March 2020

Privacy, Confidentiality and Data Security: Handbook of Research Policies and Procedures

Prepared by the Institute for Work & Health Privacy Committee

Institute for Work & Health | Research Excellence Advancing Employee Health

Original Version: June 22, 2001

Version 2: Revised June 9, 2003

Version 3: Revised July 26, 2004

Version 4: Revised August 13, 2004

Version 5: Revised November 1, 2004

Version 6: Revised February 24, 2005

Version 7: Revised September 29, 2005

Version 8: Revised November 22, 2006

Version 9: Revised May 25, 2007

Version 9a: Revised December 4, 2007

Version 10: Revised November 6, 2016

Version 11: Revised January 22, 2017

Version 12: Revised June 25, 2019

Version 13: Revised December 18, 2019

Institute for Work & Health

Privacy, Confidentiality and Data Security: Handbook of Research Policies and Procedures

Authors: Institute for Work & Health Privacy Committee

Date: March 2020

Contents

1. Why a handbook?

This handbook is intended to help individuals become acquainted with Institute for Work & Health privacy policies and practices as they relate to the use of personal information for research purposes[1]. For more details about our policies and procedures visit our website [2,3].

We regard the access to personal information for research purposes as an important privilege. Protecting the privacy of individuals whose personal information is used in our research and the confidentiality of personal information in our custody is an integral commitment and responsibility of the Institute. Institute staff are expected to comply at all times with the Institute's privacy protection policies and procedures, contributing to the integrity of our privacy protection culture.

How this handbook is organized

Following an introduction that describes the Institute and our privacy commitment, this handbook presents a summary of research ethics principles, a description of the current legislative framework governing personal information in Ontario and a summary of the ten privacy protection principles which shape current information privacy practices. This background information is followed by specific information on the Institute's privacy protection policies and procedures, including our research ethics review practices, and our commitment to describing the privacy impacts of our research. The privacy committee, in consultation with other Institute staff, prepared the policies and procedures outlined in this handbook.

[1] Throughout this handbook, the term personal information encompasses the definitions of both (1) personal information as defined in the Freedom of Information and Protection of Privacy Act (FIPPA https://www.ontario.ca/laws/statute/90f31) and (2) personal health information defined in the Personal Health Information Protection Act (PHIPA https://www.ontario.ca/laws/statute/04p03)

[2] Institute for Work & Health privacy policies: https://www.iwh.on.ca/privacy-policies

[3] A full set of detailed policies and procedures, for staff use only, are located on IWH's internal website

2. About the Institute for Work & Health

The Institute's mission

The Institute for Work & Health focuses on a single mission: to promote, protect and improve the safety and health of working people by conducting actionable research that is valued by employers, workers and policy-makers. In pursuing this mission, we strive to ensure our research and knowledge exchange activities adhere to the values of excellence, integrity, accountability and respectfulness. And we follow six key principles in our conduct: listen, align, collaborate, be independent, be impartial and innovate[4].

What we do

The Institute for Work & Health conducts research in two broad areas: primary prevention to ensure workers remain healthy and safe at work by preventing work-related injury and illness, and secondary prevention to improve the health and recovery of workers who have sustained a work- or non-work-related injury or illness that affects their ability to work. This research is conducted using study methods that are appropriate to the research question and that give rise to reliable, valid and trustworthy findings. Research results are then shared with stakeholders through a two-way knowledge transfer and exchange process, which is a core part of our mandate alongside research.

Our funding and governance

The Institute for Work & Health is a not-for-profit organization that operates with core funding from the Province of Ontario, with the Ontario Ministry of Labour, Training and Skills Development holding the stewardship for this funding. The Institute has an arm's-length relationship with the Ministry to ensure the independence and impartiality of our research. We are governed by a Board of Directors made up of senior business, labour and academic leaders, and we receive scientific guidance from a Scientific Advisory Committee, which reports to the Board of Directors.

[4] For more details on the six principles, visit: https://www.iwh.on.ca/about-us/mission-and-values

3. Privacy commitment

The Institute's mission is underpinned by our commitment to respect personal privacy, safeguard the confidentiality of personal information in our custody, and ensure a secure environment for electronic and physical records containing personal information.

