Computerised Systems for Clinical Trials

SOP Reference: JRCO/SOP/030

Version Number: 6.0

Effective Date: 18/02/15

Review by: 18/02/17

Author: Christopher Ente, Research Facilitator

Approved by: Gary Roper

Date: 18/02/15

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final 1.0</td>
<td>17.06.2007</td>
<td></td>
</tr>
<tr>
<td>Final 2.0</td>
<td>24.06.2008</td>
<td>Annual Review</td>
</tr>
<tr>
<td>Final 3.0</td>
<td>08/02/2010</td>
<td>Formation of Joint Research Office</td>
</tr>
<tr>
<td>Final 4.0</td>
<td>14/07/11</td>
<td>Annual Review</td>
</tr>
<tr>
<td>Final 5.0</td>
<td>03/12/12</td>
<td>Annual Review</td>
</tr>
<tr>
<td>Final 6.0</td>
<td>18 Feb 2015</td>
<td>Scheduled Review</td>
</tr>
</tbody>
</table>
**Table of Contents**

1. **Purpose**  
   Page 3

2. **Introduction**  
   Page 3

3. **Procedure**  
   Page 3
   - 3.1 Evaluation and Purchasing  
     Page 3
   - 3.2 Validation  
     Page 3
   - 3.3. Implementation  
     Page 3
   - 3.4 Back-Up and Disaster Recovery Plans  
     Page 4

4. **References**  
   Page 4
1. PURPOSE

This Standard Operating Procedure (SOP) will focus on computerised systems that 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 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.

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: http://www.imperial.ac.uk/clinicaltrialsunit/contact/

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. PROCEDURE

3.1 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.

3.2 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 JRCO/SOP/020).

3.3 Implementation
Any study that wishes to use new computerised systems (as opposed to systems already approved) must seek the approval from the relevant Trust and their Caldicott Guardians (Information System Security Policy – Code of Practice 10 and Policy 12) 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 (http://www3.imperial.ac.uk/ict/services/softwarehardware)

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

3.4 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 http://www.imperial.ac.uk/ict/services/security/helpandadvice/sensitivedata/copsendata 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 http://www.imperial.ac.uk/ict/services/computerroom/file_and_backup_services/ for further information. For servers that are used to exclusively support research data there is a charge for this backup service http://www.imperial.ac.uk/ict/services/computerroom/file_and_backup_services/bakcup_of_departmental_research_servers/. 

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: http://www.imperial.ac.uk/webguide/technologyservices/databases
4. REFERENCES

JRCO/SOP/020
ICH GCP 1996

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 - Codes of Practice

http://www.imperial.ac.uk/secretariat/collegegovernance/provisions/policies/infosystems/guidelines/copguide2
http://www.imperial.ac.uk/secretariat/collegegovernance/provisions/policies/infosystems/codes/isscop10
http://www.imperial.ac.uk/secretariat/collegegovernance/provisions/policies/infosystems/guidelines/copguide12
http://www.imperial.ac.uk/secretariat/collegegovernance/provisions/policies/infosystems/codes

http://www.imperial.ac.uk/webguide/technologyservices/databases
http://www.imperial.ac.uk/ict/services/softwarehardware