

# RESEARCH USE OF HEALTH INFORMATION: AN EVOLVING REGULATORY CONTEXT

Denis Cournoyer  
Director, Research Ethics Office



Centre universitaire de santé McGill  
McGill University Health Centre

# Research Use of Health Information Overview

1

- Key concepts

2

- Privacy Best Practices

3

- Regulatory Framework



**Centre universitaire de santé McGill  
McGill University Health Centre**

**As part of the Quality Assurance and Education Program (QAEP),  
The Research Ethics Office is pleased to present our Semi-Annual Lecture in Research Ethics:**

## **Consent to What?!**

# **Ethical and Policy Issues in Biospecimen Research**

**Presented by:**

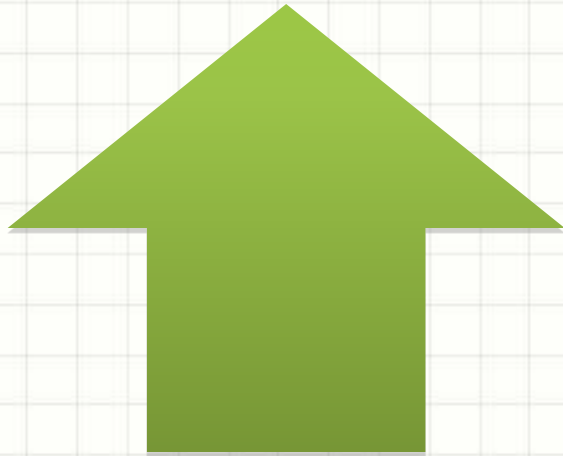
**Nancy M.P. King, J.D.**

**Friday, May 13<sup>th</sup>, 2011**

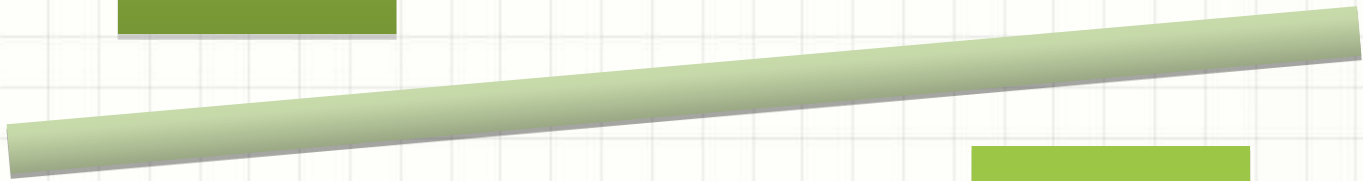
**Jack Cram Auditorium, McGill University, Faculty of Education  
3700 McTavish Street**

**11:30 – 12:00 Registration and a Light Lunch  
12:00 Lecture with Discussion to Follow**

# Research Use of Health Information



Respect for  
Privacy and  
Confidentiality



Societal Benefits of  
Research





**Privacy and Confidentiality  
in Research:  
Key Concepts**

# What Defines Research ?

**A systemic investigation/collection of data to establish facts, principles or generalizable knowledge**

- Not defined by the use of “experimental” procedures
- **Association with non-research goals such as quality-control, quality-improvement or public health activity does not affect requirement for ethics review or informed consent**



# Privacy

- An **individual's right to be free from intrusion** or interference by others
- The **right to control information** about oneself
- A **fundamental right** in a free and democratic society
- **Respect of Privacy = individuals exercise control** over personal information **by consenting to**, or withholding consent for, the collection, use and/or disclosure of information
  - Exceptions to consent requirement ?

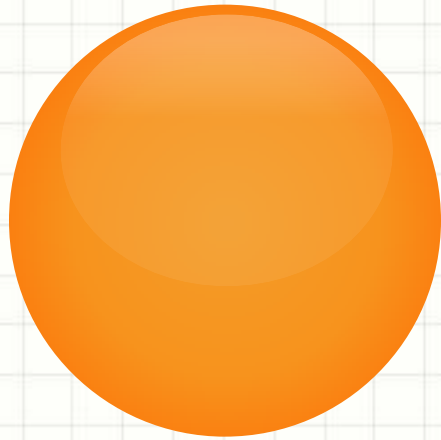
# Confidentiality

- **Ethical duty** of an individual or organization **to safeguard entrusted information**
- Includes **obligation to protect information** from unauthorized access, use, disclosure, modification, loss or theft
- **Essential to the trust relationship** between researcher and participant and to the integrity of the research project.



