

Privacy Code
Manitoba Centre for Health Policy
November, 2002

The Manitoba Centre for Health Policy (MCHP) through the University of Manitoba acts as a trustee for anonymized health care administrative/statistical data from Manitoba Health and other agencies. The term anonymized means that the collecting agencies or groups have removed and/or encrypted individual-identifiable information before data are accepted into the repository. Use of the data are regulated under the Manitoba Personal Health Information Act (PHIA) and the Freedom of Information and Protection of Privacy Act (FIPPA). These Acts clarify the responsibilities of those groups that collect, administer and use health information.

MCHP has developed and implemented policies and procedures reflecting the legislative requirements in matters concerning the collection, administration, use and disclosure of personal health information. Even though the data are anonymized MCHP continues to apply the same standards that would be required if the data contained accessible personal identifiers under PHIA or FIPPA.

Research utilising data from the repository focuses on the secondary analysis of statistical/ administrative data. By design, such research does not include identifiable personal information, that is, information relating to a reasonably identifiable person (Tri-Council, 1998, p 3.2). Research using these data is appropriately considered as involving minimal risk (Tri-Council, 1998, p 3.5).

Population Health Research Data Repository

The Population Health Research Data Repository (PHRDR) is a comprehensive database developed to describe and explain patterns of care and profiles of health and illness. The repository contains encrypted anonymized files from the Ministry of Health (for example - data on hospital, physician, nursing home, home care and pharmaceutical use by Manitobans) as well as data from other agencies. Subsets of the data are used in specific approved research projects.

Careful strategies have been developed to ensure that the database does not identify personal information. No individuals names, addresses, telephone numbers or similar identifiers are contained in the database. The Personal Health Information Numbers (PHIN) are included but scrambled by Manitoba Health prior to transfer of administrative data to MCHP. There are no physician names or addresses in the database. Data for reports must be presented in summary form only, in a fashion that ensures individual identification is not possible. Anonymity is typically maintained by ensuring that any table cell does not contain less than five individuals on which data is presented. All reports and papers using Manitoba Health administrative data are submitted to Manitoba Health before publication to ensure that the privacy of individuals has not been compromised.

Purpose

The Population Health Research Data Repository enables MCHP to continue to act as the focus for a program of data analysis primarily in the Province of Manitoba, in cooperation with Manitoba Health and other agencies, with regard to:

- i. the ongoing development of the Population Health Information System;
- ii. assessing the distribution of health resources;
- iii. evaluating new and existing health care interventions;
- iv. undertaking policy research and evaluation aimed at improving the process and structure of health service delivery;
- v. providing Manitoba Health with policy advice on emerging health issues; and,
- vi. undertaking academic research focussing on understanding the broader determinants of health.

Access to Data

Only those research projects which have been approved by the data providing agency, University of Manitoba Research Ethics Board and the Provincial Health Information Privacy Committee (HIPC), and which comply with all MCHP policies developed to ensure compliance with PHIA and FIPPA, are allowed access to a project-specific subset of the repository. MCHP policy limits data access to researchers, programmers, and graduate students who meet these strict protocols in order to protect the security and confidentiality of the data and to ensure research undertaken is credible and contributes to the expansion of knowledge for the public good.

Different user groups (i.e., researchers, programmers, graduate students) have different access requirements. Access is only approved at the minimum level required to meet the need, subject to any additional specific restrictions required by University of Manitoba-MCHP, Manitoba Health or the data providing agency, and all applicable legislation.

A user who has been authorized to access the data must comply with MCHP policies, procedures and any specific restrictions imposed on the project through the approval process.

Data Linkage

All information deposited in the repository have been processed by Manitoba Health or other collecting agencies to remove or encrypt identifiable personal information while preserving the capacity to follow individual histories of health care use and related events. Datasets are typically stored in an unlinked fashion and linked only for time-limited specific approved projects.

