

NAME OF DEPARTMENT	RESEARCH DIRECTORATE
NAME OF DOCUMENT	Data Management in Research
NUMBER	18.2
ASSOCIATED MELBOURNE HEALTH POLICY	Research Policy
DATE OF ISSUE	12 November 2007
REVISION NUMBER	2
FUNCTIONAL GROUP	Research Directorate
DIVISIONAL SPONSOR	Executive Director Of Research
ACHS EQUIP CRITERIA	<p>Standard 2.5 – The organisation encourages and adequately governs the conduct of health and medical research to improve the safety and quality of health care.</p> <p>Criterion 2.5.1 – The organisation’s research program promotes the development of knowledge and its application in the healthcare setting, protects consumers/patients and manages organisational risks associated with research.</p>
SUMMARY	<p>The Guidelines for Data Management in Research have been developed to set out the responsibilities of Melbourne Health staff and others using Melbourne Health resources in conducting research involving the collection, use, disclosure, storage and destruction of information. The document sets forth the role and responsibility of MH staff and others using data collected from MH so that research complies with the <i>National Statement on Ethical Conduct in Human Research (2007)</i>, <i>The Australian Code for the Responsible Conduct of Research (2007)</i> and State and Commonwealth privacy laws and principles.</p>

1. ASSOCIATED POLICY

Research Policy

2. PURPOSE AND SCOPE

Melbourne Health, as an institution where research is conducted must have guidelines for data management in research. These guidelines fulfil this requirement. The Guidelines for Data Management in Research have been developed to set out the responsibilities of Melbourne Health Staff and others using Melbourne Health resources in conducting research involving the collection, use, disclosure, storage and destruction of information in research.

These guidelines govern the collection, use, storage, disclosure and destruction of information (data) in human research. They also govern the creation and use of databanks in research. Further they govern the use of information that has previously been collected and stored in a database for a primary purpose other than research that researchers wish to access, or may wish to access in the future, for research purposes. These guidelines also apply to quality assurance activities.

These guidelines cover research and quality assurance projects approved by the Human Research Ethics Committee and the Mental Health Research and Ethics Committee.

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 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 MH kept outside of MH patient histories or computer systems eg. Homer and CIS, that are to be the source of information for research or quality assurance.

3. DEFINITIONS

<p>Data:</p>	<p>Data is information obtained directly or indirectly for research purposes and information that may be used for research purposes. For example:</p> <ul style="list-style-type: none"> • Information obtained directly from a person in interview, questionnaire, focus groups, personal and medical histories, demographics, biographies, audiotape, audiovisual 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.
<p>Databank:</p>	<p>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 or stored electronically and kept on a hard drive or on disk.</p> <p>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. Therefore such databanks are subject to these guidelines.</p>
<p>REC – Research Ethics Committee</p>	<p>This term is used throughout this document to indicate the Melbourne Health Human Research Ethics Committee and/or the Melbourne Health Mental Health Research and Ethics Committee as appropriate.</p>

--	--

4. RESPONSIBILITIES

The Research Directorate will keep a register of Databanks used for research purposes.

Heads of Departments are responsible for ensuring that staff and students under their supervision who are conducting research are aware of their responsibilities to ensure that their practices conform to this policy.

Heads of Departments are responsible for ensuring that Databanks within their department are kept according to these guidelines and must keep a register of Databanks that are held in their department.

5. GUIDELINES

5.1 INTRODUCTION

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

The principles set forth in the Health Records Act 2001, Health Privacy Principles, *National Statement on Ethical Conduct in Human Research (2007)* and the *Australian Code for the Responsible Conduct of Research (2007)*, 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. It is expected that some information will be used for such purposes.

Researchers should be familiar with the Melbourne Health Privacy Policy, which outlines the obligations of staff when dealing with personal, sensitive and health information. Melbourne Health takes its privacy obligation very seriously and a breach of the Privacy Policy may have serious consequences. Further in the case of information used in research, a breach may constitute research misconduct.

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 ensure a backup either in a paper form or storage on a secondary secure storage device.

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 fashion.

Melbourne Health and researchers have a responsibility to ensure that information is used appropriately. That is that consent is 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 Human Research Ethics Committee or the Mental Health Research and Ethics Committee 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 projects that involve the use of data must be submitted to the Research Directorate for review as per the [Melbourne Health Review of Quality Assurance Projects Procedure](#).

5.2 OWNERSHIP

All data and databanks that exist within Melbourne Health are considered to be owned by Melbourne Health. 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. As a general rule, data retained at the end of a project are the property of Melbourne Health. 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.

5.3 DEPARTMENTAL REGISTER OF DATABANKS

Department Heads are responsible for ensuring that a department register of all databanks created and existing in their department is kept. The Department Head must appoint a co-ordinator of the department register. This register should include active and archived projects and should specify the following:

- The HREC/MHREC/QA number of the project and/or the name of the databank;
- The location of the databank (including the asset number of the computer for electronic databanks);
- A description of the data, and how data are labelled;
- Security arrangements;
- The name of the databank trustee;
- The names of the researchers and any others who are authorised to access the data;
- The HREC/MHREC,QA 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, eg. Investigator files that should also be kept as above.

