SOP Number **013**

SOP Title **Confidentiality and Security of Personal Data**

	Name	Title	Signature	Date
Author on behalf of the QA Focus Group	Clare Riddle	Senior QA and Compliance Manager, Clinical Trials and Research Governance		06 SEPT 2019
Reviewer on behalf of the QA Focus Group	Elaine Chick	Deputy Head of Clinical Trials and Research Governance		19.9.19.
Authoriser	Heather House	Head of Clinical Research Support (University Lead of the Joint Research Office)		19/09/2019

Agreed by QA Focus Group	25 July 2019
Effective Date	25 Nov 2019
Review Date	24 Nov 2022

1. PURPOSE

This SOP describes the standard procedures to be followed to ensure personal data collected in the course of clinical research conducted by the University of Oxford is handled and maintained in such a way as to satisfy the legal requirements and guidelines relating to the protection of research participant confidentiality including what to do in the event of a personal data breach.

2. INTRODUCTION

The processing of personal data for research purposes is governed by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The basic principles of data privacy (fairness, lawfulness, transparency, data minimisation, security, etc), are laid down in the GDPR, and supplemented by the DPA 2018. Further information on the implications of the GDPR and the DPA 2018 for researchers is available on the University's Research Services website.

The GDPR makes it mandatory for the University to report to the Information Commissioner's Office (ICO) any personal data breach that poses a risk to the rights and freedoms of individuals, and to do so within 72 hours of becoming aware of the breach. It also requires the University to notify the individuals affected in those cases where the breach is considered to pose a high risk to their rights and freedoms. Failure to comply with these requirements may result in the University being fined. Further guidance on how to recognise a personal data breach is available on the University's Information Compliance website.

The GDPR/DPA 2018 apply to any processing of personal data carried out on behalf of the University irrespective of whether that processing takes place within the UK. Researchers based overseas should also check and comply with any relevant local requirements.

3. SCOPE

The scope of this procedure is for all clinical research studies sponsored by the University of Oxford, but may also be used for other clinical research studies at the discretion of the unit.

4. DEFINITIONS

Clinical Trial Data

Information as numerical or text values found within paper and electronic records (including images and sound) e.g. trial reports, case report forms, faxed documents, emails and attachments, trial databases, photographs and x-rays.

Personal data

Information which relates to a living individual who can be identified from that information, whether directly or indirectly, and in particular by reference to an identifier, e.g. a name, an identification number, location data, or an online identifier, such as the IP address, as long as that information can be linked to a living individual. It could also include information that identifies an individual's characteristics, whether physical, physiological, genetic, cultural or social.

Special Category Data (previously known as sensitive personal data)

Special Category Data comprises categories of personal information that are recognised as being particularly private and requiring higher levels of protection. Special Category Data includes any

personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health , genetic data, biometric data (where used for the purpose of uniquely identifying a person), or sexual life. Data relating to criminal convictions or allegations are no longer classified as Special Category Data but are still subject to additional requirements.

Personal data breach
Any breach of security leading to the unauthorised disclosure of, or access to, personal data or its accidental/unlawful destruction, loss or alteration.

Anonymised Data
Data for which it is impossible to identify the participant from the information or any other information held.

Pseudo-anonymised data
Trial participants are given an identifier by which they are known in a system (e.g. Case Record Form, computer database), which is typically a number or other identifier. One master list with the identifier and patients' details must be kept separately in order to link the patient to their data. Recital 26 of GDPR makes it clear that pseudonymised personal data remains personal data and within the scope of the GDPR.

5. RESPONSIBILITIES

Sponsor
The Sponsor has overall accountability for handling and maintaining personal clinical research data in such a way as to satisfy legal and University requirements for security and privacy. This may be delegated in a written agreement. The Sponsor is also responsible for investigating any incidents that may constitute a breach of Data Protection i.e. any incident that may result in personal data being lost or accessed by unauthorised persons.

Chief Investigator (CI) / Principal Investigator (PI) / Clinical Trial Unit (CTU)
The CI, PI or head of a CTU are responsible for data confidentiality and security within a clinical trial, including ensuring all clinical research staff are appropriately trained, equipped and made aware of their individual legal and ethical responsibilities.

All Clinical Research Staff
Clinical research staff are responsible for handling all data in accordance with their individual legal and ethical responsibilities.

