Managing Human Research Data and getting through the ethics process

Our “top 10” tips

Presenters:
Erin MacPherson, Research Data Management Librarian & Liaison, Faculty of Agriculture
Angela Hersey, Manager, Research Ethics

May 2019
Today

1. Why we care about managing human data
2. Top 10 tips for ethical human data management
3. Developing a research data management plan
Part 1
Why we care about managing human data
Why data management?

Some of the reasons include:

- Protect data from destruction
- Protect data from breaches or leaks
- Help ensure *rigour in research*
- Reduce redundances
- Be compliant with laws and policies
- Maintain public trust in research institutions and *researchers*
- Uphold ethical duty to safeguard information of participants
Audit on a $1 million study at the University of Manitoba revealed the personal health information of more than 400 participants was breached.

Data was stored off-site, without encryption with allowed for the potential for it to be accessed by a third-party company.

The Personal Health Information Act (PHIA) breach meant all tests and data from participants had to be destroyed and could no longer be used in the study.

Data loss: Manchester cancer hospital fire

“...We’ve almost certainly lost data where computers have been ruined. We’re going to go in and salvage as much of that as possible...”

“...institute was very concerned about any research it may have lost and so were “PhD students, postdoctoral fellows and group leaders carrying out experiments which were abruptly ended.”

The report was accidentally sent to two facilitators unconnected with the particular groups in this program.

Department officials first became aware in May.

Report was password protected so access to individual farmers information was not readily available.

Farmers were notified of data leak in early June.

Department immediately put corrective procedures in place.

Theft: laptop stolen from employee car

A laptop with personal and health information from research studies was stolen from the car of an employee (a computer programmer) at the Feinstein Institute for Medical Research.

- Computer and health information were password protected.
- Couldn't rule out that the data couldn’t be accessed.
- Laptop was unencrypted.
- ALL current and past participants research studies had to be contacted.
- The Institute was ultimately fined $3.9 million to settle allegations that they violated HIPAA Privacy and Security Rules.


We have the tools and resources to help you manage human research data and minimize risk.

Part 2
Top 10 tips for ethical management of human data
What is human research data?

- Human research data is...
  - Directly and indirectly identifiable information about individuals (personal details like name, income, number of children, level of education, etc.)
  - Opinions, experiences, and perspectives provided by people for research (may or may not be identifiable)
  - Health information about individuals
  - Opinions about other people
- ...collected directly from individuals, or used secondarily (was collected for other research purposes or non-research purposes)...
- ...not available publicly (i.e. through Statistics Canada, aggregated and presented in research papers, on public websites/social media sites, etc.).
1. Privacy is a process

- This is why you need a RDM plan!
2. Know the rules

- Tri-council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2)
- Tri-Agency Statement of Principles on Digital Data Management (adopted June, 2016)
- Dalhousie University Policy for the Protection of Personal Information from Access Outside Canada
- Personal Information International Disclosure Protection Act
- Personal Health Information Act (NS provincial legislation)
3. Limit collection

- Only collect what you need for the research

Image Source: https://d1qqglw5ow8lz.cloudfront.net/live-images-1/ImageDetail_cee410fd-6a11-449b-8537-3992eb57ed43_Medium
4. Storage

- Short, medium, long-term storage
- How secure?
- Separate from identifiers
- Physical location

5. Transfer

- Transfer = vulnerability
- Personally identifying info?
- To another device
- To another person
- Traveling

6. Remove identifiers

- Many types of identifiers
- De-identify or anonymize ASAP = reduced risk
- Voices – transcribe & delete
- Keep only what you need for the research
7. Encrypt

- Encrypt all personally identifiable info & master code documents
- For file encryption, Dal recommends **Vera Crypt**
- For computer encryption, **FileVault** (Mac), and **BitLocker** (Windows)
- Visit the IT Help Desk for more info and assistance
8. Protect

**From:**
- Physical loss & theft
- Access by unauthorized parties

**By:**
- Encrypting data
- Transferring properly (e.g. File Exchange)
- Being cautious about physical transfer (e.g. USB)
- Keeping laptop in sight
- Using locks (for physical data), password protection & auto timeouts (for computers)
- Keeping appropriate back-ups
9. Destroy (?)

- If disciplinary standards allow it, plan to delete human data when it is no longer needed for research.
- Partial deletion is also an option (e.g. participant code keys).

Image source: https://www.incimages.com/uploaded_files/image/1940x900/getty_635923424_360310.jpg
10. What not to do

- Don't use Dropbox, Google Drive, Evernote, Box or other cloud-based storage devices
- Avoid using USBs when possible, especially for long term storage
- Don't use OneDrive if using personal health data
- Don't auto-sync to the cloud (e.g. Voice memo on i-phones)
- Don't use non-institutional email addresses for university work
Part 3
Developing a Research Data Management (RDM) Plan
Make a Research Data Management plan

Be practical! - Develop a plan that takes into account the security and safety of participant data, but also one that is practical and makes sense for the research team. Make sure each step in the process follows best electronic data security practices.

Make it easy - Use the DMP Assistant!

- Online tool
- Guided questions on almost all aspects of the data management.
- Share and collaborate with members of your research team to develop a plan collaboratively
- Update it when necessary.
- Create an account to get started!

DMP Assistant: https://assistant.portagenetwork.ca/

Resources for data management planning: http://dal.ca.libguides.com/rdm/plan
Helpful Readings & Links


DMP Assistant: [https://assistant.portagenetwork.ca/](https://assistant.portagenetwork.ca/)


We can help

- **Research Data Management:** Contact the Dalhousie RDM team at data.management@dal.ca

- **Advanced Research Computing & ACENET:** Contact ACENET's Research Consultant for Data Management lee.wilson@ace-net.ca

- **Copyright:** Contact the Dalhousie Copyright Office.

- **Research Ethics:** Contact Dalhousie Research Ethics ethics@dal.ca

- **Privacy Officer:** Contact the Dalhousie Privacy Officer FOIPOP@dal.ca
Questions?

Contact info:

Erin MacPherson: erin.macpherson@dal.ca
Angela Hersey: angela.hersey@dal.ca