The Institute meets this commitment through the following privacy objectives:

- establishing clear principles and policies for the protection of personal information, emphasizing high standards of organizational, technical and physical security practices and protocols;
- communicating privacy protection policies and practices to Institute staff, affiliates and stakeholders;
- restricting access to personal information to those members of the organization who have authorized access for research purposes;
- submitting research protocols involving personal information to external research ethics boards;
- designating the position of Institute Privacy Officer to oversee the Institute's privacy protection policies and practices;
- ensuring all staff are trained in the principles and practices of personal information protection and requiring all staff to annually commit, in writing, to respect the Institute's principles, policies and practices in the protection of personal information; and
- ensuring that the Institute's policies and practices are consistent with the best national and international standards of privacy protection in health research and legislative requirements.

4. Ethical principles guiding research involving human participants

Respect for the privacy of research participants is an important dimension of research ethics involving human participants and a fundamental moral commitment to advancing human welfare, knowledge and understanding. Researchers,

universities, governments and private institutions undertake or fund research involving human participants for many reasons; for example, to alleviate human suffering, validate social or scientific theories, dispel ignorance, analyze policy, and understand human behaviour and the evolving human condition.

The Institute for Work & Health is committed to respecting the ethical principles involving human participants in research based on frameworks disseminated by the Interagency Advisory Panel on Research Ethics[5]. The Interagency Advisory Panel is mandated by the Canadian Institutes of Health Research (CIHR), the Natural Sciences and Engineering Research Council (NSERC) and the Social Sciences and Humanities Research Council (SSHRC) to promote high ethical standards of conduct in research involving humans through the development, evolution, interpretation and implementation of the *Tri-Council Policy Statement-2: Ethical Conduct for Research Involving Humans (TCPS2).*

5. Privacy protection principles

The Institute's privacy protection principals, listed below, draw from emerging standards at the federal and provincial levels. Specifically, key documents from the Information and Privacy Commissioner of Ontario (IPC) and the Canadian Standards Association's (CSA) ten principles for the protection of personal information[6]. The CSA principles were also used in the development of a comprehensive guideline statement from the Canadian Institutes of Health Research (CIHR), released in September 2005, titled *CIHR Best Practices for Protecting Privacy in Health Research[7].*

[5] http://www.ger.ethique.gc.ca/eng/home.html

[6] The Canadian Standards Association's (CSA) ten principles for the protection of personal information have informed the legislative objectives of the federal legislation Bill C-6 (Personal Information Protection and Electronic Documents Act [PIPEDA]) and Ontario's health information privacy protection legislation (the Personal Health Information Protection Act, 2004).

[7] http://www.cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf

Accountability

Procedures for ensuring confidentiality and security of data are strictly enforced to protect data against loss, destruction or unauthorized use. The Privacy Officer, under the direction of the President of the Institute for Work & Health, is responsible for the Institute's compliance with the principles, policies and procedures described in this handbook. The Institute is accountable for ensuring that research studies are implemented under the oversight of Research Ethics Boards, and that staff are reminded that privacy is everyone’s responsibility.

Identifying purposes of data use

Institute Scientists are required to clearly describe their use of personal health information in research proposals and study designs/plans before any personal information is collected or obtained. Personal information collected or obtained by an Institute Scientist is to only be used for the research and statistical purposes stated in the research proposal and ethics agreement.

Consent

Consistent with the ethical principle of the autonomy of research participants, individuals participating in research projects that involve the collection of personal information will be provided with a description of the purposes of the research, an assessment of the benefits of participation and an assessment of the potential harms of participation. Research participants will have the freedom to consent and withdraw from participation without any adverse consequences. In the case of research projects that propose to use personal information in the absence of individual participant consent, the Institute will refer to the guidance provided by the comprehensive guideline statement from the Canadian Institutes of Health Research, *CIHR Best Practices for Protecting Privacy in Health Research*, and by guidance received from a Research Ethics Board review of the balancing of harms and benefits.

Limiting collection

The Institute will limit the collection of personal information to that which is necessary to fulfill the research purposes of the study.

Limiting use, disclosure and retention

All administrative, registry or survey data received by the Institute will be used only for research purposes. All primary data are used only for the purposes identified prior to the collection of the data. The Institute will not disclose personal information in its custody to third parties, unless the research purpose is consistent with the original purpose of the collection and the research protocol has been reviewed and approved by a Research Ethics Board.

