RDSOP17
Research Data Management and Security

Greater Manchester Mental Health NHS Foundation Trust
**Title of Standard Operating Procedure:**

RDSOP17
Research data management and security

**Document Summary:**

The purpose of this SOP is to describe the procedures for managing research data and ensuring that research data is stored in a safe and secure manner.

**Document Author:**

Sue Dobson, Research Grants Co-ordinator

**Target Audience:**

Trust-wide, Research Community, Internal and External Researchers

**Consultation:**

R & I Office, research community and R & I Committee members

**Approval Committee:**

R & I Committee

**Cross Reference Document(s):**

Research Approval Policy
All Trust R & I SOPs

**Contact details for further information:**

Sarah Leo, Head of Research & Innovation Office 0161 271 0076 researchoffice@gmmh.nhs.uk

<table>
<thead>
<tr>
<th>Minimum Monitoring Requirement</th>
<th>Frequency</th>
<th>Process for monitoring</th>
<th>Evidence</th>
<th>Responsible Individual(s)</th>
<th>Response Committee(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review of SOP content</td>
<td>Annually</td>
<td>Review by Author, redraft, submission to R &amp; I Operational Group</td>
<td>Minutes of R &amp; I Operational Group</td>
<td>Head of R &amp; I Office</td>
<td>Research &amp; Innovation Committee</td>
</tr>
</tbody>
</table>

Ref: RDSOP17  Issue date: 19/072017  Version number: 1.0
Status: Final  Next review date: 19/07/2020  Page 1 of 8
Contents

1. Introduction........................................................................................................................................... 4
2. Purpose .................................................................................................................................................. 5
3. Roles and Responsibilities .................................................................................................................... 5
3.1. Duties within the Organisation ...................................................................................................... 6
4. Procedure ............................................................................................................................................. 6
4.1 Data Management and Security Procedure – Basic Terms .............................................................. 6
4.2 Data Management .......................................................................................................................... 7
4.3 Data Security .................................................................................................................................... 8
4.4 Data Transfer .................................................................................................................................... 8
4.5 General Data Protection Regulation – Data Transparency ............................................................... 8
5. References and Bibliography .............................................................................................................. 9
1. Introduction

All data collected for research purposes must comply with the Data Protection Act 2018 (DPA). This includes data collected from patients, families and staff. The DPA outlines the conditions that must be met by organisations and individuals who hold or process personal identifiable information about living individuals:

- Personal data should be fairly and lawfully processed
- Data should be adequate for the purpose and not excessive
- Data should be obtained for specified purposes
- Data should be accurate and up to date
- Appropriate measures should be taken to ensure confidentiality and security of the data
- Data should be processed in accordance with the rights of the data subject
- Data should not be kept longer than is necessary
- Data should not be transferred outside of the European Economic Area without an adequate level of protection

UK Policy Framework for Health and Social Care Research v3.3 07/11/17. The Framework states that: “The appropriate use and protection of patient data is also paramount. All those involved in research must be aware of their legal and ethical duties. Particular attention must be given to systems for ensuring confidentiality of personal information and to the security of those systems”.

Around the same time as the DPA was published, a review was commissioned by the Chief Medical Office of England "owing to increasing concern about the ways in which patient information is being used in the NHS in England and Wales and the need to ensure that confidentiality is not undermined. Such concern was largely due to the development of information technology in the service, and its capacity to disseminate information about patients rapidly and extensively". A committee was established under the chairmanship of Dame Fiona Caldicott, Principal of Somerville College, Oxford, and previously President of the Royal College of Psychiatrists. Its findings were published in December 1997.

The ‘Caldicott' principles and recommendations apply specifically to patient-identifiable information, and emphasise the need for controls over the availability of such information and access to it. In particular, a Caldicott Guardian, appointed in each NHS organisation, has specific responsibilities to oversee an ongoing process of audit, improvement and control.

The six Caldicott principles, applying to the handling of patient-identifiable information, are:

- Justify the purpose(s) of every proposed use or transfer
- Don't use it unless it is absolutely necessary, and
- Use the minimum necessary
- Access to it should be on a strict need-to-know basis
- Everyone with access to it should be aware of their responsibilities, and
- Understand and comply with the law.

The 2018 Data Protection Act is the key legislation covering all aspects of information processing. This includes security and confidentiality of personal information. The Caldicott requirements provide the framework to put the Data Protection Act into operation.

The EU’s General Data Protection Regulation (GDPR) came into effect on the 25 May 2018. For an organisation such as the GMMH, our role and level of involvement changes with each particular study. However, in each case we are required to be transparent in how personal data is collected, processed, accessed and stored as well as informing service users of the safeguards involved to retain compliance with appropriate legislations, and their rights around this.

2. Purpose

The purpose of this SOP is to describe the procedures for managing research data and ensuring that research data is stored in a safe and secure manner.

3. Roles and Responsibilities

3.1 Duties within the Organisation

It is the responsibility of the Research & Innovation Office to make Trust R & I SOPs available to all research active staff working on Trust-approved research studies.

It is the responsibility of the study Chief Investigator (CI) or local Principal Investigator (PI) to ensure that up-to-date copies of Trust R & I SOPs are available to research staff.

It is the responsibility of the study Chief Investigator or local Principal Investigator to ensure up-to-date SOPs are filed in the Investigator Site File and are available to research staff, and to inform the Research Support Co-ordinator of the names of all research staff involved on a study so that copies of SOPs can be distributed appropriately.

It is the responsibility of the study Chief Investigator or Principal Investigator to designate if the SOPs of another organisation are to be followed for a study. For example those of a Clinical Research Network or commercial sponsor. If there is significant conflict between the external SOP and the Trust R & I SOP it is the responsibility of the CI or PI to resolve these with the Research Office prior to starting the study.

