Data Management in Research

Document type: Organisational Guideline	Current version: November 2023
Previous version: July 2020	Next review date: November 2026

This document is relevant to all WH sites, including Bacchus Marsh, Melton and Caroline Springs

Contents

1. Overview 2
2. Applicability 2
3. Responsibility 2
4. Authority 3
5. Associated Documentation 3
6. Credentialing Requirements 4
7. Definitions and Abbreviations 4
   7.1 Definitions 4
   7.2 Abbreviations 4
8. Guideline Detail 5
   8.1 Introduction 5
   8.2 Ownership 6
   8.3 Databanks and registries 6
      8.3.1 Departmental Register of Databanks and registries 6
      8.3.2 THE REDCap Database 7
      8.3.3 Registration of Clinical and Research Databanks/Registries at Western Health 7
      8.3.4 Databank/Registry Custodian 7
      8.3.5 Requests to use a Databank/registry 8
   8.4 Data Breaches 8
   8.5 Consent 8
   8.6 Identification of Data 9
   8.7 Access, Use and Disclosure of Data 9
   8.8 Data Storage and Security 10
      8.8.1 Paper Records/Databanks 10
      8.8.2 Electronic Data/Databanks 11
      8.8.3 Audiotape and Audio-visual Records, Photographs 11
   8.9 Removal or Movement of Data 11
   8.10 Archiving 11
   8.11 Destruction of Data 12
9. Document History 12
10. References 12
11. Sponsor 13
12. Authorisation Authority 13

Appendix 1 14

1. Overview

This document provides guidance and outlines the responsibilities and obligations of persons conducting research at Western Health. This information is provided in the context of appropriate data management throughout the entire Data Lifecycle, including but not limited to; generation, collection, access, dissemination, storage and management of research data and materials in accordance with the Australian Code for the Responsible Conduct of Research (2018), the Privacy and Data Protection Act 2014 (Vic), National Statement on Ethical Conduct in Human Research (2018 and updates) and other relevant legislations.

2. Applicability

This guideline applies to all Western Health (WH) staff, adjuncts or honorary appointees, visitors and students utilising WH resources and engaged in research involving health or personal information. This guideline and associated documents aim to govern the collection, use, storage, disclosure and destruction of data/information involving health, business or personal information. They also govern the creation and use of databanks in research. Furthermore, they govern the use of information that has previously been collected and stored in a database for a primary purpose other than that of research and for which researchers now wish to access, or may wish to access in the future, for research and/or quality assurance activities.
These guidelines outline the minimum requirements which apply to research and quality assurance projects ethically approved by the WH Low Risk Ethics Panel (LREP), National Mutual Acceptance (NMA) Human Research Ethics Committee (HREC) and authorised by WH Office for Research/Research Governance Office.

These guidelines cover, but are not limited to:

- Data collected and/or used and/or disclosed for research or quality assurance purposes;
- Data collected for the purpose of creating a database or registry that may be used in the future for research or quality assurance;
- Data collected by doctors, nurses and allied health staff and other health professionals as notes from patients of WH kept outside of WH patient histories or computer systems e.g. BOSSnet, EMR and iPM that are to be the source of information for research or quality assurance.

3. Responsibility

3.1 Western Health

WH supports and promotes good research practice through the provision of policy and procedures and infrastructure systems, Information Technology, Health Information Services (HIS) and Legal services.

The WH Office for Research procedures include requirements for:

- Justification and verification of the outcomes of research (via research application and reporting);
- Ownership, stewardship and control of research Data;
- Storage, retention and disposal of research Data;
- Safety, security and confidentiality of research Data.

The WH Office for Research will keep a register of Databanks and registries used for future and ongoing research purposes.

3.2 Heads of Departments

Heads of Departments are required to:

- Take all reasonable steps to ensure on a regular basis that all staff and students under their jurisdiction who are conducting research are aware in advance of their obligations under this guideline and other relevant Data policies and procedures provided on the Western Health Website and to ensure that their practices conform to these and other applicable guidelines.
- Heads of Departments are also responsible for ensuring that research data within their department are kept according to these guidelines and must keep a register of research Databanks that are held in their department;
- Ensure access to suitable physical and electronic storage for research Data that meets security and confidentiality requirements.
- Facilitate processes within the department and organisation for storage and retention of research Data.

3.3 Principal Investigators and members of Study Teams

All persons conducting research at WH or with WH Data are responsible for conducting research with integrity and in accordance with the WH Research Code of Conduct (2023) and other applicable requirements applicable to the use of health, business or personal information. All researchers must be familiar with the institutional policies related to research specific standards and the management of Data and information.

