This is a controlled document.
The master document is posted on the RGIT website and any print-off of this document will be classed as uncontrolled.

Researchers and their teams may print off this document for training and reference purposes but are responsible for regularly checking the RGIT website for more recent versions.

Computerised Systems for Clinical Trials

SOP Reference: RGIT_SOP_030	
Version Number: 9.0	
Effective Date: 29 Aug 2024	Review by: 29 Aug 2027
Author: Thomas Barbera, Clinical Trial Monitor	
Approved by: Keith Boland, Senior Clinical Trial Manager	Date: Keith Boland Digitally signed by Keith Boland Date: 2024.08.29 16:44:59 +01'00'

Version	Date	Reason for Change
Version 1.0	17 Jun 2007	
Version 2.0	24 Jun 2008	Annual Review
Version 3.0	08 Feb 2010	Formation of Joint Research Office
Version 4.0	14 Jul 2011	Annual Review
Version 5.0	03 Dec 2012	Annual Review
Version 6.0	18 Feb 2015	Scheduled Review
Version 7.0	25 Oct 2017	Scheduled Review Responsibility section added Reference to InForm forms and team are added
Version 8.0	19 Oct 2020	Scheduled Review Templates removed and administrative changes to SOP. JRCO name change to RGIT
Version 9.0	29 Aug 2024	Scheduled Review Out of date links and information updated within SOP.

TABLE OF CONTENTS

1. PURPOSE

This Standard Operating Procedure (SOP) will focus on computerised systems that Imperial College London or Imperial College Healthcare NHS Trust may utilise as Sponsor of a clinical trial and as such, it will not be an exhaustive list of all computerised systems used in clinical trials. Information and Communication Technology (ICT) at Imperial College maintain a database of all registered information systems connected to the College network. ICT at Imperial College Healthcare NHS Trust also maintain a database of all registered information systems connected to the Trust network.

2. INTRODUCTION

It is the responsibility of the Chief Investigator (CI) in the clinical trial to ensure that any computerised system used during the study complies with Trust and College policies as well as EU and UK directives (Guideline on computerised systems and electronic data in clinical trials (europa.eu) (Last Cited: 10Mar2023).

Any data that is stored on Imperial College London networked computers, laptops or Personal Digital Assistants (PDAs) must be stored in an anonymised form with no identifiable information. Users have a duty of care to protect the confidentiality of any information which they might access through the college network in the course of legitimate employment activities or through academic studies.

OpenClinica, a web-based electronic data capture system for clinical trials of investigational medicinal products (CTIMP), is now mandatory to be used for all CTIMPs sponsored by the College or Imperial College Healthcare NHS Trust. Details about the OpenClinica system, including information on who to contact regarding set-up, can be found at the following webpage OpenClinica | Faculty of Medicine | Imperial College London (Last Cited: 10Mar2023).

Patient identifiable data must be stored on NHS systems unless the patient has given explicit consent for it to be stored outside the NHS Trust. This will need to be highlighted in the ethics application. Any system holding identifiable data should be sufficiently secure and should be assessed by the departments Data Protection Officer and comply with the organisations data protection policy.

3. RESPONSIBILITIES

This SOP must be followed by the Chief Investigator (CI), OpenClinica development team and the CI delegated person.

It is the responsibility of the Head of Research Governance and Integrity Team to ensure that this SOP is updated by the review date or as necessary.

4. PROCEDURE

4.1. Evaluation and Purchasing

It is the CI's responsibility to ensure that any computerised systems that are used for clinical trial research are compliant with Imperial College London or Imperial College Healthcare NHS Trust ICT evaluation and purchasing policies.

Any Electronic devices used in the conduct of a clinical trial would be required to abide by the ICT evaluation and purchasing policies. These include but are not limited to:

- iPads (used to collate any data that is transferred to CRF's or Source notes)
- FitBits or Wristwatch heart-rate monitors (used to collect data from a patient)
- Medically related devices which collect information from the patient.

These devices require User Acceptance Testing and Computer System Validation prior to implementation. For further guidance, please contact the IT Service desk at the following link: Contact the ICT Service Desk | Administration and support services | Imperial College London (Last Cited: 30 Mar 2023).

