<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author on behalf of the QA Focus Group</strong></td>
<td>Clare Riddle  Senior QA and Compliance Manager, Clinical Trials and Research Governance</td>
<td>[Signature]</td>
<td>15 May 2017</td>
</tr>
<tr>
<td><strong>Reviewer on behalf of the QA Focus Group</strong></td>
<td>Elaine Chick  Deputy Head of Clinical Trials and Research Governance</td>
<td>[Signature]</td>
<td>13/5/17</td>
</tr>
<tr>
<td><strong>Authoriser</strong></td>
<td>Heather House  Head of Clinical Trials and Research Governance</td>
<td>[Signature]</td>
<td>15/05/2017</td>
</tr>
</tbody>
</table>

Agreed by QA Focus Group: 26 April 2017

Effective Date: 19 July 2017

Review Date: 18 July 2020

NB If using a printed copy of this SOP, you must ensure that it is the latest approved version by checking it against the original available on the CTRG website (http://www.admin.ox.ac.uk/researchsupport/ctrг/)

Page 1 of 5
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 confidentially.

2. INTRODUCTION

The Data Protection Act (1998) legislates within the UK for the control and protection of personal data by the implementation of administrative, technical, or physical measures to guard against unauthorised access to data. The Act protects privacy, requires fair and lawful processing of personal information and restricts what can be done with it, and to whom it may be disclosed.

The Data Protection Act applies to any processing of personal data carried out by the University irrespective of whether that processing takes place within the UK. However, 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
Data which relate to a living individual who can be identified from those data, or from those data in combination with other accessible information. This includes names, addresses, NHS numbers, dates of birth, as well as combinations of data which together might identify an individual (e.g. a dataset containing hospital, gender, age, dates).

Sensitive Personal data
A category of personal information that is usually held in confidence and the loss, misdirection or loss of integrity of which could impact adversely on individuals, the organisation, or on the wider community, e.g. racial or ethnic origin, religious or political beliefs, trade union membership, physical or mental health or condition, sexual life, offences (alleged or committed).

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, but may also be an identifier. One
master list with the identifier and patients’ details must be kept separately in order to link the patient to their data.

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 the Data Protection Act 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; 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 record retention. Clinical trial data should be classified and handled according to how critical and sensitive they are.

6.2 Data Security (paper or electronic data)
All clinical research data not received in an anonymised form must be collected with the permission of trial participants, 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.

Breaches of IT security (e.g. malware infections, hacking, unauthorised access) should be reported to oxcert@it.ox.ac.uk as soon as possible and within 4 working hours.

For support and guidance with all matters relating to information security the information security team should be contacted.

NB If using a printed copy of this SOP, you must ensure that it is the latest approved version by checking it against the original available on the CTRG website (http://www.admin.ox.ac.uk/researchsupport/ctr/)
6.3 Transfer of Personal Data
All personal data transfer 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. When data is transferred by the e-mail, record of the transfer must be retained.

6.4 Breach of Confidentiality
Known breaches of data protection must be reported directly to the Information Compliance team (data.protection@admin.ox.ac.uk)

Individuals that become aware of a potential breach of data protection should take immediate steps to reduce the exposure and minimise 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.)

An 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.

All significant breaches of confidentiality where there has been a loss or inappropriate sharing of sensitive personal data outside of the University must be reported to the Sponsor immediately. This would include, for example, any loss or unauthorised disclosure of data relating to the health of study participants or non-public identifiers, such as bank details, national insurance number, passport number, which could be used for identity fraud. The Sponsor will work with the CI and trial team to investigate, document and where appropriate report breaches of confidentiality. The Sponsor may decide the Information Security or Assistant Registrar (Compliance) Office need to be informed.

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
University of Oxford policy on Data Protection
http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/
University guidance on data protection
http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/policy/
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

NB If using a printed copy of this SOP, you must ensure that it is the latest approved version by checking it against the original available on the CTRG website (http://www.admin.ox.ac.uk/researchsupport/ctrsg/)
9. CHANGE HISTORY

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Effective Date</th>
<th>Significant Changes</th>
<th>Previous Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>See first page</td>
<td>This is the first version of this SOP.</td>
<td>n/a</td>
</tr>
</tbody>
</table>