Principal Investigators and members of the study team are required to:

- Maintain adequate, clear and accurate records of study methods, source data/documents (including for clinical trials, all pertinent observations on each of the site's trial participants) and study records including any approvals granted, during and after conduct of the study
- Manage research data and source materials according to ethical approvals, legislative, organisational and any other applicable requirements;
- Ensure that appropriate research data and source materials are maintained to ensure accurate reporting and justify research outcomes, and to defend the findings of the research if challenged;
- Ensure the accuracy, completeness, legibility, and timeliness of the data in project documents and in all required reports;
- Ensuring that source documentation meets applicable GCP requirements, see "WH GCP SOP 007 Case Report Forms Source Documents Record Keeping and Archiving" on WH Office for Research website for more guidance;
- Ensure that research data and source materials are maintained in a safe and secure environment, and that Research data is stored in a retrievable manner;
- Ensure backup, archival and monitoring activities are in place to prevent loss on research data;
- Ensure that the researchers have planned for ongoing custodial responsibilities for the research data if they leave the organisation
- Maintain confidentiality of research data and source materials when given access to confidential information;
- Ensure that destruction of and research data and source materials occur only after minimum retention periods have been completed.
- Ensure that all members of the study team, including students and third parties were applicable, are aware of their responsibilities in relation to the management of research data and source materials; and
- Supervise staff, students, honorary appointees or and third parties where applicable, delegated tasks on research studies or quality assurance projects.

4. Authority

Manager, WH Office for Research

5. Associated Documentation

In support of this guideline, the following Manuals, Guidelines, Instructions, Guidelines, and/or Forms apply:

Name

Information Privacy

Record Keeping

Intellectual Property and Moral Rights

Research and Ethics

Western Health Databank Registration FORM (associated form)

Photography and Video Images

Corporate Document Management

Management of Patient Clinical Records

Patient Clinical Records Documentation

WH Good Clinical Practice (GCP) Standard Operating Procedures 007

WH Research Code of Conduct 2023

NHMRC Management of Data and Information in Research: A guide supporting the Australian Code for Responsible Conduct of Research 2018

NHMRC National Statement on Ethical Conduct in Human Research 2007 (updated 2018)

6. Credentialing Requirements

NIL

7. Definitions and Abbreviations

7.1 Definitions

Definitions For purposes of this guideline, unless otherwise stated, the following definitions shall apply:

Data/Information	Data are pieces of information, facts, observations or experiencers on which an argument, theory or test is based. This information, regardless of format, is obtained directly or indirectly for research purposes and is information that may be used for research purposes. For example: • Information obtained directly from a person in interview, questionnaire, focus groups, personal and medical histories, demographics, biographies, audiotape, audio-visual records, photographs; • 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; • Information derived from human tissue such as blood, bone, muscle, organ and waste products, including genetic and radiological information.
Databank/Database	The terms databank and database are considered to have the same meaning. A databank is a collection of data or information, as defined above. It may be stored on paper and kept in files in a lockable filing cabinet, in a secure office with controlled access in the department in which the research or stored electronically and kept on WH SharePoint or REDCap only accessible to authorised staff. A databank may be established with the intent to use the information contained within for a use other than research such as disease surveillance, trend identification and the stimulation of ideas for possible future research. It is foreseeable at some future point in time that such databanks may be useful for future research. While most data are collected, aggregated and stored for a single purpose or activity. Permission may sometimes be sought from participants to 'bank' their data for possible use in future research projects. Therefore such databanks are subject to these guidelines.
Personal Information	Information or opinion that can be used to personally identify an individual
Human Research Ethics Committee (HREC)	A body which reviews research proposals involving human participants, their data and tissues to ensure that they are ethically acceptable and in accordance with relevant standards and guidelines. The National Statement 2007(updated 2018) requires that all research proposals involving human participants be reviewed and approved by an HREC and sets out the requirements for the composition of an HREC.
Low Risk Ethics Panel (LREP)	A body which reviews low & negligible risk research proposals involving human participants and their data to ensure that they are ethically acceptable and in accordance with relevant standards and guidelines. The National Statement 2007(updated 2018) (requires that all research proposals involving human participants be reviewed and approved by an ethics committee.
Registry	A registry is a systematic observational collection of health-related information from patients. The primary purpose of a registry is to evaluate specified outcomes for a population categorized by a particular condition or disease to serve clinical or scientific purposes. Clinical registries are databases that systematically collect health-related information within an overall governance and management structure on individuals who are: • treated with a particular surgical procedure, device or drug, e.g., joint replacement; • diagnosed with a particular illness, e.g., stroke; or • managed via a specific healthcare resource, e.g., treated in an intensive care unit

