

SECURITY CONSIDERATIONS FOR SENSITIVE HUMAN RESEARCH DATA

Rachel Zand, PhD
SciNet Workshop
October 28, 2022



OVERVIEW

Brief description of sensitive data

Policies relevant to sensitive human research data

How Research Ethics Boards (REBs) evaluate sensitivity of data collected in the context of overall risk

Common privacy and security recommendations/requirements REBs make for various aspects of the research data life cycle

Areas of vulnerability/ gaps in knowledge or technology

Cautionary real-life tales

Responsibilities for RDM beyond the REB

SENSITIVE DATA

Any data that, if released to the public, would have an adverse effect or cause potential harm to an individual, community, group or organization.

Personal information/ Personally identifiable information (PII)

Personal health information (PHI)

Educational records

Financial information

Criminal information

Geographic information

Confidential personnel/administrative information

Information entrusted with intent that it be kept private

Information protected by institutional policy

POLICIES AND STANDARDS RELEVANT TO SENSITIVE HUMAN RESEARCH DATA

Tri-Council policy statement: Ethical conduct for research involving humans (TCPS2)

Privacy legislation

Tri-Agency research data management (RDM) policy

- Institutional RDM strategy

Tri-Agency statement of principles on digital data management

Institutional policies and guidelines

TRI-COUNCIL POLICY STATEMENT (2018) (TCPS2)

Requirements for Canadian institutions on conducting and reviewing human research

Fundamental principles: Respect for persons, Concern for welfare, Justice

Research Ethics Board (REB): body to review all human research conducted at or under the auspices of the institution for ethical acceptability

- Diversity of members
- knowledgeable in fields and methods,
- knowledgeable in law
- knowledgeable in ethics
- Community representation

TCPS2

Privacy – the right to control information about oneself – expressed through consent

Confidentiality – obligation to safeguard entrusted information

Security – physical, administrative and technical safeguards of information

Identifiability:

- Directly identifiable
- Indirectly identifiable
- Coded – direct identifier removed and replaced by a code
- Anonymized – irrevocably stripped of identifiers, code discarded
- Anonymous – never had identifiers

REBs need to determine that researchers have appropriately planned for and will maintain compliance with privacy, confidentiality and data security requirements

PRIVACY LEGISLATION (ONTARIO)

Personal health information protection act (PHIPA)

Freedom of information and protection of privacy act (FIPPA)

- Use of personal health information or administrative records (e.g. student records, grades, HR records) for research purposes
- Consent-driven or with REB-approved waiver
- REB-approved research plan
- Used only for approved purposes
- Not disclosed or accessed by unauthorized individuals – must specify who on research team has access
- Returned or destroyed at the end of the research

TRI-AGENCY RESEARCH DATA MANAGEMENT POLICY (2021)

Institutional strategies: By March 1, 2023, research institutions subject to this requirement must post their RDM strategies and notify the agencies when they have done so.

Data management plans (DMPs): Starting spring 2022, the agencies are identifying funding opportunities that are subject to the data management plan requirement.

Data deposit: After reviewing the institutional RDM strategies, and in line with the readiness of the Canadian research community, the agencies will phase in the deposit requirement.

INSTITUTIONAL RDM STRATEGY

Recognize data as an important research output

Promote importance of data management

Support, guide, adopt best practices and provide tools to researchers to establish and implement data management practices

Provide or support access to repository services

Recognize that Indigenous RDM policies are determined by Indigenous communities

Data created about or by Indigenous communities are owned by them and should follow their RDM policies

DATA MANAGEMENT PLAN (DMP)

Living document that describes all stages of RDM:

- Data collection
- Documentation and metadata
- Storage and backup
- Preservation for long term access
- Sharing and reuse
- Responsibilities and resources of research team/ data custodian
- Ethical and legal compliance as relates to data retention, deposit, future uses



Digital Research
Alliance of Canada

Alliance de recherche
numérique du Canada

[Français](#)

