**RESPONSIBLE EXECUTIVE** Angela Watt

**PRIMARY AUTHOR** Sarah Rickard

**IMPLEMENTATION STRATEGY** Email update to all employees and uploaded to the Office for Research website.

**EVALUATION STRATEGY** Updated policy to be evaluated by Melbourne Health Office for Research Governance management team.

**STANDARD/S** (National, Aged Care, Disability Services) NSQHS Clinical Governance Standard.

**VERSION SUMMARY** The Data Storage and Security Guideline is a supporting document for the MH Data Management in Research Guideline.
The Guideline has been developed to clearly set out the roles and responsibilities of Melbourne Health (MH) and persons involved in the management of storage and security for research data at MH.

These guidelines have been written in accordance with the *Australian Code for the Responsible Conduct of Research (2018)* and supporting guide Management of Data and Information in Research.


**EXECUTIVE SUMMARY**

1. MH recognises that Data are valuable, and that Data integrity relies on good documentation practices and stewardship throughout the entire data lifecycle irrespective of the format of the Data (i.e. paper, electronic, tape, film etc).
2. Heads of Departments are responsible for providing appropriate storage space for research Data and maintaining departmental database of studies and storage locations of Data, metadata etc.
3. Principal Investigators are responsible for ensuring that studies comply with Good Data management practices.
4. All study team members are responsible for appropriately managing research Data and confidential information.
5. The primary site of electronic Data storage is on the MH server.
6. The study Data Management Plan (DMP) should include elements that address Data storage and security throughout all stages of the Data life cycle.


## 1. ASSOCIATED MELBOURNE HEALTH POLICY

MH Research Policy MH18

## 2. PURPOSE AND SCOPE

To describe storage and security requirements for research Data and confidential information associated with research studies conducted at Melbourne Health (MH).

This guideline is applicable to all research data obtained or generated for research studies undertaken at MH.

This guideline is applicable to all study team members, including Principal Investigators (PI), Associate Investigators (AI), research coordinators, data managers etc., involved in research studies at M.

## 3. DEFINITIONS

| | |
|---|---|
| **Data** | Data are facts, observations or experiences on which an argument, theory or test is based. Data may be numerical, descriptive or visual. Data may be raw or analysed, experimental or observational. Research Data includes:<br>• Laboratory and field notebooks.<br>• Primary research data (including research data in hardcopy or in computer readable form).<br>• Information obtained directly from a person in interview, questionnaire, focus groups, personal and medical histories, demographics, biographies, audiotape, audio-visual records, photographs, film.<br>• Clinical, social or observational information from a source other than the person whose information it is, such as from medical history notes, doctors' notes, surgical notes, carer or relative.<br>• Test responses.<br>• Models.<br>• Information derived from human tissue such as blood, bone, muscle, organ and waste products, including genetic and radiological information.<br>Research collections may include slides; artefacts; specimens; samples. Provenance information about the data might also be included: the how, when, where it was collected and with what (for example, instrument). The software code used to generate, annotate or analyse the data may also be included. |
| **Data Management Plan** | A Data Management Plan (DMP) typically outlines what research Data will be used and created during the course of a research project and as well as plans for sharing and preserving the Data and any restrictions that may need to be applied. |
| **Metadata** | Metadata are information that describes the Data or primary materials, and normally includes such details as the means of creation of the data, the purpose of the data, time and date of creation, the creator or author of data, the location of the data, etc. It assists in the discovery, use/re-use and management of the data, and in allowing correct attribution to the creators of the work.<br>For example, recording a participant's pulse is the data (result) but the Metadata are that data that goes around the result that makes it worthwhile and includes the protocol, visit number, information on the instruments used, their settings, whether the participant was sitting or lying down, time of day etc.<br>For laboratory research Metadata could include notes in laboratory notebooks, batches of chemicals used, facility temperatures etc.<br>Refer to https://www.ands.org.au/guides/metaData-working for further information. |
| **Primary Materials** | Physical objects acquired through a process of scholarly investigation from which research data may be derived. It may include raw physical materials such as ore, soil samples or biological material, or physical or digital objects such as artefacts, questionnaires, sound recordings or video. Depending on discipline, primary materials may be considered research data, and may be required to be retained if they are required to validate the outcomes of research and defend those outcomes against challenge. |