Principles

The principles of fair information practice articulated in this document are based on the ten principles found in the Code for the Protection of Personal Information outlined in Schedule 1 to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Statutes of Canada, 2000. The MCHP principles have been developed to be consistent with the *Privacy Code for the Institute for Clinical Evaluative Sciences* (ICES) and *Privacy and Confidentiality of Health Information at CIHI: Principles and policies for the protection of health information*, developed by the Canadian Institute for Health Information (CIHI).

The Privacy Code for the Manitoba Centre for Health Policy complies with current legislation and guidelines. This document will be reviewed every two years to ensure that the principles and policies are relevant and reflect current legislation and best practice.

Principle 1 — Accountability

Principles and procedures for ensuring confidentiality and security of anonymized data are strictly enforced in order to respect the privacy of users and providers of the health care system, and to protect data against loss, destruction or unauthorized use. The University of Manitoba - MCHP as designated trustee, acts as a steward for all data held in its custody.

The University of Manitoba and designates (MCHP Director) are responsible for MCHP's compliance with these principles, for ensuring that all research studies are implemented in accordance with prevailing ethical standards and comply with all applicable laws, and that they adhere to these principles of privacy, confidentiality and security. The MCHP Director is accountable to the MCHP Advisory Board and is supported in this activity by the MCHP Access, Privacy, Confidentiality and Security Committee, the MCHP Security Officer, and all MCHP staff who share individual responsibility for adhering to MCHP health information protection policies and procedures.

- 1.1 Designated MCHP personnel are responsible for the day-to-day processing of health information.
- 1.2 MCHP has developed and implemented policies and practices to give effect to the principles outlined in this Privacy Code, including but not limited to:
 - Procedures to protect anonymized individual-level information;
 - Procedures to receive and respond to complaints and inquiries; and
 - Orientation and training of staff regarding MCHP procedures, policies and practices, as well as reinforcing staff sensitivities to privacy protection on a regular basis.

Principle 2 — Identifying Purpose

Each research project will identify the purpose(s) for use of the requested anonymized health information by development of a research proposal and study design/plan before the information is accessed. Data are used for research and statistical purposes only.

- 2.1 In accord with agreements with Manitoba Health and other data-providing agencies, anonymized individual-level data is used to address the purposes outlined in the Purpose section of this document. Summary information is provided to decision-makers, analysts and providers, so they can offer services which are effective and efficient in maintaining and improving the health of Manitobans. University- based researchers have a responsibility to publish new knowledge derived from research.
- 2.2 To fulfill the purpose, anonymized individual-level data are transferred from one responsible keeper (such as Manitoba Health) to the University of Manitoba - MCHP as trustee, with a chain of accountability for data protection. Responsibility for consent to transfer and legal authority to transfer to the University of Manitoba - MCHP as trustee rest with the primary collector and are articulated in MCHP data agreements.
- 2.3 Each project that requires access to the Population Health Research Data Repository will be granted access by MCHP to only those data that are required for the specific project.
- 2.4 If a new purpose is subsequently identified for the use of data referred to in 2.3, the new purpose will be identified and approved by all relevant agencies prior to use.

Principle 3 — Consent

The University of Manitoba - MCHP as a health information trustee and recipient of anonymized individual-level health information works within the provisions of the Manitoba Freedom of Information and Protection of Privacy Act (FIPPA) and the Manitoba Personal Health Information Act (PHIA). As such, in accordance with FIPPA - section 47 and PHIA - sections 22 and 24, researchers do not seek individual consent for use of these data for research and statistical purposes.

The use of anonymized health information without seeking individual consent is permitted by legislation:

- where the data will be used for approved research, policy formulation and/or statistical purposes; *and*
 - the research is of sufficient importance;
 - the purpose cannot reasonably be accomplished unless the data are provided;
 - it is unreasonable or impractical to obtain consent from individuals;
 - processes are in place to safeguard the data; and,
 - identifying information is removed or destroyed at the earliest opportunity.

When researchers seek to link prospectively collected survey data with administrative data, informed consent of the individual is required prior to the link.

