
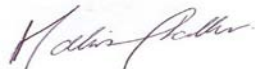


Standard Operating Procedure

Number:	UoM/IT Security and Encryption/SOP18/4.0		
Title:	IT Security and Encryption		
Version:	4.0 (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: 		Signature: 	

Version	Date	Reason for change
2.0	January 2013	Update of weblinks and office details
2.1	May 2014	Addition of version control statement for SOP
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.

UoM/IT Security and Encryption/SOP18/4.0

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.

Page 1 of 4
Version No: 4.0
August 2016

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/>

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 encrypting sensitive data, relating to Clinical Trials of Investigational Medicinal Products (CTIMP), which is stored on removable media and local hard drives. This SOP also covers the secure transfer of sensitive data to authorised 3rd parties.

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

This SOP applies to all sensitive data relating to Trials which come under the CTIMP Regulations, where the University of Manchester is the Sponsor. The requirements of this SOP should be applied as a minimum to such trials and in conjunction with all applicable University policies and procedures and the policies and procedures of the relevant NHS Trust.

3.0 Procedure

As a general rule, all sensitive or confidential information or data should always be stored or transmitted in an encrypted form. Any sensitive data stored on the internal hard drives of desktop or laptop computers, removable media (including but not limited to CD/DVD, USB memory sticks, external hard drives) or data that requires transmission to an authorised 3rd party should be encrypted to compliant encryption standards using University prescribed software.

It is important that unencrypted versions of the data exist, should encryption passwords/passphrases be lost or forgotten. For this reason secure University network storage is the recommended location for storing unencrypted copies of sensitive data.

User guides and video walkthroughs for fully or partially encrypting USB memory sticks, external hard drives and the creation of encrypted containers on local hard drives are available on the University Cyber Security website (see the references section for links).

UoM/IT Security and Encryption/SOP18/4.0

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.

Page 2 of 4
Version No: 4.0
August 2016

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/>

Full system encryption is performed by default on all new laptops by IT Services staff as part of the setup and installation process, before delivery to the end user. Full system encryption of existing desktop and laptop computers is strongly recommended when sensitive data is stored locally and can be requested via the University's IT Service Desk (see the contact list section for details).

It is recommended that desktops and laptops are secured with anti-theft devices to provide additional physical IT Security.

The University recommends that sensitive data is **NOT** transferred by email. Where this is unavoidable the data must be anonymised, with the key index sent separately. If sensitive data must be sent via email then the sensitive data should be encrypted using University prescribed encryption software prior to sending to an authorised party. A strong, complex passphrase should be used to encrypt the data and this passphrase should only be relayed to the recipient via an alternative method of communication, such as telephone or text message, once the identity of the recipient has been confirmed.

Note: NHS information security guidelines state that a minimum of 256bit AES encryption must be used to encrypt sensitive data. When collaborating with authorised staff on Trust IT systems it is recommended that the Trust provide guidance on the encryption software that should be used to satisfy their security requirements. Advice can be obtained via the University's IT Service Desk.

4.0 Related Procedures and references

UoM Cyber Security website:

<http://www.itservices.manchester.ac.uk/cybersecurity/>

Encryption User Guidance

<http://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/>

UoM Information Security Policies (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>

3rd Party Encryption Requirements

<http://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/partners/>

UoM Data Protection website

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

Contact list

UoM/IT Security and Encryption/SOP18/4.0

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/>

Page 3 of 4
Version No: 4.0
August 2016

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/>

UoM/IT Security and Encryption/SOP18/4.0

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/>

Page 4 of 4
Version No: 4.0
August 2016