# Security

- **Measures used to protect private information**
- Includes physical, administrative and technical safeguards
- Adopting and enforcing appropriate security measures contribute to fulfilling duties of confidentiality



# **10 ELEMENTS OF PRIVACY BEST PRACTICES**

CIHR Best Practices for Protecting Privacy in Health Research (2005) 



## **DETERMINING THE RESEARCH OBJECTIVES AND JUSTIFYING THE DATA NEEDED TO FULFILL THESE OBJECTIVES**

- Identify and document research objectives and questions as a basis for determining what data will be needed
- Anticipate and document potential secondary uses of the data, including possible collaborations with other researchers or possible commercial uses



## **LIMITING THE COLLECTION OF PERSONAL DATA**

- Define identifiable information and minimum level of identifiability required
- Limit collection of sensitive or potentially stigmatizing data
- Dataset without direct identifiers may still present a risk of indirectly identifying subjects if the dataset contains sufficient information

# Types of Personal Information

- **Identifiable:** information that may reasonably be expected to identify an individual, alone or in combination with other available information
- **Directly identifying:** information that identifies a specific individual through direct identifiers (e.g., name, social insurance number, personal health number, MRN)
- **Indirectly identifying:** information that can reasonably be expected to identify an individual through a combination of indirect identifiers (e.g., date of birth, place of residence, postal code or unique personal characteristic)

Personal Details	<b>Most Identifiable</b> ↓ <b>Least identifiable</b>
<p><b>Subject name</b></p> ↓ <ul style="list-style-type: none"> <li>• Full name</li> <li>• Partial name</li> <li>• Initials</li> <li>• Code</li> <li>• Blank</li> </ul> <p><b>Age</b></p> ↓ <ul style="list-style-type: none"> <li>• Birth day/month/year</li> <li>• Birth month/year</li> <li>• Birth year; Age at a time of data collection</li> <li>• Age range (e.g. 5 or 10-year age group)</li> </ul> <p><b>Facilities and service providers</b></p> ↓ <ul style="list-style-type: none"> <li>• Name of institution/provider</li> <li>• Specific type of facility, provider (university hospital, family physician)</li> <li>• Generic class (hospital, medical doctor)</li> </ul>	<p><b>Location of residence</b></p> ↓ <ul style="list-style-type: none"> <li>• Street address</li> <li>• 6-character postal code (e.g. one side of a city street; average of 15 households)</li> <li>• first 3 characters of postal code/Forward Sortation Area (average of 7,000 households)</li> <li>• first character of postal code (province or region; e.g. A = Nfld/Lab.; J = Que. West; K = Eastern Ont.)</li> </ul> <p><b>Census area</b></p> ↓ <ul style="list-style-type: none"> <li>• Block (an area equivalent to a city block bounded by intersecting streets; the smallest geographic area for which population and dwelling counts are disseminated)</li> <li>• Census enumeration or dissemination area (small area composed of one or more neighbouring blocks, used by Statistics Canada for distributing questionnaires to households and dwellings for the census collection)</li> <li>• Census subdivision (e.g. municipality, village)</li> <li>• Census agglomeration (urban core: min. 10,000 pop.)</li> <li>• Census metropolitan area (urban core: min. 100,000 pop.)</li> </ul>



# Degrees of De-Identification

- **Coded information:** direct identifiers are removed and replaced with a code. Given access to the code list, it is possible to re-identify specific participants
- **Anonymized information:** the information is irrevocably stripped of direct identifiers, a code is not kept to allow future re-linkage, and risk of re-identification of individuals from remaining indirect identifiers is low or very low
- **Anonymous information:** the information never had identifiers associated with it (e.g., anonymous surveys) and risk of identification of individuals is generally very low



**Determining whether consent from individuals is required**



# Secondary Use of Identifiable Information: Conditions for REB Waiver of Consent

- **Identifiable information is essential** to the research
- Use without consent **unlikely to adversely affect the welfare of individuals**
- **Appropriate measures to protect the privacy** and safeguard the information
- Researchers **will comply with any individual expressed preferences** about use of their information
- It is **impossible or impracticable** (i.e. undue hardship that jeopardizes the conduct of the research) **to seek consent**
- Researchers have obtained any other necessary permission

**ALL CONDITIONS NEED TO BE MET  
LIMITED TO SECONDARY USE OF EXISTING INFORMATION  
NO CONTACT PERMITTED WITH RESEARCH SUBJECTS  
NO THERAPEUTIC INTERVENTION**

# ICH Guidance E6: Good Clinical Practice: Consolidated guideline

**4.8.1** In obtaining and documenting informed consent, the investigator should **comply with the applicable regulatory requirement(s)**, and should adhere to GCP and to the ethical principles that have their origin in the Declaration of Helsinki. Prior to the beginning of the trial, the investigator **should have the IRB/IEC's written approval/favourable opinion of the written informed consent form** and any other written information to be provided to subjects.

