MANCHESTER
1824

The University
of Manchester

Standard Operating Procedure

Number:	UoM/Computer Systems/SOP16/4.0		
Title:	Computerised Systems for Clinical Trials - Site Set Up and Initiation		
Version:	2.0 (August 2016)	**Effective Date**	August 2016
Author:	Lee Moffatt	**Review Date**	August 2018
Reviewed by : Prof Deborah Symmons		**Approved By:** Prof Nalin Thakker	
Position: Chair of Clinical Trials Management Group		**Position:** Associate Vice President for Research Integrity	
Signature: DSymmons		**Signature:** Nalin Thakker	

Version	Date	Reason for change
2.0	**January 2013**	**Update of weblinks and office details**
3.0	**October 2015**	**Update of weblinks and office details**
4.0	**August 2016**	**Update of weblinks and office details**

When using this document please ensure that the version you are using is the most up to date either by checking on the Research Governance and Integrity Team website (http://www.staffnet.manchester.ac.uk/services/rbess/governance/) for any new versions or contacting the author to confirm the current version.

1.0 Background

In order to be compliant with the European Directive on Good Clinical Practice in Clinical Trials (2001/20/EC) organisations conducting Clinical Trials of Investigational Medicinal Products must have clearly documented Standard Operating Procedures covering all aspects of conducting Clinical Trials. The SOPs also apply to all other projects that fall under the Research Governance Framework for Health and Social Care, 2nd Edition, Department of Health 2005.

A Standard Operating Procedure (SOP) is defined by ICH Harmonised Tripartite Guideline for Good Clinical Practice as "Detailed, written instructions to achieve uniformity of the performance of a specific function". These SOPs are written instructions and records of procedures agreed and adopted by the University of Manchester.

2.0 Purpose

This Standard Operating Procedure (SOP) describes the process of setting up computerised systems to assist with the capture and processing of data relating to Clinical Trials of Investigational Medicinal Products (CTIMP)

This SOP is underpinned by the University of Manchester's IT Security Policies (see the reference section for links), based on Universities and Colleges Information Systems Association (UCISA) best practice, which, in turn, draws heavily on the standards BS7799 and ISO 27001.

3.0 Roles and responsibilities

3.1 Procedures

When designing a Clinical Trial it is important to consider how trial-related data will be collected, stored and processed for the duration of the trial. This is likely to include the design of any computerised systems that will be required to assist with the management of trial data. Paramount in the design will be the security of the data management system and the data itself (see also the SOP for Data Management and SOP on IT Security and Encryption).

The IT Security Checklist (Appendix 1) should be completed initially and returned to Lee.Moffat@manchester.ac.uk (IT Security) for review to ensure that some fundamental aspects of data management and IT Security are being considered. Any areas of concern will be followed up by IT Security. Examples of areas which should be addressed are:

- data processing
- data transmission
- computer and data security
- physical security
- data archiving
- IT and information security awareness, procedures and training

IT Security (Lee.Moffat@manchester.ac.uk) will review the completed checklist and dependent on responses, will arrange a site visit if required to audit existing IT systems and working processes and provide guidance around best practice in data handling, IT and information security best practices. IT Services staff will also work with trial staff to implement and support trial related computer systems. Visit arrangements can be made via the University's IT Service Desk (see the contact list section for details).

4.0 Related Procedures and references

SOP for Data Management

SOP for IT Security and Encryption

SOP for Developing and Implementing a System Level Security Policy

UoM Cyber Security website:
http://www.itservices.manchester.ac.uk/cybersecurity/

UoM Information Security Policy (last updated May 2016)

http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525

UoM Information Security Responsibilities (last updated November 2014)
http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=8039

UoM Data Protection website

http://www.dataprotection.manchester.ac.uk/

Contact list

The University's IT Service Desk
t: 0161 306 5544
#
w: http://www.itservices.manchester.ac.uk/help/

Research Governance and Integrity Team
http://www.staffnet.manchester.ac.uk/services/rbess/governance/

Appendix 1

The University of Manchester
IT and Information Security Checklist for Clinical Trials

Throughout this document the use of the term 'data' means 'clinical trial data or other sensitive data stored or processed in an electronic format'.

1. Background Information

Title of the Trial	
Chief or Principal Investigator	
Data Custodian	

Primary site / building	
Other sites / buildings	
Do you maintain an inventory of IT equipment? If so, please provide brief details.	
Is your IT equipment connected to the University's network?	
Who provides support with respect to IT equipment used within the Trial?	
Do you maintain documented standard operating procedures (SOPs) with respect to 'IT and Information Security' and 'data handling' within the Trial Master File?	

This document/SOP is a controlled document.
Any printed version of this document may not be current. It is the responsibility of colleagues to ensure that the most recent version of the document is accessed and the procedures stated within the document followed.

To access the most up-to-date version of this document please visit the University of Manchester Research Governance website:
http://www.staffnet.manchester.ac.uk/services/rbess/governance/

2. Data Processing

Where do staff store, process and backup data?