7.2 Abbreviations

For purposes of this procedure, unless otherwise stated, the following abbreviations shall apply:

AI	Associate Investigator
EMR	Electronic Medical Records
GCP	Good Clinical Practice
HIS	Health Information Services
HREC	Human Research Ethics Committee
ICH	International Conference on Harmonisation
LREP	Low Risk Ethics Panel
NMA	National Mutual Acceptance
PI	Principal Investigator
REDCap	Research Electronic Data Capture
SOP	Standard Operating Procedure
QA	Quality Assurance
WH	Western Health

AI	Associate Investigator
EMR	Electronic Medical Records
GCP	Good Clinical Practice
HIS	Health Information Services
HREC	Human Research Ethics Committee
ICH	International Conference on Harmonisation
LREP	Low Risk Ethics Panel
NMA	National Mutual Acceptance
PI	Principal Investigator
REDCap	Research Electronic Data Capture
SOP	Standard Operating Procedure
QA	Quality Assurance
WH	Western Health

8. Guideline Detail

8.1 Introduction

These guidelines are in accordance with the *National Statement on Ethical Conduct in Human Research 2007(updated 2018), the Australian Code for the Responsible Conduct of Research (2018*), Australian laws and the *International Conference on Harmonisation (ICH) Guidelines for Good Clinical Practice (GCP) (2016)*.

The principles set forth in the *Privacy and Data Protection Act (2014)*, Health Records Act (2001), *Health Privacy Principles*, *National Statement on Ethical Conduct in Human Research 2007(updated 2018)and the Australian Code for the Responsible Conduct of Research (2018)*, allow for and encourage research using information obtained in the course of the provision of health care. It is important that data can be used in research to improve knowledge of diseases and to develop treatments and potential cures. Similarly, institutions should conduct quality assurance to improve their practice and it is expected that some information will be used for such purposes.

Researchers should be familiar with the WH policies: *OP-CM3 Information Privacy* and *OP-CM5 Record Keeping*, which outlines the obligations of staff when dealing with personal, business, sensitive and health information. WH takes its privacy obligation very seriously and a breach of *OP-CM3 Information Privacy* may have serious consequences. Further in the case of information used in research, a breach may constitute research misconduct, see *WH Research Code of Conduct (2023)*.

Good Data management is important to ensure Data integrity throughout the entire Data lifecycle including:

- Identification of relevant Data to be collected for a study;
- Data collection;
- Disclosure of Data to collaborators;
- Data storage, including Databanks and registries;
- Use/reuse of Data (including disclosure to external parties after publication etc.); and
- Destruction of Data.

Research staff should plan Data management requirements and processes for each study as soon as the study planning activities begin i.e. with the start of protocol development or on approach by a sponsor for a feasibility review. Data management should protect the rights, safety, and well-being of the research participants and the wider community and be in accordance with this guideline and other WH requirements. It is recommended that department business areas complete a Privacy Impact Assessment (https://ovic.vic.gov.au/privacy/for-agencies/privacy-impact-assessments/). For guidance and review of data management plans, contact the WH Corporate Records Manager.

Also see *WH GCP SOP 007 Case Report Forms Source Documents Record Keeping and Archiving*, *OP-CM3 Management of Patient Clinical Records*, *OP-CM3 Patient Clinical Records Documentation* and the *OP-CM5 Corporate Document Management* for further guidance.

Researchers must ensure the integrity of their research. Research data must be accurate, complete, authentic and reliable. Research data should be recorded in a form that is adequate for verification of research results. As data may need to be reviewed for the verification of results and reference some time into the future, data must be stored in a durable and secure format. Researchers who use electronic storage should only use WH SharePoint or REDCap to ensure backup of storage through the WH system. No external hard drives, USBs or personal storage solutions (e.g. Dropbox, Google Drive) can be used.

Data related to publications must be available for discussion with other researchers. Where protection of participants privacy applies, as is the case in research involving participant's or the use of participant's data in health-related research, the data must be kept in re-identifiable (coded) or non-identifiable format.

WH and researchers have a responsibility to ensure that information is used appropriately. This means that consent has been obtained where it is inappropriate to use the information without consent; that data are secured to ensure privacy and that data are stored for the required length of time and subsequently destroyed in an appropriate manner.