***No provision for waiver of informed consent since ICH GCP addresses therapeutic research where such waiver is not permissible***



## MANAGING AND DOCUMENTING CONSENT

- Opt-in vs. opt-out (presumed) consent
- Written vs. oral consent



## **INFORMING PROSPECTIVE RESEARCH PARTICIPANTS ABOUT THE RESEARCH**

- Primary and secondary use of data collection
- Nature of data collected, duration of retention, anonymization
- Right to withdraw participation and data  
(exception to right to withdraw data: regulated CT)
- Safeguards to protect confidentiality





## **RECRUITING PROSPECTIVE RESEARCH PARTICIPANTS**

- Assemble a list of eligible individuals
  - May requires REB waiver of consent & DPS approval
- Establish initial contact with eligible individuals
  - By someone that individuals expect to have relevant information about them
- Inform eligible individuals about the research, and seek consent
  - Avoid therapeutic or hierarchical relationships



## SAFEGUARDING PERSONAL DATA

- Includes organizational, technological and physical measures
- **Risk management** approach to protect from loss, corruption, theft or unauthorized disclosure, as **appropriate for the sensitivity and identifiability of the data**

Oh, don't worry  
Mrs Davidson. It is  
only a small micro-chip  
implant behind the  
ear. No one with a  
clear conscience need  
have any concern.



# Organizational safeguards

- **Ongoing commitment to privacy by all involved**
- Access conditional to **pledge of confidentiality**
- Access strictly limited on a **need-to-know basis**
- **Data-sharing agreements** prior to providing any access to data
- **Consequences for breach of confidentiality clearly stipulated**
  - E.g. dismissal, loss of institutional privileges
- Ongoing **institutional commitment** to adequate resources:
  - develop, monitor and **enforce privacy and security policies and procedures**
  - **appoint privacy officers**
  - **implement internal and external privacy reviews and audits**

# Technological measures

- **Encryption, scrambling of data**
- **Direct identifiers should be removed** at the earliest possible opportunity
- If **direct identifiers** must be retained, they should be **isolated on a separate dedicated server/network without external access**
- **Authentication measures** (e.g. password protection, unique log-on identification, etc.)
- **Special protection for remote electronic access**
- **Virus-checking programs and disaster recovery safeguards**
- **Where possible, audit trail monitoring system** to document the person, time, and nature of data access, with **flags for aberrant use** and **"abort" algorithms** to end questionable or inappropriate access



# Physical security

- Computers and files holding personal information in secure settings in **protected rooms** with **paper files stored in locked storage cabinets**
- The **number of locations** in which personal information is stored should be **minimized**
- **No public access** to areas where sensitive data are held
- **Routine surveillance** should be conducted
- **Protection of data from hazards** such as floods or fire



# Ethical Duty of Confidentiality

- **TCPS2**
  - **Article 5.1** *Researchers shall safeguard information entrusted to them and not misuse or wrongfully disclose it. Institutions shall support their researchers in maintaining promises of confidentiality.*
  - **Article 5.4** *Institutions or organizations where research data are held have a responsibility to establish appropriate institutional security safeguards.*
- **Duty of confidentiality** must, at times, be **balanced against** competing ethical considerations or legal or professional **requirements that call for disclosure** of information obtained or created in a research context e.g. **to protect the health, life or safety of a participant or a third party**

# Judging Adequacy of Protection of Confidentiality

- **Type of information** collected
- Appropriateness of **security safeguards**
- **Purpose** for which the information will be used, and the purpose of any **secondary use** of identifiable information;
- **Limits on the use**, disclosure and retention
- **Risks to participants** of eventual breach of security
- **Use of recording** of observations (e.g., photographs, videos, sound recordings) that may allow identification
- **Potential linkage of research data with other** public or personal records about participants



## **CONTROLLING ACCESS AND DISCLOSURE OF PERSONAL DATA**

- Controlled levels of data access within research team and for secondary use
- Data linkage (by data holder, third party, researcher)
- Data sharing with other jurisdictions

# Harmonized Model Consent – FRSQ Confidentiality – Other Jurisdictions

“The **information collected** about you **can** by itself, or together with other information collected from other studies **be shared** with government groups in Canada or **in other countries**, or with the people that do business with the study’s sponsor. This means that your study information could be sent to other countries. **The sponsor must respect Quebec and Canadian privacy laws and those in all the countries where your study information will be sent.**”



## **SETTING REASONABLE LIMITS ON RETENTION OF PERSONAL DATA**


- Pre-defined retention periods
- Duration of data retention sufficient to meet research objectives and related purposes such as validating or auditing research
- Long-term retention = anonymization of data when linkage completed



## **ENSURING ACCOUNTABILITY AND TRANSPARENCY IN THE MANAGEMENT OF PERSONAL DATA**

- Individuals and organizations = accountable for research use of personal data
- Requires adequate resources for communication, education and training
- Transparency can enhance public support for research



The background features a light gray grid pattern. Two prominent, flowing blue wavy lines are positioned at the top and right sides of the slide. The top line curves from the left towards the right, while the right-side line curves from the top towards the bottom. Both lines have a gradient and a slight shadow effect, giving them a three-dimensional appearance.

