United Lincolnshire Hospitals NHS
NHS Trust

Standard Operating Procedure for the EDGE Clinical Research Management System

SOP Title	EDGE Clinical Research Management System
SOP No.	SOP 20
Authors	Helen Ayre
Consulted Departments	Lincolnshire Clinical Research Facility, Research and Development, ICT, NIHR CRN East Midlands
Lead Manager Sign and Print Name	Dr. Tanweer Ahmed Director of LCRF and Head of Research and Development and Trust IP Lead On File
Original date of publication	15/03/2016
Date current version published	15/03/2016
Review date of SOP	15/03/2017
Version	Final Version 1.0

1. Purpose:

The development and implementation of Standard Operating Procedures (SOPs) is a clinical and information governance requirement to inform staff of their responsibilities, in this instance when staff are using the EDGE Clinical Research Management System. This document also contains information on how to access the system, access training and the terms of use of the system.

A standard operating procedure: specifies in writing,

- What should be done,
- When
- Where
- By whom

The EDGE Clinical Research Management System ('EDGE') is available to support the care of patients participating in clinical research and to monitor and report on research activity within the Trust.

2. Applies to:

The policy applies to all staff involved in clinical research activity, specifically those required to utilise the EDGE system. Staff groups include:

Lincolnshire Clinical Research Facility Staff

Research & Development/Study Support Service Staff

Medical Staff supporting clinical research (Co-investigators / PI's etc.)

Nursing Staff supporting clinical research

Supporting Department Personnel (Including but not limited to Radiotherapy, Pharmacy, Pathology etc.)

The Information Asset Owner (IAO) for this system is the Director of Lincolnshire Clinical Research Facility / Head of R&D. If new staff groups are identified as requiring access to this system the IAO will be required to consider the request prior to access being granted.

3. Relevant SOP documentation:

SOP 1 – How to write an SOP
SOP 3 - Adverse Events/Adverse Reactions/Serious Adverse Reactions/ Serious Adverse Events and Suspected Unexpected Adverse Events
SOP 5 – Privacy and Data Protection
SOP 9 – Training Record
SOP 14 – Study Planning and Feasibility

4. Definitions:

BCP – Business Continuity Plan
CAUP – Computer Acceptable Use Policy
DOB – Date of Birth
GP – General Practitioner PID – Patient Identifiable Data
IAO – Information Asset Owner
ICT – Information, Communications and Technology
IP – Intellectual Property
PI – Principal Investigator
PID – Patient Identifiable Data
R & D – Research & Development
ULHT – United Lincolnshire Hospitals NHS Trust

5. Policy:

ULHT Small ICT systems Business Continuity Plan (BCP)
ULHT Electronic Patient Record Acceptable Use Policy
Intellectual Property Rights
Research Fraud and Misconduct
ULHT Health Records Policy

6. Procedure:

6.1 Terms of Use

These Standard Operating Procedures should be viewed in conjunction with the ULHT Electronic Patient Record Acceptable Use Policy and Small ICT Systems Business Continuity Plan.

In addition to all Trust policies relating to the processing of patient data (which can be viewed on the Information Governance area of the Trust intranet site) staff are also required to adhere to the following requirements listed below.

a) Staff with access to patient data within EDGE must only access data which they have a legitimate reason to do so for the purposes of supporting clinical research activity

b) Patient identifiable data must not be accessed outside of Trust premises. Staff accessing other functions within the EDGE Clinical Research Management System should do so only via Trust approved, encrypted devices and ensure that they 'lock' or log-out of terminals/devices immediately when not in use.

c) Staff accessing EDGE in areas within the Trust, or via media, where there is the possibility of patient data being viewed by unauthorised personnel (i.e. via tablets in clinics etc.) must ensure that the screen lock function is enabled immediately when the device is not in use.

d) Staff must not print any patient identifiable data from the system unless expressly permitted by the IAO. In all cases where PID is printed from the system, this must be appropriately marked as 'confidential'.

e) Confidentiality markings must also be used on all reports / documents printed from the system which contain staff or Trust sensitive information.

f) EDGE should not be used as a reference database for up-to-date patient contact details – any contact or demographic details should be referenced against the Medway system prior to use. As such only the minimum required patient identifiable data should be entered into EDGE. I.e. Study ID, NHS Number, Name, DOB, gender. (Address, telephone number, GP details are NOT required).

6.2 Access & Training

The EDGE Clinical Research Management System is managed by the ULHT Research & Development department. Staff requiring access to this system should contact a Trust Local Administrator (LCRF.EDGE@ULH.nhs.uk) rather than the ULH ICT service desk as indicated in the CAUP.

The EDGE system is a 'cloud-based' system accessible, using a username and password, from any device with an internet connection. Appropriate access rights have to be granted by designated Local Administrators to enable the individual to use the system. A role map is available (Appendix 1) outlining appropriate levels of access according to staff group. Line-managers are responsible for informing Local Administrators when staff require access granting or removing from the system

Individuals must ensure that they have received appropriate training and have read and understood applicable system policies and user guidance (http://edge.desk.com/) prior to accessing the system.

Passwords must comply with system and NHS requirements and be changed at least every 90 days.

Individuals must not share their username or password with other individuals or permit other users to access EDGE via their account. Any unauthorised use must be reported to a System Administrator to enable a password reset and system audit to identify any potential security breaches.

All activity on the system is auditable and regular planned and ad hoc audits will be conducted. ULHT is able to establish who has logged into the system and what information has been edited.

6.3 Contingencies – Business Continuity Plan

In the event of the EDGE Clinical Research Management system being unavailable staff should consult the ULHT Small ICT systems Business Continuity Plan (BCP) for guidance.

Significant access issues should be reported to the ICT Service Desk in the first instance and enquiries made regarding local issues which may be affecting access. If unresolved, the EDGE Network Administration team should be informed in the first instance. They will liaise with the EDGE central team as appropriate.

It is important to remember that if the system fails due to a Trust network error printers will not be available – paper copies of the BCP are therefore available – please consult the appropriate departmental manager regarding their location.

7. Responsibilities

Ultimately each user is responsible for ensuring they have received adequate training on the system and for ensuring they comply with this document; however it is also the line manager's responsibility to ensure that their staff are compliant and adequately trained.

8. References:

ULHT Small ICT systems Business Continuity Plan (BCP)
ULHT Electronic Patient Record Acceptable Use Policy

This SOP will be reviewed annually unless changes to legislation require otherwise
Current versions of all SOPs are located on the LCRF website and shared drive – users are responsible for ensuring that they are using the most up-to-date version.