All research that proposes to collect, use or disclose data as described above, must be submitted to the relevant HREC, LREP or WH Office for Research as appropriate for review. The exceptions to this rule are projects that involve the use of data that are non-identifiable and meaningless in their state, for example, unlabelled EEG brain wave reading data.

Quality Assurance (QA) and Clinical Audit projects that involve the use of data must be submitted to the WH Office for Research.

8.2 Ownership

All data and databanks that exist within WH are considered to be owned by WH. In projects that are conducted across institutions, an agreement should be developed at the beginning of the project covering the ownership of data and databanks.

Subject to any written agreements, WH will remain the custodian of study research Data, Meta Data, Research Results, Primary Materials and Intellectual Property. Refer to policy: *Intellectual Property and Moral Rights*.

As a general rule, data retained at the end of a project are the property of WH. However, ownership of the research data may be negotiated with another institution. It is also noted that ownership of data may also be influenced by the funding arrangements for the project.

8.3 Databanks and registries

8.3.1 Departmental Register of Databanks and registries

- Heads of Departments are responsible for ensuring that a detailed department register of all research data and databanks/registries created and existing in their department is kept. The Department Head must appoint/nominate a Data Co-ordinator to manage the department's register of databanks. This register should include active and archived projects and should specify the following:
  - The ethics approval reference number of the project and/or the name of the databank/registry;
  - The location of the databank (including the network location of electronic databanks);
  - A description of the data, and how data are labelled;
  - Security arrangements;
  - The name of the databank custodian;
  - The names of the researchers and any others who are authorised to access the data;
  - The ethics approval reference number of any project that has used data from this databank;
  - The date when the project ends and can be archived;
  - The date of any publication that the data relate to (where applicable);
  - The proposed date of destruction of the data;
  - Authorisation for destruction;

- The actual date of destruction.
- This register may also be used to register all research records that are associated with research related to the databanks, e.g. Investigator files that should also be kept as above.
- The appointed data co-ordinator must ensure that this register is kept up to date.
- This register should be kept on WH SharePoint, contact Corporate Records to set up.
- The WH Office for Research will keep a register of Databanks/Registries used for future and ongoing research purposes.

8.3.2 THE REDCap Database

- REDCap is a secure web application that can be used to collect virtually any type of data. Other by exception provided by the WH Office for Research, 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.
- From 01 July 2020, data for all WH initiated projects (WH Investigator Lead Clinical Trials, Low Risk Research and Quality Assurance projects) must be stored on the Western Health REDCap account. To obtain a login please contact Mr Frank Pham REDCap Administrator at Performance Unit by email on frank.pham@wh.org.au.
- Each project owner is responsible for setting up the project on REDCap by requesting a REDCap account via the REDCap Administrator. The project owner can request that additional research staff be afforded access to contribute to the REDCap project based on the following considerations:
  1) Only certain staff to be given permission to add, delete and amend the project details;
  2) Only certain staff to be given restricted access confined to data entry only.
- It is strongly recommended that external staff (i.e. that are not WH employees) not to be granted REDCap permission to delete data or projects and that such permission be restricted to the core WH members of the research team. With the exception of organisational appointed academic positions such as a Chair in a defined discipline and their nominated and authorised project team member/s.
- All WH REDCap projects will need to adhere to the guiding principles defined in the *WH Research Code of Conduct (2023)* and will be governed by the applicable policies and procedures that apply to the conduct of research in Australia.
- In collaborative research where WH Data are stored on REDCap housed at another organisation, data management and ownership details should be described in the research protocol and be agreed to by an appropriate research agreement. The guiding principles of the *WH Research Code of Conduct (2023)* will still apply to these projects as well.
- For further information on the use of REDCap refer to the WH Office for Research website or contact the REDCap Administrator.