Principle 4 — Limiting Collection

The University of Manitoba - MCHP as trustee for anonymised individual-level data will permit use of only those data that are necessary to address the purpose as outlined in the Purpose section of this document, as approved for specific studies.

- 4.1 Both the amount and the type of information used will be limited to that which is necessary to fulfill the research purpose identified. Projects will not use other data to enrich the research data unless such processes have been clearly identified within the purpose section of a research document and required approvals have been obtained.
- 4.2 Where anonymized data are transferred to the PHRDR from another agency, MCHP observes the guidelines of the originating agency and legislation with regard to the application and security of that data.

Principle 5 — Limiting Use, Disclosure and Retention

Subsets of the anonymized data contained in the PHRDR are used in project specific and approved studies only for the purpose as outlined in the Purpose section of this document. Access to data are allowed for approved research projects. All requests for data receive approval from the data providing agency, the University of Manitoba Research Ethics Board and the Provincial Health Information Privacy Committee (HIPC). For Manitoba Health deliverables, HIPC is notified prior to data access.

The University of Manitoba - MCHP as trustee, does not disclose individual-level information which it houses. Such an act would contravene its research agreements. All researchers present data in an *aggregated* fashion (i.e., data are collated and grouped together for presentation purposes).

Anonymized individual-level information in the Population Health Research Data Repository are maintained as long as agreements with provider agencies (e.g., Manitoba Health) are in effect. In fact, the power of the data repository resides in its capability to support studies of health outcomes over the long term.

- 5.1 Applications for use are reviewed, and approval is given to access only those data, which are relevant to the specific project under consideration. Only researchers working on approved projects can utilise the data.
- 5.2 Anonymity is typically maintained by ensuring that any table cell does not contain less than five individuals (patients or physicians) on which data is presented.

- 5.3 Different types of users (researchers, programmers, and students) have different access requirements. Access rights are given at the minimum level that will meet those needs, subject to specific restrictions required by the University of Manitoba - MCHP, Manitoba Health, other interested parties and/or legislation and specific restrictions imposed on each project by the approval process.
- 5.4 For special-case projects which might involve transfer of anonymized datasets to alternate sites, a pre-approval process with the data provider shall include review of site security procedures, the researcher's experience with the use of such data, and any other specifications requested by the data provider and/or University of Manitoba-MCHP.
- 5.5 Where appropriate, MCHP may augment databases within the secured systems environment, by linking databases. The data linkage is for a time-limited specific/ approved project. Any record linkages will be identified in the project proposal and receive all required approvals before proceeding. MCHP will undertake data linkage projects only if the purpose of the linkage is consistent with the MCHP mandate. As part of the approval process, it must be determined that the linkage is not detrimental¹ to the individual concerned and the benefits to be derived must clearly provide public benefit².
- 5.6 MCHP has developed guidelines and implemented procedures to govern the destruction of anonymized individual-level information (e.g., shredding of documents in-house, data tape erasure, etc.).
- 5.7 MCHP abides by all written agreements with data providers regarding the use, retention and destruction of anonymized data. These agreements provide for return of the data to the provider if agreements are terminated.

Principle 6 — Accuracy

The University of Manitoba - MCHP relies on the agency collecting the data to ensure that anonymized information is accurate, complete and up-to-date at the time of collection. MCHP takes considerable care to review and establish that the information derived from the PHRDR data files is valid.

- 6.1 Administrative and registry data which have been provided to the PHRDR in an anonymized form cannot be updated, unless the organization collecting the data provides updated information.
- 6.2 MCHP shall endeavour to ensure the integrity (quality, accuracy, and reliability) of records under its control, whether in written, electronic, or other form.

¹ as defined in Appendix 1 — Glossary of Terms

² as defined in Appendix 1 — Glossary of Terms

Principle 7 — Safeguards

The University of Manitoba-MCHP shall establish and require a high level of physical and electronic security for all data within its custody. MCHP personnel consider all data to be highly sensitive; thus information protection is paramount and accomplished with security safeguards appropriate to the sensitivity of the information.

