Protecting Electronically Stored Personally Identifiable Research Data

Quick Reference for Dalhousie Researchers

Prepared by Dalhousie Research Ethics and Information Technology Services

(ITS) Last updated August 2021

Research participants trust researchers to manage their personal data in a way that is secure and ensures privacy, especially for personally identifiable information. The TCPS2 (Tri-Council Policy Statement 2018) states that "information is identifiable if it may reasonably be expected to identify an individual, when used alone or combined with other available information." (The Dalhousie *Policy for the Protection of Personal Information from Access Outside Canada*[1] also defines the type of information that is considered personally identifiable.) It is the ethical responsibility of researchers to take appropriate steps to protect these data. The Dalhousie Research Ethics Boards in consultation with Dalhousie ITS have prepared this brief document to help researchers plan their research projects in ways that ensure participants' data are kept securely.

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:

- **OneDrive/SharePoint** – Almost all research data may be stored on OneDrive/SharePoint (with some limited exceptions[2]).
- **NAS drive (O:\ drive; formerly Novell)** – 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 is 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 VPN (virtual private network – see https://wireless.dal.ca/vpnsoftware.php for more information). 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*.
- **Personal Computer or Laptop** – If storing research data on a computer or device (e.g. external hard drive), the digital storage files must be encrypted and the device must be password protected. Set a time-out to automatically lock after a few minutes.

2) Prevent data theft/loss

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

- **Encrypt data** – Dalhousie recommends that all data storage locations/devices (e.g.

[1] *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

[2] To comply with provincial legislation, Personal Health Information (PHI) of participants that is protected by the NS Personal Health Information Act, and/or PCI 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 PHI, consult with the Dalhousie Privacy Office and Dalhousie ITS to develop a storage plan that is compliant with provincial legislation.

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, in the same way that you manage external hard drives.
- **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, or require offline backups (this might be based on data transfer agreements).
- **Password-protect computer, laptop, and phone** – Always password protect laptops, computers and any other device that stores research data. 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) 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.
- **Use Dalhousie/institutional emails only** – but do not email personally identifiable participant information (use OneDrive/SharePoint to share file links with them). If using email, ensure the files are not going through a third-party service, like Gmail, which you should never use 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.

4) 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[3] (beginning on p. 32). Please reach out to your support technician or support@dal.ca for assistance in determining the best way to destroy your devices/data.

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

- 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.

5) 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. There are various ways to record research sessions:

- **Microsoft Teams** – MS Teams is the recommended videoconferencing tool of choice. Recordings are automatically stored in the researcher's OneDrive, which is housed on Canadian Servers. Please review FAQ #13 on the research ethics website for further considerations about using videoconferencing software for research.
- **Voice memo for iPhone** – This is good for recording interviews. It is easy to prevent auto-syncing to i-cloud.
- **Hand-held recorder** – use of these devices 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 recorder and data are not lost (see section 2 above for advice on preventing theft or loss).

6) If storing in a data repository…

- If you plan to make data accessible in a research data repository it is best practice to only 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, and do a consultation with Dalhousie's Privacy Office.
    - Note that Dalhousie recommends Dataverse as a place to store research data long term. Please visit this Dalhousie Libraries information page for more information.

7) 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 (PHI). SharePoint is usually the preferred solution for PHI, but a consultation should be held with the Dalhousie Privacy and Information Security Offices.

8) 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 and/or Information Security Office. 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://www.dal.ca/dept/its/current.html

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/