## 4. RESPONSIBILITIES

Heads of Departments are responsible for:

- Providing storage space for research Data and metadata that meets security and confidentiality requirements.
- Maintaining a departmental research database of studies and storage locations of Data, metadata etc. The data base should include minimum retention periods, identify contact persons and information to access/retrieve records when required.

Principal Investigators are responsible for:

- Ensuring that research study data storage comply with good Data management practices and any other applicable requirement.
- Developing, implementing, managing and documenting the Data Management Plan (DMP) for each research study.
- Completing a study Source Data Identification log (SDIL) as part of the DMP.
- Training study staff in study data management requirements including the DMP.
- Ensuring that studies are listed a MH research database and on completion of the study, all storage locations of Data, metadata etc. have been identified and included in the database.

All study team members are responsible for managing research Data and confidential information appropriately and in accordance with any applicable requirements including the DMP, maintaining Data in a secure manner and allowing only appropriate, approved access to the study Data.

## 5. PROCEDURE/GUIDELINE/POLICY

### 5.1. INTRODUCTION

MH recognises that Data are valuable, and that data integrity relies on good documentation practices and stewardship.

The principles and responsibilities outlined in the Australian Code for the Responsible Conduct of Research (Code) and its sub-documents underpin responsible research conduct including appropriate data management:

- R8 of the Code requires that institutions provide access to facilities for the safe and secure storage and management of research data, records and primary materials and, where possible and appropriate, allow access and reference.
- R22 of the Code requires that researchers retain clear, accurate, secure and complete records of all research including research data and primary materials. Where possible and appropriate, allow access and reference to these by interested parties.
- Management of Data and Information in Research: A guide supporting the Australian Code for the Responsible Conduct of Research requires researchers to exercise care in handling confidential or other sensitive information used in or arising from a research project.

Data storage should be fit for purpose consideration of issues such as ease of storage, assess, security, durability, maintenance of integrity etc. in relation to the information being stored.

Refer to MH Data Management in Research Guideline and its associated guidelines for further information relating to:

- Good Data management practices that should be followed for Data that will be used and created during the conduct of research studies.
- The elements of a Data Management Plan (DMP) to address Data issues throughout all stages of the Data life cycle.

Refer to MH SOP 007 Case Report Forms, Source Documents, Records Keeping and Archiving for further information relating to:

- Completing a Source Data Identification log (SDIL)

- Case Report Forms, Data Collection Forms and Source Documents,
- Documenting research participation in iPM
- Documentation information in the participants Medical Record
- Making changes / corrections to CRFs, DCFs and source documents
- Storage of source documents – record keeping
- Archiving Source Documents

### 5.2. DATA STORAGE DURING THE ACTIVE PHASE OF STUDIES

Data storage locations and formats should be described in the DMP should.

During the active phase of the research study Data should be stored safely, securely, in a manner that maintains integrity, confidentiality, and:

- In appropriate facilities relevant to the format of the Data to protect against theft, misuse, damage or loss. It is wasteful to repeat studies due to Data loss from theft, poorly planned Data management or inadequate recording of Data.
- In accordance with the terms and conditions of research agreements including confidentiality agreements.

  Note: The PI should ensure that all research team members are aware of applicable terms and conditions outlined in research agreements.
- Data files and folders should be named consistently and organised in a way is intuitive for all users, so they can easily identify and access the information they need. This should be done irrespective of the Data format or storage system used.
- Researchers should ensure that the information and Metadata are stored together with the relevant Data set.
- For coded Data, the key to the code to re-identifiable Data must be kept separately to the Data. An electronic re-identifiable Data and its associated key to the code may be kept on the same computer, however they must be stored in separate files.