It is the personal responsibility of all staff to follow Trust (or the designated alternative organisations) procedural documents.
The Research & Innovation Office is responsible for managing Trust R & I SOPs including their approval, dissemination and archiving. All Trust R & I SOPs must be made available and published on the Trust website.

4. **Procedure**

4.1 Data Management and Security Procedure – Basic Terms

**Personal data.** Personal data is any information that may lead to the identification of a living person that if released would put them at significant risk or harm or distress.

**Anonymised data.** Anonymised data is where all patient or participant identifiers (which can include name or initials, address, date of birth, hospital or NHS number) have been permanently removed. Anonymised data are not covered by the DPA.

**Pseudo-anonymised data.** Pseudo-anonymised data is where all personal identifiers (which can include name or initials, address, date of birth, hospital or NHS number) are replaced with a unique identifier (e.g. patient study number, patient initials, date of birth). A code should be held separately from patient identifiers, and allow for study un-blinding if required by the protocol.

**Source documents.** Source documents are original documents, data and records (e.g. hospital records, clinical and office charts, laboratory notes, diaries or evaluation checklists, laboratory results, x-ray or other scan results, pharmacy dispensing records). These are the ‘essential documents’ as described by ICH GCP that allow the evaluation and verification of the research study and data collected.

**Source data.** Source data are all information in original records and certified copies of original records of clinical findings, observations, or other activities in a research study necessary for the reconstruction and evaluation of the study. Source data are contained in source documents.

4.2 Data Management

All research data containing personal information about patients or participants should be anonymised. For certain studies, such as clinical trials of an investigational medicinal product, this may not be possible and the data should be pseudo-anonymised. In these instances, un-blinding procedures for safety reasons should be clearly defined in the protocol.

Clinical trial data should be collected onto a Case Report Form (CRF). This can be a printed, optical or electronic document and designed to record all the information detailed in the protocol. All staff completing CRF’s should be trained to do so. Corrections to the printed CRF should be initialled and dated by the PI or persons delegated to do so. Correction fluid should never be used.
Clinical trial data from the CRF may be entered onto a database or other data management system. For clinical trials, data entry should be completed by the Data Manager, Data Custodian or other person designated to do so by the Principal Investigator. The data entry process (e.g. single data entry or double data entry methods) should be decided based on the size and complexity of the study. For small single site studies, single data entry (one person) with source verification is usually appropriate. This will involve a visual check between what is recorded on the paper CRF and what is entered onto the data management system.

Missing values, values outside of normal ranges or inconsistencies entered onto CRF’s should be reported to the PI.

Source data verification can be conducted by members of the research team or independent monitors. This will involve cross-checking the data entered onto the CRF against source documents for accuracy.

All research staff using a data management system should be trained in its proper operation. A training record should be kept and updated following any software changes or upgrades.

The data management system should be appropriate for the analysis planned, ensure data integrity and be auditable. In the case of certain data management systems (e.g. Microsoft Excel), it may be necessary to save and date older versions of the database or print copies.

All computer systems used in the conduct of clinical trials of investigational medicinal products (databases, Electronic Data Capture etc), must have their current release number and date of release, last release number and date of release and validation status recorded.

For information on storage and archiving of files, please refer to RDSOP37.

### 4.3 Data Security

All non- electronic data such as paper CRFs and other documents, audio and video recordings, should be kept in locked filing cabinets in lockable rooms only accessible by authorised personnel.

Electronic data should only be stored on devices that are backed up regularly such as NHS Trust or other servers (e.g. University). This should be confirmed with IT support or by consulting Trust or local policy documents.

Backup electronic copies should be kept in a separate secure location to the master copy. These should be updated daily.

Data should be password protected and access limited to authorised personnel. Authorised users should login with their own account details and should never login to provide access to another user.
A record should be kept of authorised users and their level of access.

Laptops and memory sticks used to store data should be encrypted by Trust, local IT support or the study coordinating centre.

### 4.4 Data Transfer

Research data transferred within the European Economic Area (EEA) must be fully or pseudo anonymised. Any codes held to unblind or unlock data identity should not be sent.

Research data transferred outside the EEA must be fully or pseudo anonymised. An agreement should be in place documenting that the data will be held or processed according to the principles outlined in the DPA (2018). Any codes held to unblind or unlock data identity should not be sent.

Participants should be consented for their data to be transferred to a third party.

Approvals from the relevant ethics committee and/or Caldicott Guardian (the Trust Medical Director) should be obtained before data is transferred to a third party.

### 4.5 General Data Protection Regulation – Data Transparency

As a research Sponsor, GMMH acts as the “Data Controller”. The Data Controller determines the purpose and means of processing personal data. It is the Sponsor who determines what data is collected for the research study through the protocol, case report form and/or structured data fields in a database.

As a research Host (i.e. where the Sponsor is another organisation, such as a university or commercial company), GMMH acts as the “Processor”. The Processor collects personal data on behalf of the Data Controller.

Useful transparency statements for researchers
Researchers should liaise with the research Sponsor to ensure that the appropriate transparency statements are inserted into Protocols and Participant Information Sheets. The HRA has provided some useful guidance templates here.
5. References and Bibliography

Data Protection Act (2018)

Caldicott review: information governance in the health and care system (2013)
https://www.gov.uk/government/publications/the-information-governance-review

UK Policy Framework for Health and Social Care Research v3.3 07/11/17

ICH – Good Clinical Practice guidelines

HRA GDPR Guidance 2018