STU-SOP-TM-006 – Standard Operating Procedure on Data Protection and Confidentiality in Research Projects

Version No:	5	**Effective Date:**	17-Apr-2026
Description of changes:	SOP reviewed in light of clinical trial regulations 2025 and GCP updates. Removal of STU Unit Manager title. Specific references to QPulse as the QMS have been removed. We now only refer to a QMS system.		

List of Abbreviations	
CI	Chief Investigator
CRF	Case Report Form
DC	Data Controller
DP	Data Processor
DPA	Data Protection Act
DPO	Data Protection Officer
DSA	Data Sharing Agreement
DSP	Data Sharing Plan
FoI Act	Freedom of Information Act (2000)
GCP	Good Clinical Practice
GDPR	General Data Protection Regulation
ICF	Informed Consent Form
ICO	Information Compliance Officer
ISF	Investigator Site File
PI	Principal Investigator
RGF	Research Governance Framework
SOP	Standard Operating Procedure
STU	Swansea Trials Unit
SU	Swansea University
TM	Trial Manager
TMF	Trial Master File

1. Purpose and Definitions

This Standard Operating Procedure (SOP) describes the procedure of managing identifiable personal data for research projects adopted by Swansea Trials Unit (STU). This SOP is in alignment with Swansea University's Data Protection Policy, the UK Policy Framework for Health and Social Care Research and the principles of Good Clinical Practice (GCP).

All researchers involved in clinical trials and non-interventional studies must ensure that they are aware of their legal duties in relation to data protection and confidentiality.

Following this SOP will ensure that identifiable information collected as part of any research project is recorded, handled and stored in a way that meets the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 and allows staff to comply with the Freedom of Information Act (FoI) 2000 act.

Definitions	
Confidentiality	Prevention of disclosure to other than authorised individuals of a sponsor's proprietary information or of a participant's identity or their confidential information.
Data Controller	An organisation or person who (alone or in common with others) determines the purposes and means for any personal data to be processed. They act on their own autonomy.
Data Processer	Any organisation or person who processes personal data under the instruction of the data controller.
Data Protection Officer (DPO)	Sometimes called the Information Compliance Officer, is responsible for ensuring employees of an organisation are aware of, trained on and comply with the UK GDPR.

2. Background

GDPR (see references) applies only to identifiable personal data and is based on eight principles (see below). It is an offence under GDPR to process data that is irrelevant or excessive for the purpose for which it was collected.

Participant rights:

1. **Right to be informed:** Clear, transparent information about data usage.
2. **Right of access:** Requesting a copy of personal data.
3. **Right to rectification:** Fixing incorrect information.
4. **Right to erasure:** Requesting deletion of data.
5. **Right to restrict processing:** Limiting how data is used.
6. **Right to data portability:** Receiving data in a usable format.
7. **Right to object:** Objecting to data usage, particularly for marketing.
8. **Rights related to automated decision-making/profiling**.

The DPA 2018 (see references) supplements the GDPR by completing sections of the GDPR regulation left for individual countries to interpret and implement. The DPA applies a broadly similar regime of data protection and enacts the GDPR requirements in UK law, to be known as UK GDPR. Referenced throughout this document as GDPR.

The FoI Act (see references) enables public access to all types of recorded information held by a public authority, which potentially includes confidential information. In accordance with the FoI Act, Universities and NHS organisations are defined as public authorities.

3. Roles and Responsibilities

The **Sponsor(s)** acts as a Data Controller and is responsible for the protection of research participants' identifiable data. The sponsor and employer of the Chief Investigator of a research project may all act as Data Controllers. They are responsible for finalising any Data Sharing Agreement (DSA).

Swansea Trials Unit (STU) are responsible for ensuring that all staff are aware of their responsibilities under GDPR and that any third parties contracted have appropriate systems in place to process data for research (Data Processors).

The **Chief Investigator** (CI) is a delegate of the Sponsor and is responsible for providing details of the collection, processing, storage and eventual sharing of personal information, ensuring compliance with GDPR and generating a project Data Sharing Plan (DSP).

The **Principal Investigator** (PI) at each research site is a Data Processor and responsible for making sure that all staff are suitably trained in accordance with local site requirements.

The **Trial Manager** (TM) as delegated shall oversee that the provisions of GDPR are met for research projects.

External use of SOP: This SOP and Associated Documents (AD) may be used for research projects not adopted by STU where Swansea University (SU) staff and associated NHS organisations require guidance. In such instances, oversight responsibility for any associated tasks will not be the responsibility of STU.