6. SPECIFIC PROCEDURE

6.1 Trial Protocol, Participant Information Sheets (PIS) and Informed Consent Forms (ICF)

Arrangements for data protection and security should be clearly described in the trial protocol. PIS and ICF should contain information on: the items of personal data to be collected, including whether participants could be identified; the lawful basis for the processing of that data; how the data will be used; details of any organisation that will collect, store and process the data; details of any data transfers; and the intended duration of data retention. Clinical research data should be classified and handled according to how critical and sensitive they are.

6.2 Data Security (paper or electronic data)

As with all clinical research data, personal data should be stored securely and retained for only as long as is necessary. Access to the data must be restricted to relevant members of staff, authorised by the Sponsor, CI, PI or host organisation. Staff should be granted access to data on a least-privilege basis.

All IT systems and/or third-party organisations used to store, process or transmit any clinical research data must be compliant with the University's Information Security Policy and baseline IT security requirements.

For support and guidance with all matters relating to information security the Information Security Team (IST) should be contacted. Technical threats to IT security (e.g. malware infections, hacking, and unauthorised access) should be reported to the IST (oxcert@it.ox.ac.uk) as soon as possible and within 4 working hours. If the incident involves a risk to personal data, the IST will refer the matter to the Information Compliance Team (ICT).

6.3 Transfer of Personal Data

All personal data transfers including paper and electronic should be approved by the Sponsor or delegate e.g. CI, and must be logged and documented. Data transferred by electronic means should be risk assessed, approved and protected. Where passwords are used, they should be communicated separately from the password-protected data, preferably by phone. When data is transferred by e-mail, a record of the transfer must be retained.

6.4 Personal data breaches

Potential personal data breaches must be reported immediately and directly to the University's ICT (data.breach@admin.ox.ac.uk). The ICT will determine whether the breach needs to be reported to the ICO and will liaise with the IST if technical issues are involved.

Individuals who become aware of a potential personal data breach should take immediate steps to reduce the exposure and mitigate risk (e.g. contact any person responsible and advise them to cease the activity; securely deleting, destroying or anonymising any records received in error etc.)

Any incidents requiring investigation should be opened with the aim of preventing or minimising any damage caused by the breach. Investigations should record the root cause of any breaches along with any remediation actions necessary to prevent further similar breaches.

ICT will forward any personal data breaches occurring within clinical research studies sponsored by the University of Oxford to CTRG. ICT will also forward to CTRG any personal data breaches involving clinical data where it is not possible to identify the Sponsor. CTRG will then work with the CI, trial team and the ICT to investigate, document and, where appropriate, report personal data breaches to relevant parties, such as research ethics committee and competent authorities. The ICT will remain responsible for reporting the breach to the ICO, if required.

6.5 Archiving

Clinical research personal data must be archived appropriately in line with Core SOP 005, Archiving of Essential Documents and in accordance with the relevant ethics application and approvals, Data Protection Act, and other relevant legislation.

7. RELATED DOCUMENTS

University of Oxford Core SOP 002 – Protocol Development
University of Oxford Core SOP 007 – Preparation of Participant Information Sheets and Informed Consent Forms
University of Oxford Core SOP 005 - Archiving of the Trial Master File and Essential Documents
University of Oxford Core SOP 009 – Managing Complaints Arising from Clinical Research

8. REFERENCES

Guidance on reporting of data breaches
https://www1.admin.ox.ac.uk/councilsec/compliance/gdpr/reportingdatabreaches/

Flow chart to assist in recognising a data breach
https://www1.admin.ox.ac.uk/media/global/wwwadminoxacuk/localsites/councilsecretariat/oxonly/documents/GDPR_Chart.pdf

Guidance for researchers on the GDPR
https://researchsupport.admin.ox.ac.uk/policy/data

University policy on Data Protection
https://www.admin.ox.ac.uk/councilsec/compliance/gdpr/universitypolicyondataprotection/

University of Oxford Information Security Policy and guidance
https://infosec.ox.ac.uk/guidance-policy
https://www.infosec.ox.ac.uk/guidance-policy/asset-management

9. CHANGE HISTORY

Version No.	Effective Date	Significant Changes	Previous Version No.
1.0	19 July 2017	This is the first version of this SOP.	n/a
2.0	19 Feb 2019	Updated following implementation of GDPR and clarification regarding grade of events reportable to the Information Compliance Team and Sponsor.	1.0
3.0	See first page	Added deadline to report to ICT in section 6.4 Change to Authoriser job title	2.0