[About](#) ▾ [Membership](#) ▾ [Services](#) ▾ [Funding Opportunities](#) [Initiatives](#) ▾ [Latest](#) ▾ [Contact](#)

[Home](#) / [Services](#) / [Research Data Management](#) / DMP Assistant

About

Membership

Services

Our Services

Advanced Research Computing

Research Data Management

FRDR

DMP Assistant

Learning and Training

Glossaries

DMP Assistant

The DMP Assistant is a national, online, bilingual data management planning tool developed by the Digital Research Alliance of Canada (the Alliance) in collaboration with host institution University of Alberta to assist researchers in preparing data management plans (DMPs). This tool is freely available to all researchers and develops a DMP through a series of key data management questions, supported by best-practice guidance and examples.

DMPs are one of the foundations of good research data management (RDM), an international best practice, and increasingly required by institutions and funders, including the Canadian Tri-Agencies as outlined in their [Research Data Management Policy](#).¹²

TRI-AGENCY STATEMENT OF PRINCIPLES ON DIGITAL DATA MANAGEMENT (2016, UPDATED 2021)

Importance of making the results of Tri-Agency funded research accessible to other researchers

Global awareness of the value of digital research data

DMP requirements

Publicly accessible


Properly acknowledged

INSTITUTIONAL POLICIES AND GUIDELINES

Data access requests

Recruitment of institutional members for surveys

Other institutions may have other policies or processes, including review by the REB

 UNIVERSITY OF
TORONTO | Institutional Research & Data Governance

Home About Us Institutional Data Governance Institutional Reports

Data Access Request

The institutional administrative data managed by UTBI is available to all staff that have a need to access data as part of their role. To receive access to the data, please do the following:

1. Download the data access form: <https://easi.its.utoronto.ca/wp-content/uploads/2017/05/UTBI-Request-Form.pdf>
2. Complete the form and select the required data sets.
3. Obtain your supervisor's approval and signature.
4. Scan and e-mail the form to access.easi@utoronto.ca

Please note: Access policies and procedures will be reviewed by the Data Governance Committee and are subject to change at a later date.

© University of Toronto
data@utoronto.ca
27 King's College Circle
Toronto, ON, Canada
M5S 1A1

Division of the
Vice-President & Provost

 UNIVERSITY OF
TORONTO

ABOUT PLANNING & POLICY COMMITTEES AWARDS & FUNDING MEN

Surveying of U of T Students, Faculty, Librarians, Staff, and Alumni by U of T Researchers, Guideline on

🏠 / Planning & Policy / Surveying of U of T Students, Faculty, Librarians, Staff, and Alumni by U of T Researchers, Guideline on

October 2020

A great deal of research involving members of the university community is conducted at the University of Toronto. Most of this research is governed by regulations within individual faculties and departments, and by regulations and procedures set forth in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (2018). The Office of the Vice-President, Research and Innovation maintains Research Ethics Boards (REBs) that must approve most research involving human participants.

This guideline establishes additional procedures for prior approval of proposed **surveys** of U of T students, faculty, librarians, staff, or alumni that will be undertaken **for research purposes** by U of T students, faculty, librarians, and staff.

This prior approval is being required given that the University also conducts quality assurance surveys of its community members, and it is important to avoid conflict among surveys, repetition, and the possibility of 'survey fatigue' that might reduce responses.

All requests to survey U of T postgraduate medical education fellows ('medical residents') should be sent to the Vice-Dean, Post-MD Education within the Temerty Faculty of Medicine, at adogme@utoronto.ca rather than through the process outlined in this guideline. (Requests to survey MD program students use the process in this guideline.)