- 7.1 *Without exception*, all data housed within the PHRDR are considered to be highly sensitive.
- 7.2 Security safeguards protect information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. MCHP will protect anonymized health information regardless of the format in which it is held.
- 7.3 The nature of the safeguards will vary depending on the amount, distribution, format of the information, and the method of storage. The methods of protection include but are not limited to:
 - (a) anonymization of data by scrambling, encrypting or removing conventional identifiers;
 - (b) physical measures; e.g. secured facility, restricted access, and security monitoring;
 - (c) organizational measures; e.g. strict employee confidentiality agreements, orientation and continual training of staff, and data access only with project approval; and,
 - (d) technological measures; e.g., the use of firewalls, moating of data making it inaccessible externally, passwords, encryption of data, security audits, etc.
- 7.4. MCHP requires, as a condition of employment, a signed confidentiality agreement from all staff, including researchers. Signed confidentiality agreements are also required from research collaborators, associates, and students who may have access to aggregate data. On an ongoing basis, MCHP makes its staff aware of the importance of maintaining the confidentiality of anonymized individual-level information.
- 7.5 All researchers who wish to access the PHRDR must comply with the specifications outlined in FIPPA and PHIA, and sign the oath of confidentiality that they guarantee they will maintain the privacy and confidentiality of the data.
- 7.6 MCHP has policies and procedures in place pertaining to the disposal or destruction of anonymized information to prevent unauthorized parties from gaining access to the information.

Principle 8 — Openness

MCHP will make information about its policies and practices relating to the management and protection of anonymized information readily available upon request. Information regarding policies and practices will be available in printed form and/or on its Web site — www.umanitoba.ca/centres/mchp/ This information will be made available in a form that is generally understandable.

8.1 The information made available will include, but is not limited to the following:

- a) The contact details for the MCHP Privacy Officer and the University of Manitoba Privacy Officer, who are accountable for the University of Manitoba - MCHP policies and practices and to whom complaints or inquiries can be forwarded;
- b) A description of the type of information held in the PHRDR, including a general account of its use; and,
- c) A copy of any brochures or other general information that explain MCHP policies, standards or codes of practice in relation to the PHRDR.

Principle 9 — Individual Access

As trustee with delegated responsibility to maintain the confidentiality of data within its custody, The University of Manitoba - MCHP cannot provide access to anonymized information within its administrative and registry datasets to individuals who are not associated with approved research projects. Upon request, MCHP will inform an individual which general data source(s) was used for research and statistical purposes, but will then refer the individual to the primary collector of such data (e.g. Manitoba Health or other relevant agency).

Principle 10 — Challenging Compliance

An individual will be able to address a challenge concerning compliance with the above principles to the MCHP Privacy Officer or the University of Manitoba Privacy Officer.

- 10.1 MCHP has procedures in place to respond to complaints or inquiries about its policies and practices relating to the handling of anonymized individual-level information. These procedures are easily accessible and simple to use.
- 10.2 MCHP will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures, including utilization of the Provincial Ombudsman, if they are not satisfied with the University of Manitoba outcome.
- 10.3 MCHP will investigate all complaints within appropriate timelines. If a complaint is found to be justified, MCHP will take appropriate measures including, if necessary, amending its policies and practices and/or disciplining staff.

Appendix 1 - Glossary of Terms

Detrimental	the purpose of a data linkage is not to make decisions about a subject individual that would result in harm to the individual, such as being denied access to appropriate health services and/or benefits to which the individual is entitled. In certain circumstances, detrimental could include consideration of potential harm to a specified group.
Public benefit	the results of the linkage are expected to contribute to: <ul style="list-style-type: none">• the identification, prevention or treatment of illness, disease or injury;• scientific understanding relating to health;• the promotion and protection of the health of individuals and communities; or• improvements in health system policy and management.