In reporting research results and findings, the Institute will present quantitative data in an aggregated form[8] and will present anonymized data[9] in qualitative research to prevent the potential identification of individual research participants.

Personal information is retained and securely archived as is required for research projects for periods varying from five to ten years. In a project-specific research agreement, earlier destruction may be a requirement.

Accuracy

Personal information collected for research purposes will be as accurate and complete as possible at the time of collection.

[8] Aggregate-level data is summed and/or categorized data that can answer research questions about populations or groups of organizations. The data has been compiled from record-level data to a level that ensures the identities of individuals or organizations cannot be determined by a reasonably foreseeable method. (https://www.cihi.ca/en/faq/what-is-aggregate-level-data)

[9] Data anonymization is a type of information sanitization meant to protect privacy. It is the process of either encrypting or removing personally identifiable information from data sets, so that the people described by the data remain anonymous.

Safeguards

All personal information in the custody of the Institute will be protected from unauthorized access and disclosure. The methods of protection include:

- *organizational security*, including training and educating employees, ensuring the completion of up-to-date employee confidentiality agreements, limiting access to data, investigating potential security breaches, and enforcing consequences for breaches of policy;
- *physical security*, including keeping data in a locked facility with tracked key access, locking filing cabinets, restricting access to offices, and ensuring on-site security after hours; and
- *technical security*, including using firewalls and passwords, encrypting data, and anonymizing personal information by removing person-identifiable variables.

Openness

The Institute makes information about its policies and practices relating to the management and protection of personal information (with the exception of procedures for IT security) readily available by request. The Institute Privacy Officer is the designated individual responsible for ensuring privacy policies and practices are communicated clearly and openly.

Individual access

In the event a research participant wishes to review his or her personal information following collection and use in a research study, the Institute will comply with reasonable requests. Participants should receive a study information letter and can request a copy of their signed consent form. This right of access will be limited to information collected directly from research participants who consented to participate in the research project. The Institute will not provide access to information contained in secondary data sources.

The Institute Principal Investigator and Privacy Officer are responsible for responding to general questions or information requests from research participants concerning privacy policies, privacy practices and confidentiality, as they relate to participation in

an Institute research study. All research participants are entitled to receive clear and open communications regarding their privacy and confidentiality requests.

Challenging compliance

An individual who wishes to address a concern about compliance with the Institute's privacy policies and practices may direct this concern to the Institute Privacy Officer via email at: PrivacyOfficer@iwh.on.ca

6. Legislative framework: Personal information and research

Throughout this handbook, we describe principles, policies and procedures for the protection of personal information. As a research organization with a mandate to improve understanding of effective methods for protecting the safety and health of workers, personal information of research interest to the Institute often describes the health status of individuals. The collection, use and disclosure of personal health information in the Province of Ontario is governed by regulations established by the Personal Health Information Protection Act (PHIPA), which came into effect on November 1, 2004. Personal information that does not meet the PHIPA definition is governed by the federal Freedom of Information and Protection of Privacy Act (FIPPA).

The Institute will conduct privacy protection research practices in compliance with the general principles established in PHIPA. Also, in specific research projects that involve the disclosure of personal health information to the Institute from a health information custodian[10] as defined by PHIPA, the Institute will comply with the requirements of Section 44 of the Act.

Under FIPPA, personal information is defined as recorded information about an identifiable individual, including race, nationality, ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status, education, medical history (physical, psychiatric and psychological), criminal history, employment history and financial transactions.

[10] http://www.health.gov.on.ca/english/providers/project/priv_legislation/info_custodians.pdf

The federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA)[11] gives individuals the right to:

- know why an organization collects, uses or discloses their personal information;
- expect an organization to collect, use or disclose their personal information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented;
- know who in the organization is responsible for protecting their personal information;
- expect an organization to protect their personal information by taking appropriate security measures;
- expect the personal information an organization holds about them to be accurate, complete and up-to-date;
- obtain access to their personal information and ask for corrections if necessary; and
- complain about how an organization handles their personal information if they feel their privacy rights have not been respected.

