Respecting the New Privacy Rules: How Will They Affect Health Research?

The ability to carry out research—including studies that explore many aspects of workplace health and injury—depends on the appropriate collection, disclosure, and use of personal information.

Institute scientists, associates, and students draw health and employment data from various national and provincial databases which contain information about thousands of people including workers. They also collect personal information directly from individual research subjects during the course of ongoing studies.

“Research responds to the human desire for new knowledge and understanding,” says IWH President and population health scientist Dr. Cameron Mustard. “But we must constantly balance the benefits of research against potential risks and harms borne by those who participate in research studies.”

While everyone wants to enjoy the fruits of high quality research, Canadians also care about keeping their personal health and employment information confidential. This concern has produced an ever-growing array of privacy rules and regulations:

• All Canadian researchers who obtain certain types of federal funding are expected to comply with the Tri-Council Policy Statement:

Ethical Conduct for Research Involving Humans. This document includes rules about obtaining consent from research subjects and protecting the privacy and confidentiality of their personal information.

• In 2004, Ontario’s Personal Health Information Protection Act (PHIPA)—aimed at further safeguarding the health information of patients and research subjects—came into effect. At the same time, federal regulations, known as the Personal Information Protection and Electronic Documents Act (PIPEDA), were adopted to help protect personal information collected in the course of commercial activities.

Respecting privacy was the focus of a recent set of guidelines developed by the Canadian Institutes of Health Research (CIHR). The CIHR is Canada’s premier health research funding agency which supports thousands of researchers in universities, teaching hospitals, and institutes across the country.

The CIHR guidelines, entitled Protecting Privacy and Confidentiality in the Design, Conduct and Evaluation of Health... (continued on page 2)
Research (see page 3), have become a touchstone for research organizations across Canada, says Mustard. “Indeed, they provided guidance to the Institute as we developed our own privacy policies,” he adds.

Everyone agrees that privacy legislation is not intended to deter legitimate health research. Even so, some groups have expressed concern that growing pressure to comply with different regulations—along with different interpretations of the rules—might negatively affect the quantity or the quality of research being done in Canada.

In 2003, the Institute participated in an international workshop entitled Harmonizing Research and Privacy. The workshop brought representatives from various research, policy, academic and government organizations together to examine current privacy regulations and to discuss streamlining the system.

There were also discussions about the challenges of complying with existing privacy standards. For example, the new federal legislation requires organizations to appoint or hire a Privacy Officer to train staff in privacy issues and to take “all reasonable precautions” to prevent private information from being used outside the terms of existing privacy policies and regulations.

The expanding focus on privacy protection has cost implications, both for individual researchers and also for their sponsors. In their report, organizers of the harmonization workshop suggest that funding for privacy diligence be built into the costs of running research organizations.

Case study: The challenge of compliance

Right now, privacy guidelines and regulatory requirements vary widely from province to province and country to country. This can make it difficult for researchers to conduct cross-border studies.

For example, a University of Montreal researcher collaborating with an investigator at a federally-funded U.S. institution would have to comply with an array of privacy requirements.

These would include regulations established by the Canadian Institutes of Health Research, Health Canada and U.S. Food and Drug Administration (FDA), as well as rules contained in the Quebec Civil Code and the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).
“Best Privacy Practices” for Researchers

To develop their newest guidelines, the Canadian Institutes of Health Research (CIHR) undertook lengthy consultations with a panel that included privacy experts, health sciences researchers, health care providers, patients, data custodians and producers, ethicists and policy-makers.

The document—Protecting Privacy and Confidentiality in the Design, Conduct and Evaluation of Health Research—is intended to help researchers ensure privacy, confidentiality and security in health research. The guidelines will also serve as a resource for Research Ethics Boards (REBs) across Canada which regularly review how research studies are designed and conducted.

According to the CIHR, “At the heart of these best practice guidelines are two core values: respect for the privacy of individuals and recognition of the social value of health research. The challenge is to balance these values—not one against the other, but with a view to maximizing the benefits of both values, while minimizing potential harms from the neglect of either one.”

Here are some of the key elements contained in the CIHR’s best privacy practices:

- **Determine the research objectives and justify the data needed.** Health researchers should identify and document research objectives and questions as thoroughly as possible from the very start. This will help them determine what data will be needed. They should anticipate and document research questions related to the study’s primary research objective and also consider likely future uses of the data, including possible collaborations with other researchers or possible commercial uses.

- **Limit the collection of any personal data.** Researchers should plan to collect personal data at the “lowest level of identifiability necessary to achieve the research objectives.” Limiting identifiability means minimizing the collection of direct identifiers, such as the person’s name and street address.

- **Determine if consent from individuals is required.** When information is collected directly from the individual subject, obtaining consent is almost always required. When there is a legitimate reason for collecting personal data from other sources, consent is generally required unless the researcher can demonstrate why this requirement should be waived. Under limited circumstances, a waiver or partial waiver of a consent requirement may be permitted by law and approved by a Research Ethics Board.

- **Manage and document consent.** Consent or the refusal of consent should be given by legally competent individuals or authorized third parties. This may be done in writing (preferred), orally, or clearly indicated by conduct. Evidence of consent (or refusal) should be clearly documented and available.