8.3.3 Registration of Clinical and Research Databanks/Registries at Western Health

- All research databanks/registries that exist or are created by WH Staff and others accessing WH facilities must be registered with the WH Office for Research.
- At WH, the primary purpose for collection of data from or about individuals is usually for the provision of a health care service. Examples of such databanks are: Health Information Services, BOSSnet, EMR, iPM, Pharmacy dispensing databanks, etc.
- Clinical Databanks that already exists within the organisation can and should be registered with the WH Office for Research if they are also being used for research, by completion and submission of the *Western Health Databank Registration Form.*
- Secondary purposes for collection of data from or about individuals would be purposes such as for research, quality assurance, disease surveillance. Examples of such databanks are:
  - Data pertaining to the illness, health history, testing and treatment of patients of WH;
  - Data pertaining to the services provided to individual patients by WH and/or their opinion of the care they received;
  - Data pertaining to WH employees and/or their experiences related to working at WH.
- Databanks/Registries for a specific research project can be registered as part of the initial submission for approval of the research project by completion and submission of the *Western Health Databank Registration Form* with their application.
- New databanks that an employee wishes to create, for future unspecified research projects, e.g. a databank to be used for disease surveillance, must be submitted for approval, to the appropriate HREC/LREP and the WH Office for Research, as a research project in itself. The application must include the *Western Health Databank Registration Form.*

8.3.4 Databank/Registry Custodian

- Heads of Departments are responsible for ensuring that all databanks within their department have a nominated databank custodian. Heads of Departments must review the position of databank custodian when staff leave or move within their department.

- All databanks must have an appointed databank custodian. The role of the data custodian is to ensure that the databank is created, used, accessed, stored and destroyed in accordance with this document. Any laws, codes of practice, contractual agreements that apply must be in line with the requirements stated in the original application for approval, submitted and approved by the HREC/LREP and the WH Office for Research.
- The databank custodian should be chosen, taking into consideration their role in relation to the databank. In the case of research this will normally be the Principal Investigator (PI), however, in the case of student researchers and QA projects the most appropriate person may be the Department Head. In some circumstances departments will have existing clinical databanks, which were not created as part of a single clinical study. In such cases the Department Head may be the appropriate person to be the Databank Custodian. Alternatively the Department Head may appoint an appropriate person to be the data custodian of the databank.
- In the case of new research projects and quality assurance projects creating a databank for future unspecified research (not just a single project), PIs should submit a WH Databank Registration Form with their submission of the project to the appropriate ethics committee/panel and the WH Office for Research for review.
- In the case of existing clinical databanks the databank custodian should complete and submit a *Western Health Databank Registration Form* to the WH Office for Research if they are to be used for research.
- The databank custodian must provide the data co-ordinator of their Department Register with a copy of the completed *Western Health Databank Registration Form.*

8.3.5 Requests to use a Databank/registry

- The databank custodian is the person to whom requests to use the databank should be made. The data custodian must ensure that the proposed disclosure and use of the data is appropriate, meets the requirements of these guidelines. To do so, the data custodian of a databank must have access to the original consent forms that were signed by participants. In cases where the HREC waived the requirement for consent, the data custodian must have access to the original ethics submission and approval letter to be able to assess the access.
- Once the database custodian has approved the use of the databank and the new research project is approved by the HREC/LREP and the WH Office for Research, the database custodian can allow access to the researchers.

8.4 Data Breaches

Data breaches include:

- The collection, use, disclosure and storage of data as defined above without consent or the HREC providing a waiver of the need for consent. NB. This may also constitute research misconduct. Refer to the *WH Research Code of Conduct (2023)*
- Inappropriate destruction of data;
- Loss of data, for example: the researcher, PI or data custodian being unable to locate the whereabouts of a paper file or an electronic storage device on which data is held;
- The removal of identified data from the WH premises.

PIs/databank custodians must report any data breaches to the Head of the Department and to the WH Office for Research as soon as it becomes known.

Data breaches may also result in privacy breaches, WH takes its privacy obligation very seriously, and a breach to the policy: *Information Privacy* may have serious consequences.

Further in the case of information used in research, a breach may constitute research misconduct.

8.5 Consent

In most cases where data is to be collected, used, stored or disclosed for the purposes of research, consent for the use of the data, either written, verbal or implied as appropriate, **is required**.

Generally, information must only be used in ways agreed to by those who have provided the information. To promote access to data kept in a databank, consent should be obtained in such a way that will allow the use of the data in the future. When considering approval of a project using data already collected and in a databank the HREC/LREP will review the application in view of the consent that was given for the information to be added to the database.

When collecting data for deposit in a databank, researchers should provide to the participant clear and comprehensive information about:

- The form in which the data will be stored, (identifiable, re-identifiable, non-identifiable);
- The purposes for which the data will be collected, used and or disclosed;
- Whether the data may be kept and potentially used in future research and indicate the type of future research;

- Whether the data may be destructed and how will be destructed.
- The details of protection of the individual's privacy in any publication;
- How an individual can gain access to their data.