REB MANAGEMENT OF SENSITIVE HUMAN RESEARCH DATA

As determined by:

Method/sensitivity of the topic

Location of the research (geo-political context)

Vulnerability of participant group

Identifiability

Regulations and policies (Canada, and host country)

Considerations are multi-faceted and nuanced

REB DETERMINATION OF RISK

Group Vulnerability	Research Risk		
	Low	Medium	High
Low	1	1	2
Medium	1	2	3
High	2	3	3

Risk level 1 – minimal risk, reviewed by delegated process – 1-2 members of the REB

Risk levels 2 and 3 – reviewed at full board; subject to post-approval review visits

Sensitivity of data may be influenced by both research risk and group vulnerability

REB-RECOMMENDED DATA SECURITY STRATEGIES

What is often recommended

Gaps, weaknesses with recommendations

Situations that have arisen

1. LIMIT SENSITIVE DATA COLLECTION

Only collect as much/what is needed for the research

Use methods that allow for anonymous data collection (e.g. surveys)

Use pseudonyms when possible

Choose a less vulnerable participant group (e.g. advocates)

Limits further analyses, usefulness of dataset

Most research requires follow up with participants

May need specific participant group, otherwise may compromise the research

Anonymity can lead to poor quality responses

Pseudonyms may be identifiable, if used often

Considerations re IP address and other potential identifiers

EXTERNAL PRESSURE TO DISCLOSE RESEARCH DATA (WHEN PSEUDONYMS DON'T WORK)

Quebec court keeps criminologists' research with Luka Magnotta out of police hands

Adam Feibel © 2014/01/30, 5:39 am



U of O profs stress importance of confidentiality in criminal investigations

Photo by Adam Feibel

The two University of Ottawa professors who conducted a research study that included an interview with accused killer Luka Magnotta have won their legal bid to quash a Montreal police warrant for the video.

Professors Christine Bruckert and Colette Parent took the matter to court last March in order to

Christine Bruckert and Colette Parent U of Ottawa 2013

Went to court to challenge the seizure of a video interview with (now convicted) killer Luka Magnotta

“Jimmy” was interviewed for “Sex Work and Intimacy: Escorts and Their Clients” that took place between 2004 and 2008

Magnotta was one of 20 male escorts, 20 female escorts, and 20 clients of escorts who agreed to participate in the study under the promise of confidentiality

Wigmore criteria used

Quebec Superior Court Justice ruled that the importance of preserving the relationship between the researcher and the subject outweighed the video's usefulness to police

2. ENSURE PHYSICAL SECURITY

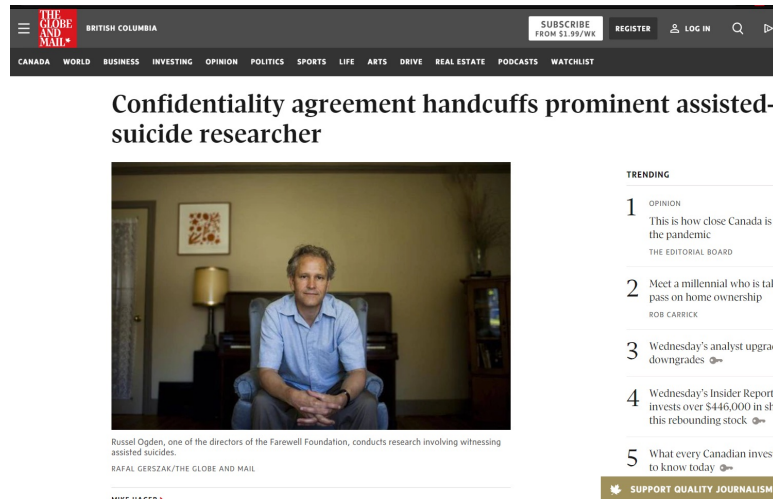
Locked cabinet in locked office for hard copy records

Clean desk policy

When possible, minimize data carried on your person, or in your car



EXTERNAL PRESSURE TO DISCLOSE RESEARCH DATA (2) (WHEN NECESSARY, BURY YOUR DATA)



