


Standard Operating Procedure (SOP) Computerised Systems

SOP ID Number:	JRESGOVSOP0024	Effective Date:	04/11/2021
Version Number and Date:	Version 3.0 22/04/2021	Review Date:	04/11/2023
Author:	Georgia Bullock	Title:	Research Development and Governance Manager
Approved by:	Subhir Bedi	Date:	27/09/2021
Signature of Authoriser			

This is a controlled document.

The master document is posted on the JRES website and any print-off will be classed as uncontrolled.

Researchers and their teams are responsible for checking the JRES website for the most recent version.
They may print off this document for training and reference purposes.

SOP Chronology		
SOP Version Number:	Reason for Change:	Author:
Draft v1.0	New SOP	Lucy H H Parker
V2.0	Updated trust name; trust logo; newly added information	Mallikarjuna Rao Vemula (Arjun)
V3.0	Updated links to relevant websites. Addition of Associated JRES documents table. Minor amendments to text in all sections including amending JREO to JRES.	Georgia Bullock

Associated JRES documents

SOPs	WPDs	Docs	LOGs
JRESGOVSOP0038 Data Management	JRESWPD0023 General Research Definitions		

Contents

1. Background	2
2. Joint Research and Enterprise Services (JRES) Policy.....	3
3. Scope	3
4. Definitions	3
5. Responsibilities	3
6. Procedure	4
7. References	5
8. Appendices.....	5

1. Background

It is the responsibility of the Chief Investigator (CI) of the clinical trial to ensure that any computerised system used during the study complies with both St George's University and St George's NHS Foundation Trust policies as well as any applicable UK regulations.

Any data that is stored on SGUL networked computers, laptops, tablets, iCloud, smart watches, smart phones 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 university network in the course of legitimate employment activities or through academic studies.

Patient identifiable data must be stored on NHS systems unless the patient has given explicit consent for it to be stored outside of the NHS Trust. This will also need to be highlighted in the ethics application and applicable supporting documentation. Any system holding identifiable data should be sufficiently secure and comply with the University/Trust's Data Protection policies. In a clinical trial, CIs or PIs wishing to access patient data without consent must obtain permission from the Confidentiality Advisory Group (CAG).

<https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/confidentiality-advisory-group/>

2. Joint Research and Enterprise Services (JRES) Policy

All JRES SOPs will be produced and approved in accordance with the JRES SOP on SOPs and must be used in conjunction with local NHS Trust and University policies and procedures.

The JRES acts as the representative of both St George's University of London (SGUL) and St George's University Hospitals NHS Foundation Trust (SGHT). St George's will be the official name used on all SOPs to represent either institution acting as Sponsor.

3. Scope

This Standard Operating Procedure (SOP) focuses on computerised systems that St George's University Hospitals NHS Foundation Trust (SGHT) or St George's, University of London (SGUL) may utilise as the Sponsor of clinical trials and as such, is not a list of all computerised systems used in clinical trials.

Information and Communication Technology (ICT) at SGUL maintains a database of all registered information systems connected to the University network. ICT at SGHT also maintains a database of all registered information systems connected to the Trust network.

4. Definitions

For general research-related acronyms used in this SOP, refer to General Research Definitions Working Practice Document (JRESWPD0023).

Caldicott Guardian: a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly (GOV.UK). All NHS Trusts must have a Caldicott Guardian.

<https://www.gov.uk/government/groups/uk-caldicott-guardian-council>

The Guardian plays a key role in ensuring that the NHS, satisfies the highest practicable standards for handling patient-identifiable information.

5. Responsibilities

This SOP is to be followed by the Chief Investigator (CI) of all studies sponsored or hosted by St George's.

6. Procedure

Evaluation and Purchasing:

It is the CI's responsibility to ensure that any computerised systems that are used for clinical research are compliant with SGUL or SGHT ICT policies. If in doubt, the CI should contact the relevant ICT department for advice and guidance.

Validation:

The CI must ensure when using electronic systems to capture trial data that the system conforms to established requirements for 'completeness, accuracy, reliability and consistent intended performance (ie: validation). Systems used for data capture for CTIMPs must be validated or cannot be used for these trials. Evidence of computer system validation must be clearly documented. Please refer to JRESGOVSOP0038 Data Management for further guidance.

Implementation:

Any CI who wishes to use new computerised systems (as opposed to systems already approved) must seek the approval from the relevant Trust and their Caldicott Guardians as well as SGUL to ensure compliance with both Trust and University policies, in addition to applicable to UK regulations.

ICT at SGUL may be able to aid with implementation of the computerised system if the software is supported for use on Windows.

<https://www.sgul.ac.uk/about/our-professional-services/information-services/it-services>

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

Disaster Recovery/Back-up Plans:

The CI has the responsibility for the collection of data either remotely on a server or on a hard disk and should consult ICT 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 at the local Trust, he/she must put into place his/her own procedures.

7. References

ICH GCP.

Data Protection legislation:

<https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/>

8. Appendices

None associated with this SOP.