In some cases, the requirement for consent may be waived only by a HREC. Consent may be waived when the researcher can demonstrate one of the following:

- The data will be secured to ensure protection of privacy and their use carries a low risk. For example, non-identifiable data that are not of a sensitive nature;
- The research has scientific merit and it is likely that the individual is deceased and obtaining consent from the individual's next-of-kin may cause undue distress;
- The benefits from the research justify any risk associated with not seeking consent and it can be demonstrated that it is not possible or it is impractical to obtain consent from the individuals' whose information it is;
- There is no likely reason for thinking that participants would not have consented if they had been asked.

Note: Researchers should be aware that data stored in an identifiable form cannot be used in research that is exempt from ethical review.

Consent forms (and copies of), by their nature, contain identifiable data. Where applicable, original consent forms must be filed in patient medical records. All other consent forms (and copies of), that is, where participants are not patients of WH, must be kept in files preferably in a lockable filing cabinet, in a secure office with controlled access in the department in which the research is conducted and separately from the collected research data for that project.

8.6 Identification of Data

Researchers given access to confidential information must maintain confidentiality. Researchers should include in their protocol a plan for the protection of participants' privacy. Data can be labelled as:

- **Identifiable**
  Where the identity of an individual can reasonably be ascertained. Examples of identifiers include individuals' names, photos, UR numbers, and address.
- **Re-identifiable**
  Data from which identifiers have been removed and replaced by a code. It remains possible to re-identify a specific individual by, for example, using the code or linking different data sets.
- **Non-identifiable**
  Data that have never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can ever be identified. A subset of non-identifiable data is one that can be linked with other data so it can be known that they are about the same data participant, although the person's identity remains unknown.

Most data can maintain their integrity without the use of identifiers therefore, data should not be kept in an identifiable state. A researcher or databank custodian who believes that data must be kept in an identifiable state must justify 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.

Researchers should consider that although, during data collection, it may be necessary to keep a databank 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. For example, it may be necessary to identify data from a survey of patients if that data needs to be cross-referenced with medical information held in the patient's medical records. However, once the survey data has been cross-referenced the database should then be made, at least, re-identifiable (coded) or preferably non-identifiable.

Researchers and databank custodians must 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 must be kept in a re-identifiable manner to ensure the new information can be provided to the individual.

8.7 Access, Use and Disclosure of Data

Within the setting of a current research study, data must only be used for the purpose/s declared to the participants in the participant informed consent form or the participant information sheet. Similarly, disclosure of data must only be made to other people and /or organisations as declared in the participant information and consent form.

Disclosure of data is defined as allowing persons other than those who have access to the data for the purpose of the approved research study for which it was collected, access to the data. Those who would be expected to have access to the data would include, the PI, Associate Investigators, and Study Co-ordinators and associated administrative staff for the particular study for which the data was collected.

Data collected for a study, cannot then be accessed or used for another study without further approval from the HREC/LREP and the WH Office for Research.

In studies where an approving HREC has waived the requirement for consent, data may only be used for the purposes stated to the approving HREC in the study submission.

If during or after a study a new use for the data is identified that was not previously identified and declared when the study was approved by the HREC/ LREP and WH Office for Research, the researcher must apply to the WH Office for Research, for approval to use the data in the new way.

If a researcher wishes to access and use a databank they must seek the approval of the databank custodian. Evidence of this approval must be included in the submission of the project for approval, to the relevant HREC/LREP and the WH Office for Research.

In the event of legal action, research data and records may be accessed by WH and its legal counsel or delegated representatives to determine their relevance to any litigation and, if relevant, removed for use in the litigation. Research data are subject to subpoena including confidential research data and records.

Under the *Freedom of Information Act 1982 (Vic)*, WH is required to allow persons access to documents which are in WH's possession under defined circumstances. Further information should be obtained from the Freedom of Information Officer before any such access is given.

8.8 Data Storage and Security

All study team members are responsible for maintaining data in a secure manner and allowing only appropriate, approved access to the study data.

Heads of Departments are responsible for providing storage space for research data that meets security and confidentiality requirements. Whilst a project is active this space should be provided within the department where the researcher works.

Researchers must be responsible for ensuring appropriate security for confidential information. Where computing systems are accessible through networks, particular attention to security of confidential data is required. Security and confidentiality must be assured in a way that copes with multiple researchers and the department of individual researchers.

For the protection of peoples' privacy all data must be kept securely. The key to the code for re-identifiable data must be kept separately to the databank. An electronic re-identifiable databank and its associated key to the code may be kept on the same computer; however, they must be stored in separate password-protected files.

