an encrypted message or file, hence relying on the identity of the Certificate Holder and the security of the encryption offered to ensure that only the Certificate Holder will be able to decrypt the message or file; or 2) uses a digital signature certificate's public signature verification key to verify a digital signature, hence relying on the identity of the Certificate Holder and the security of the digital signature mechanism to ensure that only the Certificate Holder could have signed the message or file.
Smart Card	An electronic device, the size of a credit card that contains memory and possibly an embedded integrated circuit. Also known as Integrated Circuit Cards (ICC)
Sponsor	A Sponsor is a senior Trusted person within an organisation who represents that organisation to the respective RA, for the purpose of sponsoring users, for which they have direct management responsibility as applicants for Digital Signature Authentication Certificates. Sponsors will also be responsible for the allocation of roles for Role Based Access Control (RBAC) and eventually the allocation of RBAC roles with workgroups. Organisational sponsors are designated by the board of directors or the Caldicott Guardian only.
Scheme	UK Government sponsored scheme to provide given levels of Trust in the services offered by Trust service providers.

Equality and Human Rights Analysis

Title: IT01 Corporate Registration Authority Policy
Area covered: The delivery of Registration Authority process to ensure that patient and personnel information accessed through national applications is kept a secure as possible

What are the intended outcomes of this work? A Registration Authority (RA) manages Smartcards and the registration and access control processes. The role of the RA is to ensure all users of Smartcard Enabled applications are provided with the appropriate levels of access through the Smartcard system and have their identity rigorously checked. The RA comprises of the RA Manager, Agents and Sponsors and Local Smartcard Administrators.

For Healthcare Professionals to access NHS Digital applications, spine enabled clinical and administrative systems and the NHS Care Records Service (NCRS), they must be registered by the RA.

The registration process applies nationally and must meet the current Government requirements.

All the Smartcard Enabled applications use a common security and confidentiality approach. Access levels are identified in terms of organisation code(s), role code(s), and business function(s).

The method by which users will be able to access a National application is via a Smartcard issued during the Registration Process. The Informatics Merseyside Registration Authority manages the distribution and maintenance of Smartcards on behalf of the Trust.
Once an applicant has been successfully registered they will have a Unique User ID (UUID), Passcode and Smartcard – which will permit their access to the appropriate application (s) and information.

Who will be affected? Staff

Evidence

What evidence have you considered?

The policy

The following also referenced within the policy:

- Registration Authority Policy v1.0 2 September 2014
- NHS Employers Identity Checks (April 2016)
- Registration Authorities Operational and Process Guidance V5.0 2015
- The NHS Confidentiality Code of Practice (2003) (www.dh.gov.uk)
- On-line Terms and Conditions or RA01 Terms and Conditions
- NHS Operating Framework 2012/13
- NHS Care Record Guarantee (2011)
- NHS Code of Practice (Part 2- 2009)

Disability (including learning disability)
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people.

Sex
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people.

Race
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people.

Age
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people

Gender reassignment (including transgender)
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people.
The process needs to ensure the confidentiality of people within gender reassignment process whose information is held within the information systems and within the smartcard registering process.

Sexual orientation
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people.

Religion or belief
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people

Pregnancy and maternity
At Policy Review April 2017
This policy is supportive of the trust maintaining the confidentiality for people.

Carers
No issues identified.

Other identified groups
Provision for proof of identity for those without commonly used proof of address or identity accommodated within NHS Employer Identity Checks

Cross Cutting
At Policy Review April2017
This policy is supportive of the trust maintaining the confidentiality for people.

Human Rights	Is there an impact? How this right could be protected?
Right to life (Article 2)	At Policy Review April 2017 Does not engage this part of the Act.
Right of freedom from inhuman and degrading treatment (Article 3)	At Policy Review April 2017 Does not engage this part of the Act.
Right to liberty (Article 5)	At Policy Review April 2017 Does not engage this part of the Act.
Right to a fair trial (Article 6)	At Policy Review April 2017 Does not engage this part of the Act.
Right to private and family life (Article 8)	This policy is supportive of maintain people personal information confidential.
Right of freedom of religion or belief (Article 9)	At Policy Review April 2017 Does not engage this part of the Act.
Right to freedom of expression **Note: this does not include insulting language such as racism (Article 10)**	At Policy Review April 2017 Does not engage this part of the Act.
Right freedom from discrimination (Article 14)	At Policy Review April 2017 Does not engage this part of the Act.

Engagement and Involvement.

This policy has been developed by the Deputy Director of Informatics and the System Support Service Manager with input from RA Manager and submitted to the Policy Review Group

Summary of Analysis At Policy Review April 2017

Eliminate discrimination, harassment and victimisation

The policy does not cause discrimination, harassment or victimisation

Advance equality of opportunity

The policy allows for all staff who need access to Smartcard enabled systems to do so in a safe and controlled manner

Promote good relations between groups

N/A

What is the overall impact?

Policy seeks to protect people's personal information.

Addressing the impact on equalities

There needs to be greater consideration re health inequalities and the impact of each individual development /change in relation to the protected characteristics and vulnerable groups

Action planning for improvement

At Policy Review April 2017

This policy needs to ensure the protection of individuals personal information in relation to gender reassignment within the registration process detailed within.

For the record

Name of persons who carried out this assessment:
Fiona Jones - System Support Service Manager
Meryl Cuzak – Equality and Human Rights Lead

Date assessment completed: 13th April 2017

Name of responsible Director: pp

Date assessment was signed: 13th April 2017

NHS
Mersey Care
NHS Foundation Trust
Community and Mental Health Services

Action plan template

This part of the template is to help you develop your action plan. You might want to change the categories in the first column to reflect the actions needed for your policy.

Category	Actions	Target date	Person responsible and their area of responsibility
Transparency (including publication)	A copy of this equality and human rights analysis to be attached to the Policy on the Trust website.	April 2017	Sarah Barr
Confidentiality	The administration process needs to ensure the required data protection processes are understood and adhered to for the administration processes and the data held within the information systems.	April 2017	Sarah Barr