# **Privacy Legislations: An Overview**



# Health Insurance Portability and Accountability Act (HIPAA)

## Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform - **Privacy Rule**

- Regulates the use and disclosure of certain information held by "covered entities" (health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers)
- Establishes regulations for the use and disclosure of Protected Health Information (PHI)(any information held by a covered entity which concerns health status, provision of health care, or payment for health care)
- Security Rule deals specifically with Electronic Protected Health Information (E PHI)
- Covered entities must disclose PHI when required by law to facilitate treatment, payment, or health care operations or **if has obtained authorization from the individual**

**NO EXTRA-TERRITORIAL APPLICABILITY**



# CFR 42 2a.7 - Confidentiality Certificate

- Authorizes withholding the names and other identifying characteristics of individuals who participate as subjects in the research project.
- Persons so authorized may not, at any time, be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify the research subjects encompassed by the Certificate, except
  1. The subject consents, in writing
  2. Authorized personnel of DHHS request such information for audit or program evaluation
- **NO EQUIVALENT PROTECTION IN CANADA OR QUEBEC**



# ***Personal Information Protection and Electronic Documents Act (PIPEDA)***

- Governs how **private-sector organizations** collect, use and disclose personal information in the course of commercial business
- Gives **specific rights to protect privacy and confidentiality of individuals**
- **Requirements that organizations obtain consent when they collect, use or disclose personal information; (...)**

**Applies to inter-provincial exchange of personal information**

***An Act Respecting the Protection of Personal Information in the Private Sector*** (Quebec) was declared **substantially similar to PIPEDA and applies *in lieu* of PIPEDA in Quebec**

# Research Use of Health Information: Quebec Legal Framework





# Civil Code of Québec, S.Q. 1991, c. 64

- Article 35:
  - Every person has a right to the respect of his reputation and privacy
  - **No one may invade the privacy** of a person **without the consent** of the person unless authorized by law



# An Act respecting health services and social services, R.S.Q. c. S-4.2

19. The record of a user is confidential and no person may have access to it except with consent of the user (...)

19.1. **Consent** to a request for access to a user's record for study, teaching or research purposes **must be in writing** (...)

19.2. The **director of professional services** of an institution (...) may authorize a professional to examine the record of a user **for study, teaching or research** purposes.

Before granting such authorization, the director must, however, ascertain that **the criteria determined under section 125 of the Act respecting Access to documents held by public bodies and the Protection of personal information (chapter A-2.1)** are satisfied (...)

The authorization must be granted for a limited period (...)

# An Act respecting access to documents held by public bodies and the Protection of personal information, R.S.Q. c. A-2.1

**Section 125.** The Commission may, on a written request, grant a person or an agency the authorization to receive communication of personal information contained in a personal information file, for study, research or statistics purposes, without the consent of the persons concerned, if it is of the opinion:

- 1.that the **intended use is not frivolous** (*sic*) and the ends contemplated **cannot be achieved unless the information is communicated in nominative form**;
- 2.that the personal information will be used in a manner that will **ensure its confidentiality**.

The authorization is granted for such period and on such conditions as may be fixed by the Commission. It may be revoked before the expiry of the period granted if the Commission has reason to believe that the authorized person or body does not respect the confidentiality of the information disclosed or the other conditions.

# Access to Health Records for Research: the MSSS's Requirements



Recherche...

OK

## La recherche sur dossiers

“Tout projet de recherche devrait être évalué par un CÉR compétent. **L'autorisation du DSP ne remplace pas cette évaluation éthique, pas plus que ne le fait le consentement de la personne dont le dossier sera consulté.**”

# **Important Changes to the Review and Authorization Of Health Record Research**

**All studies that involve access to health information held in the MUHC must be reviewed by a Research Ethics Board having jurisdiction at the MUHC**

**In addition, if it is proposed to conduct the study without obtaining individual informed consent from all subjects, the access to health information must be authorized by the Director of Professional Services**

**Information on how to submit at**

**<http://muhc.ca/research/page/research-review-how-submit#HealthInfoResearch>**

# Summary

- Privacy is an “universal” right
- Health information considered very private
- Research using health information must balance societal benefits and respect for privacy
- Conducting research is a privilege granted by society, with conditions
- Must respect societal rules



# Resources

- **CIHR Best Practices for Protecting Privacy in Health Research (September 2005)** <http://www.cihr-irsc.gc.ca/e/29072.html>
- **TCPS 2—2nd edition of *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – Chapter*** <http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter5-chapitre5/>
- **Ministère de la santé et des services sociaux – Unité d'éthique – La recherche sur dossiers** <http://ethique.msss.gouv.qc.ca/site/145.0.0.1.0.0.phtml>







**QUESTIONS?**