The co-ordinator must ensure that this register is kept up to date and must provide a copy to the Research Directorate annually as requested.

5.4 REGISTRATION OF DATABANKS AT MELBOURNE HEALTH

All databanks that exist or are created by Melbourne Health Staff and others accessing Melbourne Health facilities must be registered with the Research Directorate.

At Melbourne Health, 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, CIS, HOMER, Pharmacy dispensing databanks, etc.

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 Melbourne Health;
- Data pertaining to the services provided to individual patients by Melbourne Health and/or their opinion of the care they received;
- Data pertaining to Melbourne Health employees and/or their experiences related to working at Melbourne Health.

Databanks for research can be registered as part of the initial submission for approval of the research project by completion and submission of the MELBOURNE HEALTH DATABANK REGISTRATION FORM (Appendix A).

Databanks that already exists within the organisation can and should be registered with the Research Directorate by completion and submission of the MELBOURNE HEALTH DATABANK REGISTRATION FORM (Appendix A).

New databanks that an employee wishes to create, for a purpose other than for a specific research project, e.g. a databank to be used for disease surveillance, must be submitted for approval, to the appropriate REC, as a research project in itself. The application must include the MELBOURNE HEALTH DATABANK REGISTRATION FORM (Appendix A).

5.5 DATABANK TRUSTEE

Department Heads are responsible for ensuring that all databanks within their department have a nominated Databank Trustee. Department Heads must review the position of Databank Trustee when staff leave or move within their department.

All databanks must have an appointed Databank Trustee. The role of the trustee is to ensure that the databank is created, used, accessed, stored and destroyed in accordance with this policy any laws, codes of practice, contractual agreements that apply and in line with the requirements stated in the original application for approval, submitted and approved by the REC.

The Databank Trustee should be chosen, taking into consideration their role in relation to the databank. In the case of clinical research this will normally be the Principal Investigator, however, in the case of student researchers and quality assurance projects the most appropriate person may be the Department Head. In some circumstances departments will have existing databanks, that 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 Trustee. Alternatively the Department Head may appoint an appropriate person to be the Trustee of the databank.

In the case of new research projects and quality assurance projects, Principal Investigators should submit a Melbourne Health Databank Registration Form with their submission of the project to the appropriate REC.

In the case of existing databanks the Databank Trustee should complete and submit a Melbourne Health Databank Registration Form to the Research Directorate.

The Databank Trustee must provide the co-ordinator of the Department Register within their department with a copy of the completed Melbourne Health Databank Registration Form.

5.6 REQUESTS TO USE A DATABANK

The Databank Trustee is the person to whom requests to use the databank should be made. The trustee must ensure that the proposed disclosure and use of the data is appropriate, meets the requirements of these guidelines. To do so, the trustee of a databank must have access to the original consent forms that were signed by participants. In cases where the REC waived the requirement for consent, the trustee must have access to the original ethics submission and approval letter to be able to assess the access.

Once the Database trustee has approved the use of the databank and the new research project is approved by the REC, the Database Trustee can allow access to the researchers.

5.7 BREACH OF CONFIDENTIALITY

A breach of confidentiality is defined as:

- 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 MELBOURNE HEALTH Guidelines for Research Practice);
- Loss of data, for example: the researcher or database trustee 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 researcher's work premises.

A Databank Trustee must report a breach of confidentiality to the Head of the Department and to the Research Directorate as soon as it becomes known.

5.8 CONSENT

In most cases where data are 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 REC 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;
- The details of protection of the individual's privacy in any publication.

In some cases the requirement for consent may be waived 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.

NB. 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 histories. All other consent forms (and copies of), that is, where participants are not patients of Melbourne Health, 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.

5.9 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 in most cases Melbourne Health's policy is that data should not be kept in an identifiable state. A researcher or database trustee 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 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. 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 trustees 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.

5.10 ACCESS, USE AND DISCLOSURE OF DATA STORED IN DATABANKS

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 Principal Investigator, Co-investigators, Study Coordinators 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 REC.

In studies where an approving REC has waived the requirement for consent, data may only be used for the purposes stated to the approving REC 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 REC, the researcher must apply to the REC, for approval to use the data in the new way.

If a researcher wishes to access and use a databank he/she must seek the approval of the databank trustee. Evidence of this approval must be included in the submission of the project for approval, to the relevant REC.

In the event of legal action, research data and records may be accessed by Melbourne Health and its legal counsel 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), Melbourne Health is required to allow persons access to documents which are in Melbourne Health's possession under defined circumstances. Further information should be obtained from the Freedom of Information Officer before any such access is given.

5.11 DATA STORAGE AND SECURITY

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 files.