Have you considered the security implications of storing, processing and backing up data in these locations?

	store	process	backup	security considered - comments
Shared network storage				
Personal network storage (p-drive)				
Email inbox/folders				
External hard drive				
Local drive (pc/laptop)				
USB pen drive				
Optical media (CD/DVD)				
Non-University provided equipment (pc/laptop, external drive)				
Non-University provided storage (personal email account)				
Non-University provided storage (cloud-based, eg MS Sky-Drive)				
Mobile devices (eg Blackberrys, iPhones, other PDAs				
Other (please specify)				

This document/SOP is a controlled document.
Any printed version of this document may not be current. It is the responsibility of colleagues to ensure that the most recent version of the document is accessed and the procedures stated within the document followed.

To access the most up-to-date version of this document please visit the University of Manchester Research Governance website:
http://www.staffnet.manchester.ac.uk/services/rbess/governance/

3. Data Transmission

Do staff send (/receive) data to (/from) colleagues or 3rd parties by the following means? Have you considered the security implications of sending/receiving by these means?

	send	receive	security considered - comments
University email system			
Other university email system			
NHS email system			
Other email system (eg Googlemail, Hotmail)			
Secure File Transfer over the Internet			
Postal/Courier service to send/receive USB/CD/DVD media			
Other (please specify)			

4. Computer and Data Security

Do you employ the following IT security measures to protect against equipment/data loss or theft?

	yes	no / don't know	comments
Antivirus: do you have antivirus software installed and enabled on all computers and laptops? Is it configured to receive updates on a frequent and regular basis?			
Automatic updates/patches: are your computers and laptops (and installed software applications) configured to automatically download and install patches, updates and security fixes, as and when they become available (eg from Microsoft, Apple and other software application vendors)?			
Firewall: do you have a software firewall installed, active and properly configured on all computers and laptops?			
Block remote access: are your computers and laptops accessible via 'Remote Desktop' from outside the University's network?			
Encryption: do you have disk/file level encryption tools installed on your computers, laptops, external drives and other removable media and do you use them? Note: please specify the encryption tools you use in the comments section.			
Passwords: are all your accounts protected by strong, secure passwords that are not written down or shared with others?			
Data backup: do you have a data backup policy and a standard operating procedure (SOP)?			
Data restore: do you regularly test that data backups can be restored? Is restored data tested for integrity?			
Other (please specify)			

5. Physical Security

Do you employ the following physical security measures to protect against the loss or theft of IT equipment and data?

	yes	no / don’t know	comments
Is your IT equipment located in areas that are not easily accessed by visitors and other non-authorised staff?			
Is your IT equipment kept behind doors that have adequate locks? Are doors/windows locked at lunchtimes, evenings and other times when staff are absent?			
Are your computers, especially laptops, protected by anti-theft devices (eg security cables)?			
Are laptops locked away at night? Do you use specially-designed laptop safes?			
Are monitors/screens positioned so that data cannot be viewed casually by visitors or other non-authorised staff?			
Do you have a ‘clear-desk’ policy to ensure the security of sensitive and confidential files when you are not working on them?			
Are desktops and laptops protected by a password-based screen saver?			
Other (please specify)			

6. Data Archiving

Have you considered the following issues with respect to the long term storage and archiving of data?

	yes	no / don’t know	comments
Do you have an archiving/retention policy and a suitable archiving solution for the long term storage of (and access to) data?			
Does your archiving solution ensure long term access to data stored on ‘intermediate storage media’ (eg tape, floppy disks, CDs/DVDs etc)?			
Does your archiving solution ensure data will be ‘locked down’ once the trial is formally closed?			
Will someone (the ‘archivist’), who is independent of the Trial, be responsible for the archive and will that person have appropriate control over the data?			
Other (please specify)			

This document/SOP is a controlled document.
Any printed version of this document may not be current. It is the responsibility of colleagues to ensure that the most recent version of the document is accessed and the procedures stated within the document followed.

To access the most up-to-date version of this document please visit the University of Manchester Research Governance website:
http://www.staffnet.manchester.ac.uk/services/rbess/governance/

7. IT and Information Security Awareness, Procedures and Training

The primary goal of a security awareness and training programme is to reduce security vulnerabilities and promotion good security practices.

	yes	no / don’t know	comments
Are you familiar with the University’s IT Security Policies and Guidance at: www.its.manchester.ac.uk/secure-it/			
Do you fully understand your responsibility for IT and Information Security?			
Do you have standard operating procedures (SOPs) in respect of IT and Information Security and are they reviewed regularly?			
Do staff engaged on the trial understand their responsibilities with respect to IT and Information Security?			
Do staff know how to report an IT or Information Security incident or breach?			
Other (please specify)			

This document/SOP is a controlled document.
Any printed version of this document may not be current. It is the responsibility of colleagues to ensure that the most recent version of the document is accessed and the procedures stated within the document followed.

To access the most up-to-date version of this document please visit the University of Manchester Research Governance website:
http://www.staffnet.manchester.ac.uk/services/rbess/governance/