Study PIs are responsible for ensuring that studies are listed on their departments research database and on completion of the study, all storage locations of Data, metadata etc. have been identified and included in the database.

Data MUST NOT be removed from MH unless approved under ethical and governance approvals or appropriate agreement/s.

### 5.3. LABELING RESEARCH DATA

Labelling of Data should be considered and be appropriate to each phase of the research study.

Data may be labelled as identifiable, re-identifiable or non-identifiable depending on the requirements of the study protocol and ethical approval obtained.

Important considerations for discussions of identifying/non-identifying data:

- Whether a piece of information is “identifying data’ or “identifiable” may be contextual. For example, where identifiers (names, address, date of birth etc) have been removed from data sets, the data itself may still allow identification of those whose data it is based on the number and types of data points held i.e. as you increase the number and specificity of the data points you have for a person you are more likely to be able to identify them.
- In some instances, it may not be possible to make data non-identifiable due to the nature of the data (i.e. genetic data) or participant group involved (i.e. rare diseases).

In determining the appropriate method for labelling Data, the PI and research team should ensure that:

- The protocol describes a plan for the protection of participants' privacy.
- The research team has SOP(s) to describe the identification and protection of participant Data and privacy.
- Persons given access to confidential information should maintain confidentiality.

#### 5.3.1 Non-Identifying Data

Most Data can maintain their integrity without the use of identifiers. Therefore, in most cases that Data should not be kept in an identifiable state.

Researchers should consider that although, during Data collection, it may be necessary to keep a database of identifiable or re-identifiable Data, the Data should be made non-identifiable if and or when the ability to be able to identify the individual whose information it is, is no longer required.

#### 5.3.2 Re-identifiable Data

Data may be maintained in a re-identifiable manner for the following purposes:

- Collation of Data – where Data are collected at different time points or from different sources, including external sources.
- Further health implications - Researchers and Databank/registry trustees should consider if any knowledge will be gained during analysis of the Data and associated testing, that could impact on an individual's health and wellbeing or that it would be in the best interests of the individual to know. Such Data should be kept in a re-identifiable manner to ensure the new information can be provided to the individual.
- Any other ethically approved purpose.

Re-identifiable Data should be stored in a coded manner. The 'key' linking the code to the participants identifying information must be stored separately to the re-identifiable Data and access only by authorised persons on the research team.

Note: the UR or hospital designated patient number is not an acceptable participant code for research Data as it is considered identifiable.

#### 5.3.1 Identifiable Data

Where Data will be stored in an identifiable manner, the PI should provide a justification in the protocol outlining in detail the reasons and benefits for keeping Data in an identifiable state as well as the risks and security precautions that will be taken to ensure confidentiality of the information.

### 5.4. PAPER RECORDS

Study records kept as paper records should be:

- Maintained in an orderly manner and documents filed in a timely manner.
- Stored in an appropriate filing system that is only accessible to authorised staff.
- Stored in the department where the researcher works whilst a project is active.
- Stored in an area that has controlled access and is locked when staff are not in attendance.
- Stored in filling cabinets that can be locked when not in use, where possible.

Paper records MUST:

- Not be removed from MH unless approved under ethical and governance approvals and associated agreement, or other appropriate agreement.
- Be accessible for monitoring, audit and inspection as appropriate to the study.

### 5.5. AUDIOTAPE, AUDIO-VISUAL RECORDS AND PHOTOGRAPHS

Data kept as physical audiotape, audio-visual records and photographs should be stored in lockable storage facilities in the researchers work area or department in a lockable office.

Audio-visual Data may be kept in a re-identifiable or non-identifiable state according to study approvals and consents etc. However, by their very nature these types of records may remain identifiable and if so, they should be treated as identifiable and strict security and precautions to ensure confidentiality should be taken.

