Purpose

This document outlines the minimum requirements for the transfer, storage and retention of research data and records, according to Section 2 (Chapter 2.2) and Section 3 of the *National Statement on Ethical Conduct in Human Research (2023).*

Definitions

Data: Data are pieces of information. Data can be raw, cleaned, transformed, summary or metadata (data about data). It can also be research outputs and outcomes.

Information: Information is data that has been interpreted, analysed or contextualised.

Identifier: Identifier details are those that are attached to data that identify an individual, such as name and/or contact information.

Published data: is data that has been made available for use by others.

Research data: Research data is primary data obtained through observations, measurements, interview, surveys, tests and all participant material. Research data may be regarded as clinical if it is health-related information associated with regular patient care or a clinical trial.

Research findings: Information that becomes known as a result of the research are research findings, which may take the form of:

- findings related to primary aims of the research (including individual test results)
- findings related to secondary aims of the research or that are unintended, unanticipated, inadvertent or incidental to the aims of the research.

Guidance

Researchers have legal and ethical obligations to consider privacy issues. Bellberry HRECs expect all researchers and sponsors of research to conform to relevant legislation, standards and guidelines in relation to data storage and retention, and to the privacy and confidentiality of research participants' information. It is expected that:

- data are recorded and retained in durable and secure storage,
- stored data are referenced, and the storage location recorded,
- published data are kept for at least five years from the date of publication. Clinical research data must be kept for 15 years after a study is completed.
- where computer systems are connected to and accessible from networks, including the cloud, the security of confidential data must be is ensured,
- where data may transfer across borders or be stored in another jurisdiction, transfer and storage will occur according to any relevant Australian Privacy Principles under the Privacy Act 1988 of the Commonwealth (e.g., APP 8, HPP9).
    - In particular, an entity subject to the Australian Privacy Principles must take reasonable steps to ensure that an overseas recipient will handle personal information (being information about an identified individual, or an individual who is reasonably identifiable) in accordance with those principles and will be accountable if an overseas recipient mishandles the information (subject to any relevant exception under Australian law).

- when data are obtained from limited access databases, or via contractual arrangements, the researcher will retain a written indication of the location of the original data or key information about the database from which it was collected,
- security and confidentiality systems and procedures can handle multiple researchers and any departure of researchers from an institution,
- collection, use and disclosure of personal and health information only occurs where allowed under law and with appropriate consent,
- consent to any future use of data and/or tissues obtained in research complies with relevant guidelines of the *National Statement on Ethical Conduct in Human Research*,
- all research participants understand whether information used by the research team will be identifiable, re-identifiable (coded) or non-identifiable,
- participants must be informed, where relevant, regarding the review of health records by researchers and by representatives of regulatory authorities and the sponsor for the purposes of verifying the procedures and the data collected during the research,
- publications about a research study will not present information in such a way that participants can be identified.

Data Management Plan

As per the *National Statement* (3.1.44) For all research, each site should have a data management plan in place that addresses intentions related to the generation, collection, access, use, analysis, disclosure, storage, retention, disposal, sharing and re-use of data and information, the risks associated with these activities and any strategies for minimising those risks.

The following information should be included:

(a) physical, network, system security and any other technological security measures.

(b) policies and procedures.

(c) contractual and licensing arrangements and confidentiality agreements.

(d) training for members of the project team and others, as appropriate.

(e) the form in which the data or information will be stored.

(f) the purposes for which the data or information will be used and/or disclosed.

(g) the conditions under which access to the data or information may be granted to others; and

(h) what information from the data management plan, if any, needs to be communicated to potential participants.

References

National Statement on Ethical Conduct in Human Research (2023)
Australian Privacy Principles
Notes for Guidance on Good Clinical Practice ICH GCP E6(R2)
Guidelines under Section 95 of the Privacy Act 1988
Australian Code for the Responsible Conduct of Research 2018