Russell Ogden – SFU 1994

Assisted suicide

Interviewed individuals involved and witnessed 11 assisted suicides

Promised “absolute confidentiality” to participants

Vancouver Coroner subpoenaed Ogden to appear to provide information at an inquest; Ogden refused to reveal identities

Coroner threatened contempt of court

Ogden’s legal argument was that his research met the Wigmore criteria for confidential privilege

Buried his research data (physical books) to prevent seizure

3. ELECTRONIC SAFEGUARDS

Encrypt all devices

Use VPNs when not on a secure server (e.g. for international research)

Save data onto OneDrive or SharePoint for secure access by team members (DropBox?)

Acceptable platforms for online research: REDCap (institutional storage), Qualtrics, SurveyMonkey (if using Canadian account)

Do not use US-based servers for sensitive data, particularly if identifiable or potentially re-identifiable – PATRIOT Act

- Some regions in Canada won't allow use of online platforms with servers in US, others require disclosure and consent of participants

Data may not be encrypted when in use, vulnerable to unauthorized access

Illegal to bring in encrypted devices to some countries

- Iran, China

Internet and/or VPNs may be unavailable or unreliable

- Rural areas
- Countries with authoritarian regimes – often the focus of the research

Researchers may be forced to show data at border crossings

Institutions and organizations must have appropriate security for short and long-term data storage for all data risk levels

4. VIRTUAL RESEARCH SAFEGUARDS

Evolution of Zoom for research purposes

- Concerns regarding zoom-bombing, ability to hack transmissions, recordings
- Now have institutional licenses with password protection
- Encryption has been improved
- Questions regarding use for PHI-involved research

Ongoing concerns

- Setting of where virtual research taking place
- Privacy for participants and researchers - Can others hear/see conversations?
- Can researchers see other members of participant's household
- Problematic for some research

5. SECONDARY USE OF PHI OR PII DATA

Datasets that were collected for clinical or administrative purposes, but are now being analyzed for research, or collected for a specific research purpose, and now available for other projects

- Standard research
- AI/ML research

Data custody and security, short and long term

Determination of what research is acceptable to use them - how and by whom?

Ethical concerns?

Business

LinkedIn experiment changed job prospects for millions – and it raises red flags: privacy experts



Academics suggest Canada needs stricter laws on consent and how companies use people's data



[Kiernan Green](#) · CBC · Posted: Oct 23, 2022 4:00 AM ET | Last Updated: October 25



ACCESS CONCERNS BEYOND THE REB

Unauthorized access to research data due to:

Department or research team mishandling

- Multi-lab access to one license
- Forgetting to remove access when team members leave

Phishing emails to obtain passwords

Research team members may have conflicts of interest*

Inadvertent access by friends, (ex-)partners, family members who access shared devices and/or have known passwords

Calgary

University of Calgary paid \$20K in ransomware attack



No evidence cyberattackers released personal or university data to public

CBC News · Posted: Jun 07, 2016 2:27 PM MT | Last Updated: June 8, 2016

Inadequate Security, Policies Led to LifeLabs Data Breach of 15M Patients

An audit into LifeLab's 2019 massive data breach by B.C. and Ontario privacy commissioners found the testing giant collected more PHI than necessary and lacked adequate security policies and procedures to protect patient data.

5 OCT 2022 NEWS

Canadian Sentenced to 20 Years in US Prison For Ransomware Attacks

Increased foreign threat to COVID-19 research prompts extraordinary warning from Canada's spy agencies



Warning comes a day after the U.S. intelligence agencies cited China-backed online attacks

Catharine Tunney · CBC News · Posted: May 14, 2020 3:57 PM ET | Last Updated: May 15, 2020



1153 comments

Canada's spy agencies are warning that Canadian intellectual property linked to the pandemic is a "valuable target" for state-sponsored actors — just a day after U.S. intelligence agencies warned of China-backed hacking of institutions and companies researching vaccines, treatments and tests for the novel coronavirus.