Refer to the section 5.6 for storage requirements of electronic Data.

### 5.6. ELECTRONIC DATA

Electronic Data storage should be managed to ensure secure access, storage and retrieval of Data in all phases of the study including archiving, and prevent Data breaches or losses from:

- Accidental deletion of Data/files.
- Inappropriate access/release of Data.
- Corrupt files.
- Theft of portable devices.
- Data/files becoming inaccessible due to aging technology during retention / archiving.

#### 5.6.1 STORE ELECTRONIC DATA ON THE MH SERVER

The primary site of electronic Data storage is on MH servers. There may be multiple locations for storage of electronic data such as in Departmental files and MH supported systems such as REDCap. Exceptions to this are MH systems that have off-site storage that is not on a MH server such as the Electronic Medical Record.

Benefits of storing electronic research information on the MH server include:

- Security management – registered access of users, maintenance of firewalls, etc.
- IT support.
- Backup and retrieval of Data to maintain Data integrity.
- Compliance with MH requirements.

#### 5.6.2 PROCESSES FOR DATA THAT IS GATHERED AND/OR STORED ELECTRONICALLY

Where Data are gathered and/or stored electronically, there should be processes to ensure:

- The system is secure.
- Access to Data are restricted to authorised persons i.e. should be protected by secure login and password. This is required irrespective of the storage location, i.e. server or portable device.
- The electronic system is valid for the type of Data to be collected/stored and its use has been validated. It is up to the PI/research team to determine parameters and procedures for validation of the electronic systems.
- Secure storage of portable devices to protect against in appropriate access, loss, theft etc.
- Data are securely and regularly backed up. Note: Information stored on the MH server is backed up at least daily. For electronic Data collected/stored outside of the MH server define how and is transferred to the MH sever and back-up is managed (where/how often/who is responsible/is it secure?). Contact MH IT to discuss transfer of large data files to the MH server.
- Durability of the Data i.e. the system is maintained, and Data will be available in a usable format throughout both the entire active and archiving phases of the project.

- Where electronic Data are transferred to MH from external parties, this should be in compliance with approvals, permissions, agreements and any applicable regulations, guidelines or other requirements.

### 5.6.3 NAMING ELECTRONIC FILES

An appropriate and systematic file naming system that allows ease of access, identification of study documents should be used.

Refer to Appendix A for an example of the structure for an electronic study file.

An example of a file naming system to be used for files in the project folders is provided below:

- Date of creation (i.e. year/month/day)
- Unique project number / reference such as HREC number or protocol number (2019.600 or 55376 or RCT423)
- Site reference
- Description of content (HREC correspondence, protocol, IB, participant 001 info etc.)
- Version number
- Creator/owner/project team
- Any other relevant information as applicable

For example: 2018.04.25-2018.600-MH-ESCAPE-ProtV1
2018.04.25-2018.600-MH-ESCAPE-IBV2

**Important note:** If the study Data are to be deposited into an archive or repository, files may require specific labelling and format. In these instances, researchers should confirm and use these requirements from the start of the study to avoid wasting time and effort re-labelling and/or formatting files when it comes time to deposit them into the archive or repository.

### 5.6.4 ELECTRONIC DATA SHOULD BE STORED IN FORMATS (PROGRAMS) THAT ARE FREELY AVAILABLE

The use of non-proprietary or open standard Data formats/programs is strongly encouraged.

This helps avoid situations where Data becomes dependent or “locked into” proprietary application software. It also enhances Data interchange and transformation.

Where the use of closed or proprietary Data formats cannot be avoided, consideration should be given to how licensing and access arrangements will be funded and supported into the future.

### 5.6.5 THE REDCap DATABASE

REDCap is a secure web application that can be used to collect virtually any type of Data.

Where possible use REDCap should be used to facilitate electronic management and storage of research Data for data stored outside of medical records e.g. consent database, eCRF, surveys, questionnaires etc.

