East London NHS
NHS Foundation Trust

Clinical & Non Clinical Systems Access Registration and deregistration procedure

Version number :	3
Consultation Groups	Digital Strategy Board System administrators
Approved by (Sponsor Group)	Digital Strategy Board
Ratified by:	
Date ratified:	
Name of originator/author:	Kate Lees Alison Naughton
Executive Director lead :	
Implementation Date :	
Last Review Date	January 2020
Next Review date:	January 2023

Services	Applicable
Trustwide	
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
1.0				
2.0				
3.0				

Contents

1. Introduction

This procedure provides guidance to System Administrators, staff and managers to assist in the management of system users for allowing legitimate and appropriate access to systems, based on the principle of 'need to know'. It ensures that the access rights remain appropriate over time and that users are de-registered when access is no longer required, or the user leaves the trust, or other associated organisations.

This procedure is designed to ensure that sensitive and confidential information that is held on electronic systems is protected from inappropriate, illegitimate or unauthorised access, modification or disclosure. Sensitive and confidential information includes patient information, personal information, commercial and corporate information.

Administrators and users should refer to systems operational manuals, and local system specific procedures for technical advice on how to register new users, allocate the agreed access and system roles and delete users.

This procedure applies to all electronic systems - both patient record systems and corporate systems. Legitimate access is the responsibility of all system administrators. System administrators should run regular reports to identify and manage system users.

It is the responsibility of all staff to pro-actively bring to the attention of the system administrator any suspected, potential or real incident of inappropriate or illegitimate access. Incidents should be reported using the Incident Reporting Procedure.

2. Relationship with other policies and procedures

This procedure ensures compliance with national requirements for Information Governance on access to systems.

This procedure is one of a number of procedures which support the Trust's Information Governance and IM&T Security Policy.

3. User Registration

It is the responsibility of users to

- Log a job on the IT Service desk Portal, requesting access to the relevant system.
- Each request must be properly authorised by the user's line manager.
- Each request must identify the work role of the user in order to inform the appropriate access to the electronic record/system.
- In case of doubt about the appropriate access or system role the system administrator must refer to the user's line manager.
- Never share passwords or smartcards.

It is the responsibility of system administrators to:

- Arrange the appropriate training or signpost the user to the training department.
- Set the user up on the system
- Inform the user of their login details
- Introduce - where technically possible – arrangements to ensure the system users change their password at first login.
- Ensure that Generic logins (e.g. 'temp staff' 'nurse') are never used.
- Ensure each user has only one user account on any one system.

4. User de-registration - temporary

Users may have their accounts temporarily disabled in the following circumstances:

- On the instruction of a Director or line manager e.g.
    - investigation of a security incident
    - following disciplinary action
    - long term absence
    - other exceptional circumstances

- After an agreed period of inactivity. The allowed period this may vary by system but will generally be between 1-3 months. Such deactivations will be notified to relevant line managers at least one week in advance of de-activation.

5. User de-registration - permanent.

Users should be de-registered in the following circumstances:

- On the instruction of a Director or line manager e.g.
    - following disciplinary action
    - on change of job role or team if this access is not required for the new Role/team
- If leaving the Trust (see para 6 below)
- Other exceptional circumstances
- Note that it may not be possible to delete the user from the system as they may be associated with medical history or event driven history. In this case the user account must be flagged as “disabled”.

6. De registration - staff leaving the Trust

System administrators may be informed of leavers from the following sources.

- The user
- The line manager
- **The HR leavers report.**
    - This report is sent to all line managers each month. It contains the name and team of the people leaving the Trust in the previous month.

7. Change of access rights.

A change of system access rights must be authorised by the user's line manager. Access rights may change under the following circumstances

- Change of job role
- Change of team
- Change of Directorate

8. Standards and timeframes

The Trust standard is to register new users within 1 working day of the authorised request being received. It is recognised that there may be resource constraints that may make this target difficult to achieve. The interim standard is to register new users within 3 working days of the authorised request being received.

Re-registration of users (e.g. after deregistration due to inactivity) will follow the same standards and require line or senior manager approval - as for a password reset.

Where possible, System managers will produce regular reports (monthly) on inactive system users for review and discussion with relevant line managers

9. Audit

System access is audited annually by the Caldicott Auditor using the Trust standard Caldicott Audit tool. Audit results are reported to the Information Governance Steering Group, together with a risk assessment and action plan.

10. Local system procedures

It is the responsibility of system administrators to ensure that local system specific procedures are in place. These are listed in Appendix 1.

11. Access to shared drives

Confidential and sensitive patient information is often stored on shared network drives. Access arrangements are through local managers.

Appendix 1 - List of Applications/Services at January 2020

Applications and Services	System Administrator Job title/contact details	Description
ELFT Network Access – • Trust email, calendar services • Active Directory groups and mappings • Access to shared drives • Office 365	ICT Infrastructure Manager via IT Servicedesk Portal	Person specific network drive – H Drive Shared network resources e.g. , I, K and S Drive access Areas for creating, sharing and storing information electronically
Trust Remote Access Services	ICT Server Manager Via IT Servicedesk Portal	Secure remote access to Trust network and applications
Registration Authority	Registration Authority Manager	Patient records - national spine

APPENDIX 1

Applications and Services	System Administrator Job title/contact details	Description
RiO	Clinical Systems Manager	Clinical System holding patient records
Legacy PAS	Clinical Systems Manager	Patient records accessed via an icon on the desktop
Data Warehouse	Data Warehouse Manager	Management information extracted from several varies Trust electronic systems- new sources to be added.
EMIS	Clinical Systems Manager via the IT Servicedesk Portal	Clinical system holding patient records – Community Health Newham Community Health Tower Hamlets Blood Borne Virus Team TH Homeless team
SystmOne	Clinical Systems Manager	Clinical system holding patient records – Community Health Bedfordshire
Carepath	Specialist Addiction Services	Clinical systems holding patient Records – Drug & Alcohol Services
IAPTuS	Systems Manager – Psychological Therapies	Psychological Therapy clinical system
Pathology, Radiology, Acute EPR - 8 Acute systems	IT Servicedesk via the IT Servicedesk Portal	Acute Trust clinical systems holding patient records – diagnostics/path results

Applications and Services	System Administrator Job title/contact details	Description
DATIX	Assurance Department	Clinical risk system
Electronic Staff record (ESR)	Recruitment Coordinator	Staff HR and payroll
Finance	Dion Campbell, Acting Financial Controller	Finance
Foundation Trust DB	Membership Manager	Trust membership
Training OLM	Head of Learning and development	Staff training