DALHOUSIE
UNIVERSITY

Protecting Electronically Stored Personally Identifiable Research Data

Quick Reference for Dalhousie Researchers
Prepared by Dalhousie Research Ethics, Privacy and Information Security Offices
Updated November 2024

Research participants trust researchers to manage their personal data in a way that is secure and ensures privacy, especially for personally identifiable information. This document has been prepared to help researchers plan their research projects in ways that ensure participants' data are kept securely.

Definitions:

"Information is identifiable if it may reasonably be expected to identify an individual, when used alone or combined with other available information."[1]

""Personal information" means recorded information about an identifiable individual, including, but not limited to:

a. name, address, telephone, email (personal not business);
b. race, ethnic origin or religious political beliefs or associations;
c. age, sex, sexual orientation, marital status or family status;
d. any identifying number or symbol (examples: Dalcard ID, SIN, credit card, health insurance, drivers' licence);
e. fingerprints, blood type, or inheritable characteristics;
f. medical or personal history;
g. educational, employment, financial, or criminal history;
h. personal views or opinion"[2]

It is the ethical responsibility of researchers to take appropriate steps to protect these data throughout the lifecycle of research.

General guidelines:

1) Decide where to keep different types of participant research information:

It is important to keep personally identifiable participant information, or codes that link participants to their data, separate from the actual data. The main reason is that if one device/drive (e.g. a laptop) is accessed, participants cannot be re-identified by simply matching up the two documents. It is also preferable that devices be physically stored separately. When deciding where to store codes and/or participant data, researchers should know about the tools Dalhousie offers, along with some important considerations about which ones to use:

[1] Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, December 2022. Chapter 2.

[2] *Policy for the Protection of Personal Information from Access Outside Canada*, Dalhousie University (2007).

- **OneDrive/SharePoint** – Almost all research data may be stored on OneDrive/SharePoint (with some limited exceptions[3]). SharePoint as a collaboration tool requires training to be used effectively. You must be aware of who can see the content and stay on top of permissions and access.
- **NAS drive (O:\drive)** – A network-attached-storage (NAS) device is available to faculty, and to students with permission by their department, and is appropriate for storing certain types of sensitive research data. Files and folders can be granted restricted access. Data from the NAS are stored on secure Dalhousie servers, and can be accessed when connected to the Dal network, or off-campus anywhere in the world through Dal's virtual private network. The NAS is not encrypted by default, and extra steps are required to properly secure content on the NAS with encryption. *Note: use of NAS may be subject to a fee*.

Additional information is available in Dalhousie's *Electronic Information Storage Guidelines*.

2) Prevent data theft/loss

Theft or loss of data is possible. It is the researcher's responsibility to take precautions to prevent this from happening, and that means being smart with where data are stored and how accessible they can be by an outside party. Here are a few good practices:

- **Encrypt data** – Dalhousie recommends that all data storage locations/devices (e.g. computers, tablets, phones, USB drives, etc.) use automatic encryption. Alternatively, auto- encrypting storage services can be used (OneDrive/SharePoint, etc.); these services automatically encrypt data and store it on Canadian servers. If you require extra protection for specific files or intend to use the Dalhousie NAS (O:\ drive), a solution such as VeraCrypt can be used to encrypt specific research data files.
- **Encrypt your laptop** – FileVault is a tool available for Macs. BitLocker is available for Windows.
- **Encrypt external hard drives** – Always encrypt external hard drives that store research data. You can do this with either FileVault or Bitlocker (or with external drives that come with their own built-in encryption solutions which are cross-platform).
- **Avoid using USB keys** – USB keys are small and easy to lose or have stolen. They are also generally not very stable in the long term. USB keys should be used as a last option, and they should always be encrypted and secured with a password.
- **Store on NAS** – This is only accessible with a Dalhousie NetID and password. If you are off-campus, you must connect through a VPN (see second bullet in section 1, above). Please note that this solution is not encrypted by default and is only recommended for certain data storage solutions. The NAS could be considered as a data storage solution when research data providers (e.g. data custodians) require non-cloud storage.
- **Password-protect computer, laptop, and phone** – Always password protect laptops, computers and any other devices. Set a time-out as well so it automatically locks after a few minutes.
- **Watch your device** – Laptops, USB keys, mobile devices, voice recorders, etc. should be stored safely – lock them in a drawer or other physically secure area when not using them.

