Computerised Systems for Clinical Trials

SOP Reference: RGIT_SOP_030	
Version Number: 8.0	
Effective Date: 19 Oct 2020	Review by: 19 Oct 2023
Author: Sarangan Ragulan, Clinical Trial Monitor	
Approved by: Ruth Nicholson, Head of Research Governance and Integrity	Date: Ruth Nicholson Digitally signed by Ruth Nicholson Date: 2020.10.14 10:18:19 +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

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, 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.

Any data that is stored on Imperial College London networked computers, laptops or Personal Digital Assistants (PDAs) must be stored in an pseudonymised 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.

InForm, a web-based electronic data capture system for clinical trials of an investigational medicinal product (CTIMP) was introduced into the College in late 2008 and is now mandatory for all CTIMPS sponsored by the College or Imperial College Healthcare NHS Trust. Details about the InForm system can be found at the Inform Clinical Trials Unit page.

Patient identifiable data must be stored on NHS systems unless the patient has given explicit consent for it to be stored outside their NHS Trust. This will also 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 Investigators (CI), InForm 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.

The Chief Investigator and delegated person should refer to InForm SOP IN021 via the Quality Assurance SOP site (Cited 10 Jul 2020).

The Chief Investigator should complete the INA021-AF. These forms can be obtained by emailing the InForm team at inform_estimates@imperial.ac.uk. The CI can delegate this task to one of the team members.

4.2. Validation

The CI must ensure when using electronic trial data and/or remote electronic trial systems that the system conforms to established requirements for completeness, accuracy, reliability and consistent intended performance (i.e. validation) (ICH GCP 5.5.3). This should be documented (see RGIT_SOP_020 this SOP which can be found on the SOP, Associated Documents & Templates page).

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 (Information System Security Policy – Code of Practice 4 and Policy 7) 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 facilitates the purchase of new PCs and renewal of old ones and supplies a variety of software for staff and students, available for download or purchase from the Software Shop.

The CI must also ensure that there are appropriate SOPs for the chosen computerised system.

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. See the Imperial College Sensitive Info page (Cited 10 Jul 2020). for further information.

The College ICT service has a data backup service that provides a reliable means of protecting data held on departmental and research groups file servers. ICT does not backup files on local desktop machines. Owners of such machines are responsible for protecting local files. See the Imperial college File recovery and backup page (Cited 10 Jul 2020). 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) (Cited 10 Jul 2020).

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: Supported databases for web applications (Cited 10 Jul 2020).

5. REFERENCES

RGIT_SOP_007 – CRF Design
RGIT_SOP_020 Data Management
ICH GCP E6 R2

Information Systems Security Policy - Guideline 2: Backing-Up Data
Information Systems Security Policy - Code of Practice 10: Security of Laptops and the Data Stored Therein
Information Systems Security Policy - Guideline 12: Guidance for Information Security Liaison Officers Completing the Annual Information Security Assessment
Information Systems Security Policy - Codes of Practice
Information Governance Policy Framework (Cited 10 Jul 2020)

Information Security Policy (Cited 10 Jul 2020)

Information Security Codes of Practice (Cited 10 Jul 2020)

Information and Communication Technologies - Get Software

Clinical Trials Unit - Quality Assurance SOPs (Cited 14 Jul 2020)