

Data storage of human participant data – the REB perspective

April 19, 2018

Catherine Paquet

Directrice, Bureau d'éthique et d'intégrité de la recherche (BEIR)

Director, Office of Research Ethics and Integrity (OREI)

cpaquet@uOttawa.ca | 613-562-5800 Ext. 1787
<http://www.research.uottawa.ca/ethics/index.html>



uOttawa

Le Bureau d'éthique et d'intégrité de la recherche The Office of Research Ethics and Integrity

Depuis / Since 2009*

- Éthique de la recherche avec les êtres humain
- Research ethics – humans

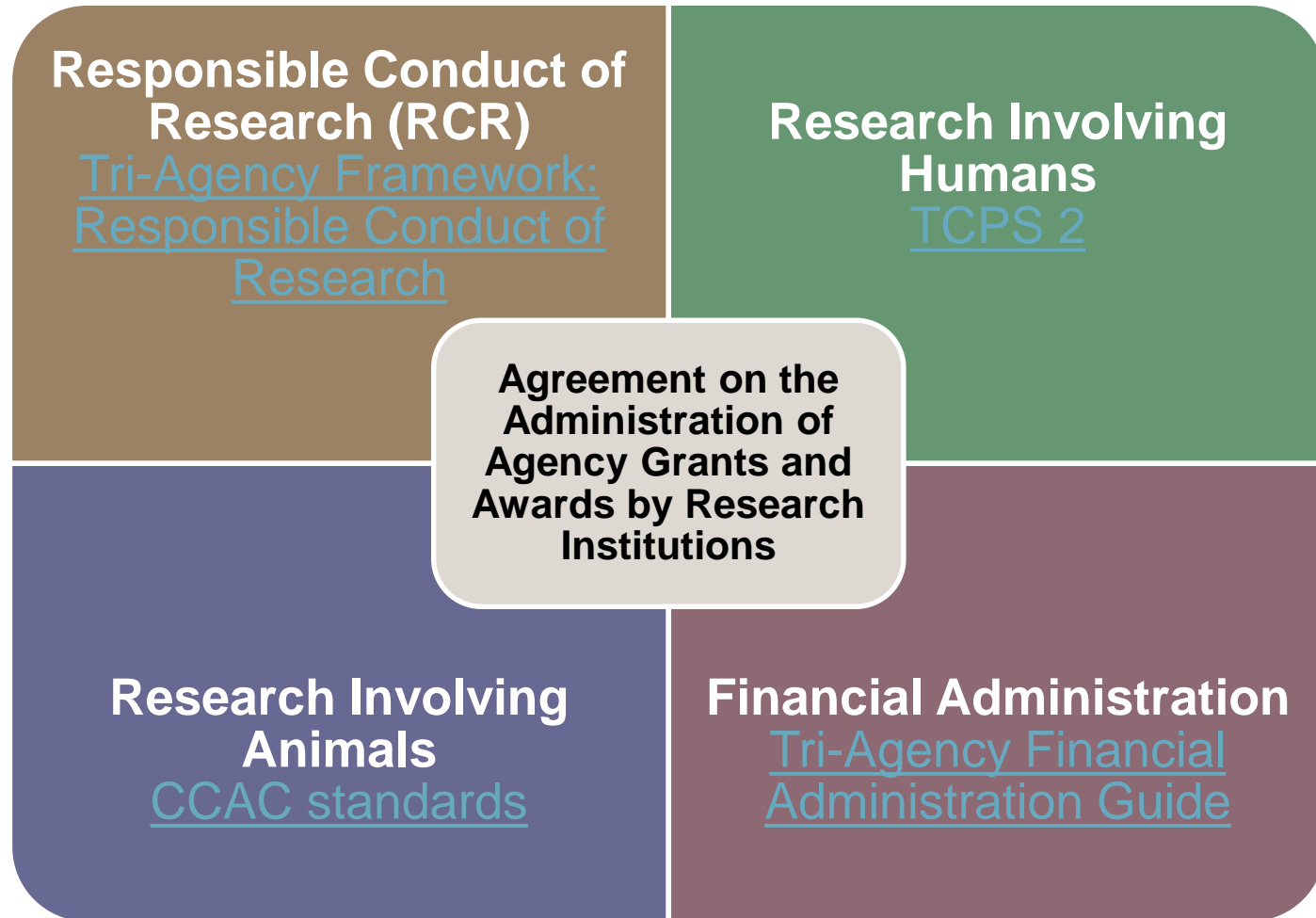


Depuis / Since 2011

- Conduite Responsable de la recherche
- Responsible Conduct of Research

- Service de consultation pour les chercheurs / Consultation service for researchers
- Ateliers offerts aux professeurs, étudiants, membres de CÉR / Workshops offered to professors, students, REB members
- Information & ressources sur notre site Web / Web site information & resources
- Travaille avec les chercheurs de l'Université pour s'assurer que leurs projets de recherche respectent les politiques établies par les Organismes fédéraux (CRSH, IRSC, CRSNG) / works with researchers to ensure that their research projects meet the requirements of the tri-councils