- **Inform prospective research participants about the research.** Researchers must make sure a prospective research subject has the chance to fully discuss and contemplate his or her participation in a scientific study. The consent procedure should include explaining the nature of the research, what personal information will be collected and how it will be used, and the risks and benefits of the research to participants. This allows the person to make a truly informed decision about whether or not to participate.

- **Safeguard data confidentiality.** Data security measures should include organizational, technological and physical measures. Researchers and their employers should take a risk management approach that is “appropriate to the extent, sensitivity and identifiability of the data.”

- **Limit access to personal data.** Sharing data for research purposes is an important way of enabling socially valuable research. It also avoids unnecessary data collection, which reduces the burden on individual organizations and allows researchers to use safeguard, protocols for such “third party” research must have been reviewed and approved by a Research Ethics Board.

- **In reporting research results and findings, IWH presents quantitative (numerical) data in an “aggregated” form (see page 4). Qualitative research is presented in the form of “anonymized” narratives (see page 4) to prevent possible identification of individual research subjects.**

- **Personal information about research subjects is kept and securely archived for periods varying from five to ten years, according to the original research agreements. In some cases, the data may be destroyed sooner.**

---

How IWH is working to protect the privacy of research subjects

All research involving human subjects carried out by scientists at the Institute for Work & Health are governed by the **Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.**

Because the Institute is a not-for-profit organization, its research activities are exempt from the new federal privacy regulations which focus on commercial transactions of personal information.

Over the past year, the Institute has updated policies and practices aimed at protecting personal information. The emphasis has been on developing high standards of organizational, technical and physical security practices and protocols.

For example:

- **All administrative, registry or survey data received by IWH is used only for research and statistical purposes.**
- **All data collected directly by researchers (primary data) is used only for the purposes identified before collection.**
- **Only authorized staff have access to personal information about research subjects, and all staff are regularly trained in the principles and practices of protecting personal information.**
- **The Institute does not disclose personal information in its custody to other researchers unless their purpose is consistent with the original reason for the collection of this data. As an added
Demystifying the language of privacy and research

Those who discuss privacy issues, especially as they relate to health research, often speak in a language of their own. The following definitions may be helpful:

**Aggregate data**

This type of statistical information describes the average habits and characteristics of a group of people. For example, a study may add up the total number of workers (but not their names) in a given year or employment sector who made a workplace injury claim. Researchers can compare this with similar data from a different year or job sector to look for trends. Although assembled from personal information about individuals, no individual identities are revealed in aggregate data.

**Anonymized data**

This refers to personal information about an individual in which any possible personal identifiers have been removed so there is no way for anyone to determine the identity of research subjects.

**Consent**

Consent can have many meanings. The idea evolved in the context of medical interventions and clinical trials, where participants are informed about the known risks and benefits of a procedure and then asked to provide verbal or written consent. However, where personal information is collected for statistical analyses at a population level, it is harder to apply the basic concept of informed consent. Research Ethics Boards will often contribute to assessing the balance of benefits and potential risks in studies which are based on information provided without consent.

**Data linkage**

This is a complex process which researchers use to study a particular phenomenon. In some cases, they create a new record—for example, the number of miners in Canada receiving permanent disability compensation—by linking two or more existing records which refer to the same individual. In this case, they might link provincial job sector databases with provincial data on permanent disability compensation. (also known as “record linkage”)

**Encrypted data**

This refers to data that is scrambled either just prior to transmission or as it is being entered into a database using special encryption software. The purpose is to protect the confidentiality of data.

**Personal information**

Privacy guidelines deal with all kinds of personal information (and data) about individuals used in the health research context, ranging from clinical data to information relating to the use of health care services to information relating to broad determinants of health, such as education, employment, and income level. Personal information is generally defined as information that identifies an individual (e.g. name and street address), or that could potentially identify a person if data in the record was combined with other available information.

**Personal health information**

This is defined as identifying information about an individual whether oral or recorded, if the information relates to (among other things) the physical or mental health of the individual, including family health history, his/her health insurance number or the name of his/her health care provider(s).

**Pseudonomized data**

This refers to information where a unique number or some other symbolic equivalent has been substituted for personal identifiers such as a worker’s name, age, employer or job sector.

**Research Ethics Board (REB)**

Universities, hospitals and other organizations which conduct research involving human subjects must establish “arms-length” Research Ethics Boards or REBs. The REB helps ensure that research studies meet the highest ethical standards, and that the greatest protection is provided to participants who serve as research subjects.

“Best privacy practice for researchers” (continued from page 3)

- Ensure accountability and transparency. When it comes to privacy, roles and responsibilities should be clearly defined and understood. Individuals and organizations should be open to the public about their research objectives and also about policies and practices for managing personal data used for research.

Respecting the new privacy rules: How will they affect health research? (continued from page 2)

- Encrypted data

- Aggregate data

- Personal information

- Anonymized data

- Consent

- Data linkage

- Pseudonomized data

- Personal health information

- Research Ethics Board (REB)

- "Best privacy practice for researchers" (continued from page 3)

- Respecting the new privacy rules: How will they affect health research? (continued from page 2)