The REDCap program is hosted on MH servers and managed by the Business Intelligence Unit.

Note: Data stored in REDCap at external organisations (i.e. University of Melbourne) is stored on that organisation’s server.

REDCap access requires individual login and passwords and it has a tracked and auditable trail of access/use.

In collaborative research where MH Data are stored on REDCap housed at another organisation, data management and ownership details should be described in the research protocol and agreement.

For further information on the use of REDCap refer to:

- Guidance for using REDCap
- MH REDCap FAQ
- Book into a REDCap support group sessions
- The REDCap project home page at https://projectredcap.org/ (this is an external site)

### 5.6.6 USE OF PORTABLE STORAGE DEVICES FOR RESEARCH DATA

The primary site of electronic research Data storage should be the MH server.

Copies of research Data may be stored on portable devices (e.g. laptops, tablets) and portable storage devices (i.e. hard drives, USBs).

Where research data are stored in portable devices or storage devices researchers should:

- Transfer the data to MH server as soon as possible after collection to prevent loss.
- Password protect access.
- Password protect files stored.
- Log off or lock access to portable devices when they are not in use, even for short periods of time.
- Consider encrypting portable storage devices and information stored on portable devices.
- Regularly scan portable devices and portable storage devices for viruses and other malicious software with MH required programs.

  Note: *This can be achieved by connecting the device to the MH system and running a virus scan. For further information contact the MH IT department*.
- Be aware that portable devices are a target for theft.
- Store portable devices and portable storage devices securely to prevent theft/damage when not in use.
- Be aware that portable devices and portable storage devices are also easily lost/ misplaced.

## 6. ASSOCIATED POLICIES/PROCEDURES/GUIDELINES

- MH Research Policy MH18
- Intellectual Property Policy MH12
- Documentation and Records Management MH 05
- Data Management in Research Guideline
- Agreements, Ownership and Intellectual Property Guideline
- Archiving retention and disposal of data Guideline
- Databanks and Registries Guideline
- Guidelines for the Use of Human Tissue Samples in Research
- SOP 7 CRFs, Source Documents, Record Keeping and Archiving
- Guidance for using REDCap

## 7. REFERENCES

- Australian Code for the Responsible Conduct of Research (2018)
- Guide to Managing and Investigating Potential Breaches of the Australian Code for the Responsible Conduct of Research (2018)
- Authorship - A guide supporting the Australian Code for the Responsible Conduct of Research
- Management of Data and Information in Research - A guide supporting the Australian Code for the Responsible Conduct of Research
- National Statement on Ethical Conduct in Human Research (2007updated 2018)
- ICH Good Clinical Practice (GCP) - Integrated Addendum to ICH E6 (R1) Guideline for Good Clinical Practice E6 (R2) (formerly adopted by the TGA with annotations on 8 February 2018)
- International Conference on Harmonisation / Good Clinical Practice (ICH/GCP) Guidelines

## 8. FURTHER INFORMATION

Contact the office for research on 03 9342 8550 or research@mh.org.au for further information or assistance.

## 9. DOCUMENTATION

- Research Collaboration agreement (MACH template)
- Source data identification log template form - refer to GCP SOP OO7
- Data Management Plan template form - refer to SOP Data Management Plan
- Data Sharing and Access plan for published data template form - refer to SOP Data Sharing and Access Plan
- Application to share/access research data template form - efer to SOP Data Sharing and Access Plan
- DSAP internal review process template form - refer to SOP Data Sharing and Access Plan
- Researcher request for copies of study materials when leaving Melbourne Health form

## 9. REVISION AND APPROVAL HISTORY

| Date | Version | Author* and contributors |
|---|---|---|
| 5/9/2019 | 1 | Sarah Rickard, Manager Research Governance and Audit |

**APPENDIX A: Example of the structure for an electronic study file**

Note: customise the electronic study folder to the Investigator Site File (or Research folder) Table of Contents.