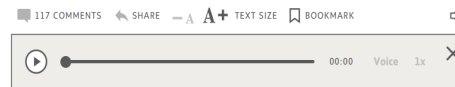
"The Communications Security Establishment has assessed that it is near certain that state-

CSIS warns about China's efforts to recruit Canadian scientists

ROBERT FIFE · OTTAWA BUREAU CHIEF
STEVEN CHASE · SENIOR PARLIAMENTARY REPORTER
OTTAWA
PUBLISHED AUGUST 6, 2020

PUBLISHED AUGUST 6, 2020

This article was published more than 6 months ago. Some information in it may no longer be current.



The Canadian Security Intelligence Service has warned the country's universities and research institutions that Beijing is using academic recruitment programs such as its Thousand Talents Plan to attract scientists to China in hopes of obtaining cutting-edge science and technology for economic and military advantage.

The federal spy agency says the Thousand Talents Plan (TTP), which Beijing created in 2008 to identify and recruit leading scientific experts around the globe, is an example of the way China is attempting to get academics to share — either

TRENDING

- 1 Royal Bank expands reach into booming Canadian tech sector with new RBCx platform
- 2 Why lumber prices are down 36% from the peak
- 3 CREA revises home price forecast, sees 19% increase this year
- 4 OPINION
Why I've accepted an honorary doctorate from a school named after Egerton Ryerson
TANYA TALAGA
- 5 OPINION
Hitting 'Control-Alt-Delete' on the

SUPPORT QUALITY JOURNALISM.

DATA DEPOSIT AND FUTURE USE

REBs don't review beyond consent information, not responsible for reviewing DMPs

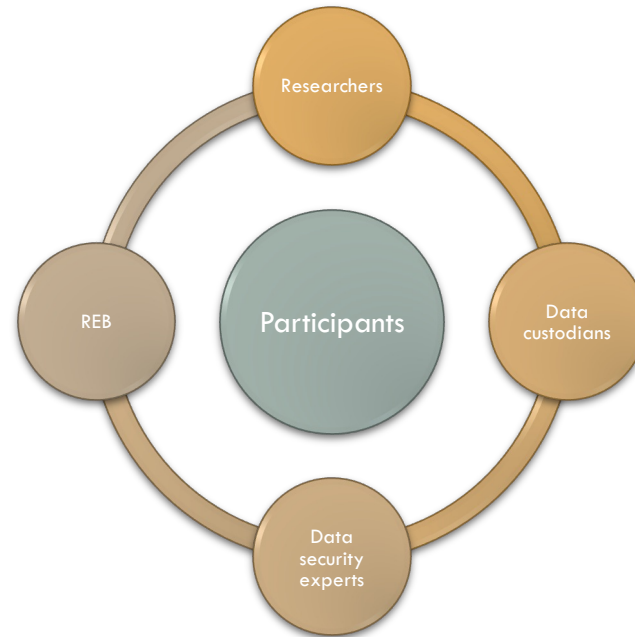
Appears to be a gap between REB, data custodians

- Who ensures sensitive data are appropriately de-identified, protected?
- Requirement for projects involving anonymized data (once had identifiers) to be submitted for review

Solution may be part of implementing Institutional RDM strategies

Communication between data security professionals, data custodians, researchers and REB necessary

DATA SECURITY AS A JOINT RESPONSIBILITY



SUMMARY

Sensitive data encompass a wide range of types and risks

There are various policies that govern collection, use and management of sensitive human data

Recommendations may include considerations of what data will be collected and from whom, physical and electronic security measures

These recommendations may not always be sufficient, and researchers need to be cognizant of potential risks to data security

Also, data deposit and long-term storage are beyond the scope of the REB, requiring other roles within institutions to take ownership of data security issues

Security of sensitive human research data is a joint responsibility between REBs, researchers, data custodians and data security experts



QUESTIONS?

rachel.zand@utoronto.ca