4. Procedure

The overall process is to ensure that access to identifiable personal data are restricted to those personnel who are authorised to see it. Documents holding identifiable information include consent forms, original interview data (prior to redaction), and some source data e.g. x-rays. Wherever possible, identifiable data should not be held at STU unless consent has been obtained for this.

4.1 Research Data Collection and Processing

Data protection in relation to data collection must be considered during protocol development. Only data that is absolutely necessary and required by the approved research project protocol should be collected and the requirement for directly identifiable data versus pseudo anonymised data should be justified. The protocol should describe how data will be handled and include information about the data to be collected and the method(s) of collection and who will have access to the data. The protocol should also detail arrangements to be made for data sharing following conclusion of the trial.

4.1.1 Data collection

When data are **pseudo anonymised**, one master list with the identifier/codes and the participants' details will be kept separately from research data in order to link the participants' research data and medical health records. For multicentre studies, there may be several lists, one kept at each site to identify that site's participants. Such lists should be kept in locked cabinets separate from the Investigator Site File (ISF) in a secure environment or in an electronic format as password-protected files saved on a secure network. Multiple copies should not be made of the master list. It is not always possible to anonymise data (e.g. consent forms, qualitative research) but the collection, storage and access to such data must be adequate and justified.

4.1.2 Data processing

Researchers must comply with the DPA principles as appropriate for their research. If data collected for research purposes is **anonymised** it does not fall under the scope of the DPA.

4.2 Storage of Research Data

Where necessary, advice on suitable methods of storage should be sought from the University and relevant Sponsor DPO.

4.2.1 Paper-based data

All site data received in an identifiable form must be stored securely and separately from the project data and Case Report Forms (CRFs). Essential identifiable project documents can be kept as a separate part of the Trial Master File (TMF) and ISF until the point of destruction. The TM should write a file note to indicate the location of the identifiable data within the TMF and details of people who have access.

4.2.2 Electronic data

Files containing identifiable electronic data, including electronic data capture systems and electronic CRFs, must have restricted access or be password-protected and stored on a secure network. There may be instances where a secure portable device is used for short periods e.g. qualitative interview recordings prior to transferring to a secure server. Identifiable electronic data should be stored separately from the main ISF or TMF with their location and access details recorded in the ISF or TMF.

4.3 Transfer/Sharing of Research Data

Data requests for transfers or sharing to an external party(ies) must follow STU-SOP-DMS-012. A signed Data Sharing Agreement or Data Access Agreement (DAA) as appropriate must be held in the TMF.

4.4 Archiving and Destruction

Source documents, trial-related electronic and other data must be stored safely and in accordance with the requirements of STU-SOP-TC-001 Archiving.

At the end of the study, hard copy identifiable data must be disposed of in a confidential waste bag or shredded. Identifiable electronic data will be held securely for the minimum time possible. The research contract and local policy on data destruction should be followed and advice sought from the CI or relevant DPO where necessary.

4.5 Confidentiality

Research team staff have a duty of confidentiality in relation to identifiable personal data. For a STU adopted research project any breaches of confidentiality by research team staff or STU personnel must be immediately notified to stu@swansea.ac.uk. Research site staff will notify the CI and TM who will inform research sponsors and local site staff as appropriate. All relevant DPOs must also be informed by the relevant email.

4.6 Freedom of information

Under the FoI Act, members of the public can request access to any recorded information held by a public authority e.g. a University or an NHS Health Board or Trust. Any request for information must be handled in accordance with the public authorities policy(ies) and forwarded to their DPO or equivalent for information on how to respond.

4.7 Deceased participants

Although GDPR relates only to living individuals, any research project data relating to deceased participants should be held, archived and destroyed in accordance with GDPR and this SOP.

5. References

- UK policy framework for health and social care research (2017) - https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/uk-policy-framework-health-social-care-research/
- UK Medicine for Human Use (Clinical Trials) Regulations 2025 -

https://www.legislation.gov.uk/uksi/2025/538/contents

- Swansea University data protection policy https://www.swansea.ac.uk/about-us/compliance/data-protection/
- Caldicott review: information governance in the health and care system https://www.gov.uk/government/publications/the-information-governance-review
- General Data Protection Regulation https://gdpr.eu/
- Data Protection Act 2018 - http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Freedom of Information Act 2000 - http://www.legislation.gov.uk/ukpga/2000/36

It is assumed that by referencing the principal regulations that all subsequent amendments are included in this citation.

6. Associated Documents

Number	Title	Location
N/A	N/A	N/A