The storage, retrieval and disposal of records must be conducted in accordance with the policy: *P-CM3 Information Privacy Policy*, or the procedure: *OP-CM5 Corporate Document Management*, and as applicable to your particular research project.

8.8.1 Paper Records/Databanks

- 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.
- When storing for archiving, they must be set offsite to WH approved offsite provider. Contact Corporate Records for details.
- Paper records MUST:
  - Not be removed from WH 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.

8.8.2 Electronic Data/Databanks

- Electronic data storage should be managed to ensure secure access, storage and retrieval of data in all stages of the study (including archiving) and prevent data breaches or losses. The primary site of electronic data storage is on WH SharePoint and REDCap (from 01 July 2020).
- Benefits of storing electronic research information on the WH SharePoint include:
  - Security management – registered access of users, maintenance of firewalls, etc.
  - IT support.
  - Tracking of history of access and edits to ensure version control and monitoring.
  - Backup and retrieval of data to maintain data integrity.
  - Compliance with WH requirements.
- Research data should not be captured, managed and stored on portable devices. It is highly recommended to use ShareFile for transferring data externally, contact Corporate Records for guidance. Only if deemed necessary should certain data be transferred and saved on portable devices such as: USB, portable computer or mobile phone. If data is to be temporarily stored on portable devices, the following must be adhered to:
  - Device must be password protected.
  - Only the minimum data required to perform the intended activity should be downloaded into a portable device
  - All data on portable devices must be re-identifiable (coded) or non-identifiable data.
  - Portable devices must not contain patient master identifier code list or any other information that could facilitate the identification of patients. This master identifier code list must not leave WH premises.
- All data should be properly deleted from the portable device once its use has been fulfilled.

8.8.3 Audiotape and Audio-visual Records, Photographs

- Data kept in this form must be stored in lockable storage facilities in the researcher's work area or department in a lockable office. Audio-visual data should be kept in a re-identifiable or non-identifiable state, however by their very nature they may remain identifiable and if so they must be treated as identifiable and strict security and precautions to ensure confidentiality must be taken. Also see procedure: Photography and Video Images for further information on WH procedures.

8.9 Removal or Movement of Data

Identifiable data must never leave WH premises. If a researcher wishes to move a databank or data from the premises it should be made re-identifiable or non-identifiable prior to leaving the premises.

In the event of a researcher or databank custodian leaving WH, they may negotiate with the Head of Department to take copies of non-identifiable or re-identifiable research data (but not the key to the code) and records with them, but original data and records are to remain in the department. Any future use of such data in research would still require the approval of the original approving HREC/LREP and the WH Office for Research.

Research data, including de-identified data, should not be shared through non WH data sharing accounts. Email, Dropbox and Google Drives are not WH approved applications for sharing de-identified research data. WH SharePoint should be used internally and WH ShareFile should be used for sharing data externally.

8.10 Archiving

Heads of Departments are responsible for providing or arranging secure archival storage.

In Victoria, the minimum recommended period of retention of health information is 7 years after the last occasion on which a health service was provided to the individual (*Health Records Act (2001)*). The minimum recommend period of retention of research data is 5 years from the date of publication – whichever is the later.

Documentation should be maintained as specified in the *Australian Code for Responsible Conduct of Research 2018 (Management of Data and Information in Research, Section 2.3)* as indicated below:

- For short term research projects, that are for assessment purposes only (e.g. research projects completed by students), retention of research data for 12 months after completion of the project may be sufficient.
- Study documentation should be maintained for a minimum of 15 years for adult studies or 25 years for paediatric studies after trial closeout.
- For areas such as gene therapy, research data must be retained permanently (e.g. patient records).
- If the work has community, cultural or historical value, research data should be kept permanently, preferably within a national collection. Permanent records will need to be transfer to Public Record Office Victoria, contact Corporate Records to assist.
- If results from research are challenged, all relevant data and materials must be retained until the matter is resolved.

The requirements outlined above are the minimal requirements for storage. Funding bodies may have specific requirements for retention of data and records. Researchers should be aware of any conditions of any award or obligations of contracts supporting their research.

If a legal action is taken involving a research project, all data and records must be kept until after all avenues of legal action have been exhausted.

Consideration should be given to the long term preservation of research data and records of archival value. For example, projects:

- That made a major contribution to research;
- That were controversial, challenged, subject to extensive debate or interest;
- That involve the use of major new or innovative techniques;
- That involves a "first of a kind" process or product or significantly improved or changed procedures.