Paper Databanks

Data kept on paper must be stored in an appropriate filing system that is only accessible to authorised staff. Wherever possible, data should be kept in filing cabinets that can be locked when not in use. The data must be stored in an area that has controlled access and is lockable when staff are not in attendance.

Electronic Databanks

Data kept in an electronic form on a hard drive, mainframe or portable device must be protected by a password.

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

Re-identifiable databanks may leave the premises, however the key to the code must not leave the premises.

Audiotape and audiovisual records, photographs

Data kept in this form must be stored in lockable storage facilities in the researchers work area or department in a lockable office. Audiovisual 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.

5.12 REMOVAL OR MOVEMENT OF DATA

In the event of a researcher or Databank Trustee leaving Melbourne Health, 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 REC.

5.13 ARCHIVING

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

In accordance with state legislation and the *Australian Code for the Responsible Conduct of Research*, the minimum recommended period for retention of research data is 5 years from the date of publication. However in any particular case the specific type of research should determine the period for which data should be retained.

- For research in areas such as gene therapy, research data must be retained permanently. e.g. patient records.
- If the work has community or heritage value, research data should be kept permanently at this stage, preferably within a national collection. (Confidentiality issues would need to be addressed).
- Clinical trials data must be retained for at least 15 years from the end of the trial.
- Most quality assurance activity should be kept for 1 year from the completion of project. However if the project results are published, or the results are controversial or are the basis for a significant change in practice they should be kept for 5 years. There may be value in keeping some quality assurance project data for more than one year and up to or longer than 5 years. Advice should be obtained from the Research Directorate.
- All other research data should be kept for a minimum of 5 years.

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 involve a “first of a kind” process or product or significantly improved or changed procedures.

5.14 DESTRUCTION OF DATA

The destruction of research data must only be authorised by the Department Head. The Department Head should liaise with the coordinator of the department register and the databank trustee to establish that it is appropriate to destroy the documents as per this policy. A record of approval for destruction must be recorded

on the departmental register and notification of the destruction should be forwarded to the Research Directorate.

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;
- Audiovisual 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.

6. REFERENCES

- [National Statement of Ethical Conduct in Human Research 2007](#)
- [Australian Code for Responsible Conduct of Research 2007](#)
- [Melbourne Health Guidelines for Research Practice 2007](#)
- Melbourne Health Privacy and Confidentiality Policy
- 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
- The Information Privacy Act (VIC) 2000
- The Public Records Act 1973
- International Conference on Harmonisation – Guideline for Good Clinical Practice.1996 (ICH – GCP)
- Therapeutic Goods Administration Note for Guidance on Good Clinical Practice 2000.
- The Freedom of Information Act 1982 (Vic).

7. FURTHER INFORMATION

Contact the Office of the Research Directorate on 9342 8530 or email: research.directorate@mh.org.au

8. REVISION AND APPROVAL HISTORY

Date	Rev No	Author and approval
1/10/2007	First Draft	Angela Gray, Assistant Manager Research Directorate
12/11/2007	2	Angela Watt, Manager Research Directorate

MELBOURNE HEALTH DATABANK REGISTRATION FORM
(Appendix A: Guidelines for Data Management in Research)

1. HREC / MHREC / QA number: (where applicable)	
2. Trustee of the Databank: (Responsible person)	
3. Name of the Databank:	
4. Department:	
5. Type of Data bank – choose both if applicable	<input type="checkbox"/> Paper <input type="checkbox"/> Electronic

6. **Location** - describe exactly where the information is kept:

7. What data is stored on the databank? Personal Information (Eg. Name, UR no. Date of Birth etc) Health Information (Eg. Illness, treatment, test results etc.) Sensitive Information (eg. genetic information, infectious disease status etc.)

8. **Labelling of Data**

Please describe how the data is labelled:

- Identifiable** (Labelled with identifiers such as name, UR number, DOB, contact details)
- Re-identifiable** (Coded using a numbering system that is unique to this project eg. 001 The key to the code is kept in a separate secure file)
- 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)

- If identifiable please justify.
- If re-identifiable, is the key to the code kept in a different location to the database? Please describe.

9. **Security**

Please describe the security system to protect the information on the databank and to maintain confidentiality.

10. When was the databank setup?

11a. What is/was the original purpose of the databank?

11b. What was the source(s) of the data?

(E.g., Doctors notes, surgical reports, hospital medical records, test results, directly from those whose information it is). NB: Information may have been collected as part of routine care, for example, doctors' notes; surgical notes; for quality assurance activities; or for research etc. Please comment on your response.

11c. Consent

Was consent to add the information to the database sought from the person(s) whose information it is? Yes No

12. 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).

13. Are data still being added to the databank or is it closed? If closed state the date of closure.

14. Name all staff who presently have access to the databank

Name	Position

– add more rows if needed

15. Is it the intent to keep this databank indefinitely?

Yes No

15a. If No, when will the database be archived and/or destroyed? Please provide details of how it will be destroyed.

Signature of Trustee	
Date	