Tri-Agency Policies



Mandat des CÉR

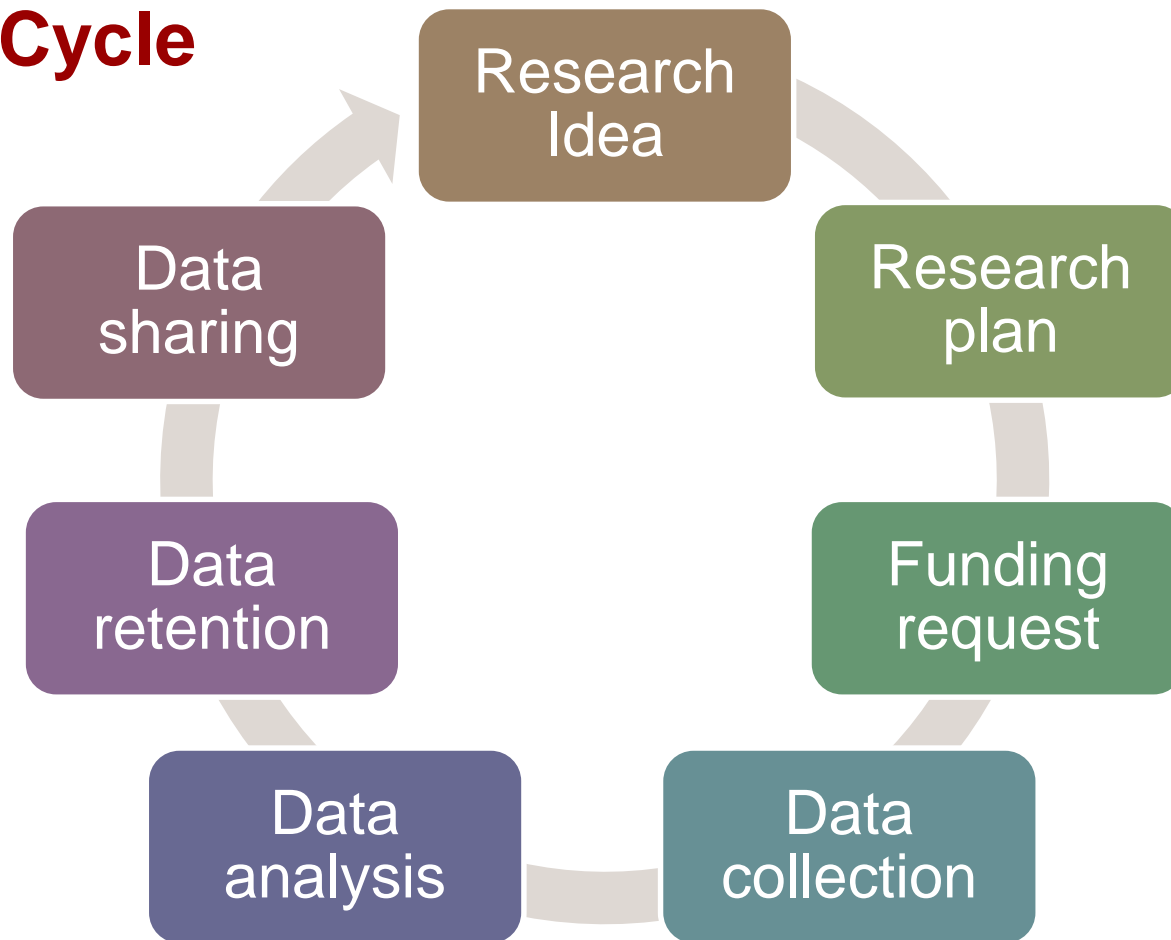
REB Mandate

- Les établissements doivent constituer ou mandater des CÉR pour évaluer, conformément à la présente politique, l'acceptabilité éthique de tout projet de recherche avec des êtres humains réalisé sous leur autorité ou sous leurs auspices, c'est-à-dire par les membres de leur corps professoral, leurs employés ou leurs étudiants, et ce, peu importe l'endroit où les travaux de recherche sont exécutés. (ÉPTC 2, Article 6.1)
- Institutions shall establish or appoint REB(s) to review the ethical acceptability of all research involving humans conducted within their jurisdiction or under their auspices, that is, by their faculty, staff or students, regardless of where the research is conducted, in accordance with this Policy. (TCPS 2 Article 6.1)

Application of the Policy (Chapters 1 & 2)

- In the context of both initial and continuing research ethics review, the REB assesses the **ethical acceptability** of a research project through consideration of the **foreseeable risks**, the **potential benefits** and the **ethical implications** of the project (see Article 2.9).
- In designing and conducting research or reviewing the ethics of research, researchers and REBs must be mindful of the **perspective of the participant**.

Research Cycle



Researcher responsibilities

(RCR Framework Article 2.1.2; uOttawa Procedure 29-2, Article 5)



Follow best research practices honestly, accountably, openly and fairly

Follow institutional policies & professional or disciplinary standards

i.e. Know the rules and follow them

Comply with applicable laws and regulations

Things the REB needs to consider when reviewing a research project

What type of data is being collected?

How / where is it being collected?

How / where is it being stored?
For how long?
Is it secure?

Who will use it?

Who will access it at different time points?

- During: PI; Supervisor; Co-researchers; RA; Other(s)
- After: (as above +) journals, other researchers, 2nd use

Always need to consider

- Sensitivity of the data
- Risks to participants;
 - If there are risks, do the benefits outweigh them?
- What is reasonable in the specific research environment?

Things the REB needs to consider (cont'd)

Possible harms in case of data breach

- Legal repercussions (e.g., possibility of participant being sued, charged with criminal activity)
- Social repercussions (e.g., possibility of marginalization, being negatively judged by peers or employer)
- Breach of privacy (sensitive information)

De-identification of data

- Limits exist
- Anonymity does not mean that individuals cannot be identified
- De-identification can affect the worth / relevance of some data
- Not always necessary