The *Act* requires organizations to:

- obtain consent when they collect, use or disclose individuals' personal information;
- supply individuals with a product or a service even if they refuse consent for the collection, use or disclosure of their personal information, unless that information is essential to the transaction;
- collect information by fair and lawful means; and
- have personal information policies that are clear, understandable and readily available.

As a not-for-profit research institute, the provisions of the federal legislation concerning the regulation of intra-provincial and inter-provincial commercial

[11] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

transactions of personal information will generally not apply to the Institute's research activities.

Under PHIPA, personal health information is defined as identifying information about an individual that meets at least one of the following criteria:

- relates to the physical or mental health of the individual, including information about the individual's family health history;
- relates to the provision of health care to the individual, including the identification of a person who provides health care to the individual;
- is a plan of service within the meaning of the Long-Term Care Act, 1994;
- relates to payments or eligibility for health care in respect of the individual;
- relates to the donation by the individual of any body part or bodily substance, or is derived from testing of such body part or substance;
- is the individual's health number; and
- identifies the individual's substitute decision-maker.

Personal health information also includes other identifying information that is contained in the same record with the information described above. Information is "identifying" when it discloses an individual's identity or when it is reasonably foreseeable in the circumstances that it could be used, either alone or with other information, to identify the individual.

7. Institute privacy protection policies and procedures

The policies and procedures for the collection, use and disclosure of personal information used in research at the Institute are located on the organizations internal website. The site is structured as follows:

Chapter 1: *Privacy*

Chapter 2: *Security*

Chapter 3: *Compliance*

Chapter 4: *Governance and risk management*

Research ethics review policies and procedures

All research protocols proposing to use personal information are required to present a copy of the research protocol to a Research Ethics Board (REB) at a health-care institution or university. Where personal information is collected or disclosed by a health-care institution, an additional institutional level REB approval may also be required.

It is the responsibility of the Institute Principal Investigator to prepare a REB submission and to respond to any concerns raised in the ethics review. All proposed research, whether funded from internal Institute resources, external granting agencies or contract-funding sources, must receive a REB review and approval before research activity may commence.

Investigators are always encouraged to discuss questions or concerns about REB review requirements with the Institute's Privacy Officer, the Director of Research Operations or their delegate.

Use of secondary data and record linkage

Secondary or administrative data sources can be very useful resources for research. These data sources are collected by organizations to conduct their business. For example, workers' compensation boards collect information in the course of administering employee compensation claims and collecting employer insurance premiums. Compared to directly surveying or interviewing respondents, these administrative data sources generally save time and money for the researcher, as well as reduce the burden on respondents. Often, these data sources cover entire populations.

Contemporary standards for ethical research practice expect that researchers obtain informed consent from people who are invited to participate in research. It is often not feasible to obtain individual consent from people whose information is recorded in administrative records. To address this special circumstance, enhanced standards for using secondary data sources without individual consent have been developed through an initiative called Harmonizing Research & Privacy, funded by the Canadian Institutes of Health Research.

The Institute is committed to respecting these standards and the guidance outlined in the CIHR document, *Best Practices for Protecting Privacy in Health Research*

(September 2005). To that end, whenever we plan to conduct a study using secondary data and/or record linkage without individual consent, we submit our study protocol for ethical review to a Research Ethics Board at a recognized organization. This submission includes assessments of the benefits of conducting the research, the risks involved, whether other methods could be used, and the safeguards in place to protect the data and the confidentiality of the study subjects.

Visit the Institute website to review a list of research projects conducted at the Institute that are using secondary data without individual consent[12].

Training

All new Institute employees receive a privacy orientation and sign a confidentiality agreement as a condition of employment. Privacy information sessions are offered annually, and attendance is mandatory for all employees.

Information breach

A privacy breach is the loss of, unauthorized access to, or disclosure of personal information. Some of the most common privacy breaches happen when personal information is stolen, lost or mistakenly shared[13] . The Institute has a procedure for containing breaches. If you feel there has been a breach, please contact the Institute Privacy Officer.

How to contact the Institute's Privacy Officer

For more information, requests or comments on Institute research studies or our general privacy policies and procedures, please contact the Privacy Officer by email at: PrivacyOfficer@iwh.on.ca

[12] https://www.iwh.on.ca/privacy-policies/research-privacy-policy

[13] Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/