4.2. Validation

The CI must ensure when using electronic trial data and/or remote electronic trial systems that the system conforms to the established requirements for completeness, accuracy, reliability and consistent intended performance (i.e., validation) (ICH GCP 5.5.3). The CI should base their approach to validation of such systems on a risk assessment that takes into consideration the intended use of the system and the potential of the system to affect human subject protection and reliability of trial results. This should be documented within the Data Management Plan (see RGIT_SOP_020 SOP, Associated Documents & Templates page (Last Cited: 30 Mar 2023)).

4.3. Implementation

If a study team wishes to use a new computerised system (as opposed to systems already approved), they must seek approval from the relevant Trust and their Caldicott Guardians (National Data Guardian – Principles 4 & 7 (Caldicott_Guardian_guidance_v1.0_27.08.21.pdf (publishing.service.gov.uk) (Last Cited: 10 May 2023)) as well as Imperial College to ensure that Trust and College policies, as well as EU and UK directives, are complied with.

ICT at Imperial College will be able to aid with implementation of the computerised system. The College also supplies a variety of software from the Software HUB Get software | Administration and support services | Imperial College London (Last Cited: 30Mar2023).

The CI must ensure that there are appropriate SOPs in place for the chosen computerised system as well as sufficient user training. The SOPs should cover system setup, installation and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning and decommissioning. The responsibilities of the sponsor, investigator and other parties with respect to the use of these computerized systems should be clear and the users should be provided with training in their use.

The CI must also ensure that the systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e. maintain an audit trail, data trail, edit trail).

4.4. Back-Up and Disaster Recovery Plans

The CI has the responsibility for the collection of data either remotely on a server or on a hard disk and should consult with the Departmental/Divisional ICT representative regarding the existence of local back-up systems (to guard against loss of data due to software and environment disasters) and disaster recovery procedures.

If the CI does not use the facilities provided by ICT, or those of the local Trust, the CI must put into place their own procedures. Please see Keep your files and data safe | Administration and support services | Imperial College London page (Last Cited: 30 Mar 2023) for further information.

The College's ICT department has a data backup service that provides a reliable means of protecting data held on departmental and research group file servers. ICT does not backup files on local desktop machines. Owners of such machines are responsible for protecting local files. For further information, please see the File sync, recovery and backup | Administration and support services | Imperial College London webpage (Last Cited: 10 Mar 2023) for further information.

For servers that are used to exclusively support research data, there is a charge for this backup service Virtual servers for research groups (Private Cloud) (Last Cited: 10 Mar 2023).

Where any data is stored on a database supported by a web application, please see the College Database Management Systems policy for further information on special Data Protection Act requirements for such systems: Information Systems Security Policies | Administration and support services | Imperial College London (Last Cited: 30 Mar 2023).

5. REFERENCES

RGIT_SOP_007 – CRF Design SOP, Associated Documents & Templates | Research and Innovation | Imperial College London (Last Cited: 10 Mar 2023)

RGIT_SOP_020 - Data Management SOP, Associated Documents & Templates | Research and Innovation | Imperial College London (Last Cited: 10 Mar 2023)

ICH GCP E6 R2 ICH: E 6 (R2): Guideline for good clinical practice - Step 5 (europa.eu) (Last Cited: 10 Mar 2023)

Contact the ICT Service Desk | Administration and support services | Imperial College London

Guideline on computerised systems and electronic data in clinical trials (europa.eu) (Last Cited: 10Mar2023)

Caldicott_Guardian_guidance_v1.0_27.08.21.pdf (publishing.service.gov.uk) (Last Cited: 10May2023)

OpenClinica | Faculty of Medicine | Imperial College London (Last Cited: 10 Mar 2023)

Information Systems Security Policies | Administration and support services | Imperial College London (Last Cited: 10 Mar 2023)

File sync, recovery and backup | Administration and support services | Imperial College London (Last Cited: 10 Mar 2023)

Keep your files and data safe | Administration and support services | Imperial College London (Last Cited: 30 Mar 2023)

Information and Communication Technologies - Get Software (Last Cited: 10 Mar 2023)

Virtual servers for research groups (Private Cloud) (Last Cited: 10 Mar 2023)