What the TCPS 2 says

- Issues are related to privacy, confidentiality and data conservation ([Chapter 5](#) and [Article 10.4](#))
- **Security** refers to measures used to protect information. It includes physical, administrative and technical safeguards. [...] Physical safeguards include the use of locked filing cabinets, and the location of computers containing research data away from public areas. Administrative safeguards include the development and enforcement of organizational rules about who has access to personal information about participants. Technical safeguards include use of computer passwords, firewalls, anti-virus software, encryption and other measures that protect data from unauthorized access, loss or modification.
- **Identifiable Information**
- Where researchers seek to collect, use, share and access different types of information or data about participants, they are expected to determine whether the information or data proposed in research may reasonably be expected to identify an individual. For the purposes of this Policy, researchers and REBs shall consider whether information is identifiable or non-identifiable. Information is identifiable if it may reasonably be expected to identify an individual, when used alone or combined with other available information. Information is non-identifiable if it does not identify an individual, for all practical purposes, when used alone or combined with other available information. The term “personal information” generally denotes identifiable information about an individual. The assessment of whether information is identifiable is made in the context of a specific research project.
- “Ethical concerns regarding privacy decrease as it becomes more difficult (or impossible) to associate information with a particular individual. These concerns also vary with the sensitivity of the information and the extent to which access, use or disclosure may harm an individual or group.

Challenges in assessing ethics of data management

The Case

- A researcher will conduct interviews in Mexico with people who have conducted illegal activities.

Risks

- There is a risk of legal repercussion should participants be identified / the data be accessed by authorities
- Possible risk of physical harm to them (their families?)

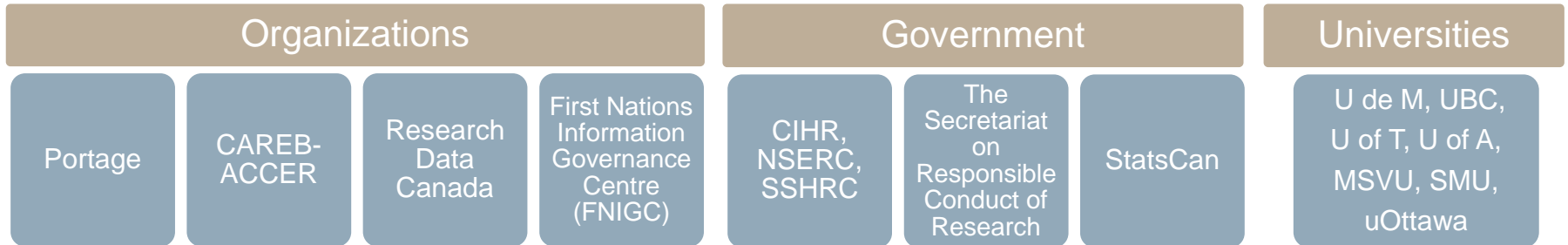
Issues to consider

- Where should the data be stored during the collection period, i.e. in Mexico?
 - Better to keep on a secure device vs. cloud?
- Is there a risk (loss, theft, access by authorities) during travel (e.g., at airport)?
- What type of confidentiality measures have been put in place?
 - How is consent obtained – is there a consent form? A signed consent document could put participants at risk.
 - What information is provided to participants in terms of confidentiality assurances?
- Where should the data be stored after the collection period?
Is it possible that the data could lead to identification of participants, even if they are not named (e.g. age, gender, location, other characteristic(s))?

DISCUSSION

Portage Working Group on Responsible Research Data Management Practices for Sensitive Data

Members include people from



Mandate

The group will identify best practices from both the international community and Canadian experiences, while investigating and addressing ethical issues surrounding research data. This work will help Portage and other organizations develop both practical and policy responses to the RDM needs of Canadian researchers and will contribute to the expertise of the broader RDM community of practice in Canada. Outcomes from this group are anticipated to have value in the research ethics application process and would be integrated into Data Management Plan (DMP) templates on the Portage-supported DMP Assistant.

Working groups

1. Developing guidelines and best practices for handling sensitive data for research ethics forms, linking ethics form text to DMPs, and providing guidance on data access agreements for research data repositories
2. Creating training materials to facilitate relationships and awareness between researchers, research ethics boards, libraries, and other institutional stakeholders (e.g., finding/modifying and/or creating a workflow decision-making tree/ flowchart)
3. Environmental scan of practices for the management of Indigenous data

QUESTIONS?