[3] To comply with provincial legislation, Personal Health Information of participants that is protected by the Nova Scotia Personal Health Information Act, and/or Payment Card Industry regulated (card holder) financial data cannot be stored on OneDrive. More detailed information can be found here: https://dalu.sharepoint.com/sites/its/docs/electronic-information-storage-guidelines.pdf. If you need to store personal health information, consult with the Dalhousie Privacy Office and Dalhousie ITS to develop a storage plan that complies with provincial legislation.

Transfer data properly

Sharing and sending data with others can introduce risks. The general rule of thumb is not to transfer via the cloud, and always use secure transfer methods for sending and receiving data. Here are some good options for sharing and transferring data:

- **Use OneDrive/SharePoint** – OneDrive has the capability to securely send and receive encrypted files between internal and external people (follow this link for instructions). SharePoint has better tools for secure sharing with research team members where access needs to be restricted (contact support@dal.ca for training).
- **Use Dalhousie/institutional emails only** – but do not email personally identifiable participant information (use OneDrive/SharePoint to share file links with this information). If using email, ensure the files are not going through a third-party service, like Gmail, which you should not be used for University work.
- **If transferring from mobile device to computer (e.g. audio interview data)** – use a cable when possible, or sync directly through Dalhousie-provided secure services such as OneDrive or SharePoint. Do not email files to yourself, or sync/transfer files via a non-Dalhousie cloud service over the Internet.

3) Destroy data properly

Devices/services that contain research data scheduled for destruction must be securely wiped or destroyed.

- Devices must be securely wiped so that the data is unrecoverable, or the device storage must be destroyed. Best practices for deletion/destruction can be found in this guide[4] (beginning on p. 32). Please reach out to support@dal.ca for assistance in determining the best way to destroy your devices/data.
- When a device is to be destroyed via a professional destruction service, it is recommended to be sent to the company currently under contract with Dalhousie for device destruction. A certificate of destruction can be provided by the company. If you require this service, please reach out to support@dal.ca.

4) If recording research sessions…

Sometimes you may want to record a research session with participants, such as interviews or focus groups. Recording interviews means that personally identifiable information is being collected about a person as their face and/or voice is personally identifying. Ensure participants are notified prior to each recording session and appropriate consent has been received. Keep in mind only to collect the information necessary for the purpose (consider when to start/stop recording and if audio only will suffice). There are various ways to record research sessions:

- **Microsoft Teams** – MS Teams is the recommended videoconferencing tool; it has been vetted by Dalhousie University for privacy compliance. Recordings are automatically stored in the researcher's OneDrive, which is housed on Canadian servers.
- **Voice memo for iPhone** – This is good for recording interviews. Avoid auto-syncing to i-cloud.
- **Hand-held recorder –** Use of recorders reduces the risk of personal information travelling over the internet and can sometimes be the simplest tool for recording interviews. Note that physical security measures should be in place to ensure the

[4] Or its successor. This document is the NIST 800-88 Security Standard and outlines procedures for best practices for deletion/destruction on various devices.

recorder and data are not lost (see section 2 above for advice on preventing theft or loss).

5) If storing data in a repository…

- If you plan to make data accessible in a research repository, it is normally most ethical to include non-identifiable information. If you plan to include any personally identifiable information, ensure you receive explicit consent to do so through the informed consent process.
    - Note that Dalhousie Libraries recommend Dataverse as a place to store research data long term. Please visit this Dalhousie Libraries information page for more information.

6) What not to use

Not all tools are suitable for storing participant research data due to storage and security risks. Do not store any personally identifying participant data on:

- Google Docs, Dropbox, Evernote, Box, or other cloud-based storage services not offered by Dalhousie.
- OneDrive, if using personal health information. SharePoint is usually the preferred solution for personal health information, but a consultation should be held with the Dalhousie Privacy and Information Security Offices.

7) Make a plan that works

- **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. Start by thinking what you'd like to do and then make sure each step in the process follows best electronic data security practices. There is more than one way to keep participant data secure.
- **Consult** – Schedule a consultation with the Dalhousie Privacy Office (foipop@dal.ca) and/or Information Security Office (info.security@dal.ca). These resources can help you build a data privacy and data security plan for your research.

For more information on Information Security at Dalhousie, please visit https://dalu.sharepoint.com/sites/its/SitePages/security-topics.aspx

Link to the *Personal Information International Disclosure Protection Act*: http://nslegislature.ca/legc/statutes/persinfo.htm

Link to the Dalhousie *Policy for the Protection of Personal Information from Access Outside Canada*: https://www.dal.ca/dept/university_secretariat/policies/governance/protection-of-personal-information-policy-.html

Link to the *Personal Health Information Act:* https://novascotia.ca/dhw/phia/