8.11 Destruction of Data

The destruction of research data must only be authorised by the Head of Department and must be destroyed according to WH Corporate Records destruction guidelines. The Head of Department should liaise with the data co-ordinator/department data manager of the department register and the databank custodian to establish that it is appropriate to destroy the documents as per WH Corporate Records requirements.

A record of approval for destruction must be recorded on the departmental register and notification of the destruction should be forwarded to the WH Office for Research and WH Corporate Records.

When data are destroyed this should be done so in such a way as to ensure complete destruction of the information:

- Data stored in a paper format should be shredded;
- Data stored in an electronic form should be destroyed by rewriting or reformatting. "Delete" instructions are not sufficient to ensure that all systems pointers to the data incorporated in the system software have also been removed;
- Audio-visual tapes should be destroyed by "magnetic field bulk eraser".

At the time of destroying data, researchers should ensure that they employ the most effective method since this may change over time with technological advances.

9. Document History

Number of previous revisions: 1

Previous version dates: July 2020

Minor amendment: not applicable this version

10. References

- National Statement of Ethical Conduct in Human Research (2018 and updates)
- Australian Code for Responsible Conduct of Research (2018)
- Western Health Research Code of Conduct (2023)
- Western Health Information Privacy Policy
- Western Health GCP SOP 007 Case Report Forms Source Documents Record Keeping and Archiving
- Western Health Intellectual Property and Moral Rights
- Western Health Management of Patient Clinical Records
- Western Health Patient Clinical Records Documentation
- Western Health Corporate Document Management Procedure
- Western Health Photography and Video Images
- ICH Guidelines for Good Clinical Practice (GCP) 2016

- The Health Records Act 2001 (Vic)
- The Health Records Act 2001 (Vic) - Health Privacy Principles
- Statutory Guidelines on Research issued for the purposes of Health Privacy Principles 1.1(e) (iii) & 2.2(g) (iii). Feb. 2002.
- The Privacy Act 1988 with amendments up to Act No.159,2001 Commonwealth including the National Privacy Principles
- Privacy and Data Protection Act 2014 (Vic)
- The Public Records Act 1973
- The Freedom of Information Act 1982 (Vic)

11. Sponsor

Research Program Director, Western Health

12. Authorisation Authority

Chief Medical Officer, Western Health

Appendix 1

Western Health

WESTERN HEALTH DATABANK REGISTRATION FORM

Refer to *OG-GC7 Data Management in Research*

All research databanks that exist or are created at WH for future unspecified research projects must be registered with the Office for Research. Please complete this Databank Registration Form and all relevant documentation to ethics@wh.org.au. Contact the Office for Research for any queries.

Date: Select date	**Databank Reference** (Office Use):
Project Number: (where applicable)	E.g. 41234; HREC/18/WH/123; QA2018.123
Name of Databank:	Enter text
Data Custodian:	Enter text
Department Name:	Enter text
Type of Databank:	☐ Electronic ☐ Hardcopy

1. Purpose

For what research purposes is the databank used? List any project for which the databank is used to either source information or to store information.

Enter text

2. Timelines and Retention

a. **When was this databank set up:**	Enter text
b. **Is the intent to keep this databank indefinitely?** If No, complete c & d below:	☐ Yes ☐ No
c. **Anticipated date of when this databank will be closed:**	Enter text
d. **Describe how databank will be archived/destroyed:**	

Enter text

3. Location of Databank (Complete all that apply)

Electronic network location:	Enter text
Hardcopy storage location:	Enter text

REDCap: ☐ Yes ☐ No*

If yes, ensure WH REDCap account and login requests are made to Bill.Karanatsios@wh.org.au
*Required from 01 July 2020

4. Identification of Data

☐	**Identifiable** (Labelled with identifiers such as name, UR number, DOB, contact details) If identifiable, please clarify why data is in identifiable form
	Enter text
☐	**Re-identifiable** (Coded using a numbering system that is unique to this project e.g. 001. The key to the code is kept in a separate secure file) If re-identifiable, describe coding process and storage of master identifier list?
	Enter text
☐	**Non-identifiable** (All links with the source of the data are permanently broken and it is not possible to link the data with the data source)

5. Security *Refer to Information Privacy Policy (P-CP2.1) & Corporate Document Management Procedure (OP-IM2.2.1)*

Please describe the security system to protect the information on the databank and to maintain confidentiality and access for electronic and/or hardcopy files.

Enter text

6. Consent