Digital Data Collection

It is important to have a plan for digital data collection and storage in place before conducting research. Your application must include a description of how you will collect and store your data. The following information can assist you in building a plan for digital data collection and storage.

General Guidelines

1. Always keep an unedited copy of the original data file(s). You never know when you might be called upon to verify your original data!
2. Store your data on a secure, password-protected device. Do NOT share the access password with anyone who is not an approved member of the research team.
3. It is preferable to store your data on a password-protected external hard drive, which can then be locked away in a secure cabinet when not in use. Using a disconnected device avoids any and all issues related to account or network hacking.
4. Be sure to specify in your research plan how data will be stored, and how and when it will be disposed of when no longer required.

Using Digital Devices to Collect Data (such as mobile devices)

1. Ensure that your device is either password or biometrically-protected.
2. It is preferable to use a removable storage card (i.e. a micro-SD card), and to configure your device so that it saves the data you are collecting to the removable storage.
3. Transfer any data collected (images, video, audio files, etc.) to your password-protected computer (see General Guidelines) immediately.
4. It is advisable to copy the data from your device to your computer, rather than to “move” it (especially when not using a removable storage card). Verify that the file has transferred properly. Then, delete the file from your portable digital device.
5. If you are using a removable storage card, you can keep a copy of the collected data on that card – be sure to follow general guidelines about securing physical storage of that card. Do NOT keep a removable storage card with collected data in your portable device.

Using Online Applications to Collect Data

1. Use institutionally licensed and controlled data collection applications (such as Microsoft Forms).
2. Use data collection applications that will store the collected data on a server that is physically located on Canadian soil.
3. When using cloud-based applications to collect survey data, be sure to use available features (and be able to describe how you used them) to ensure the integrity, reliability, and validity of the data collected.
4. When using cloud-based applications to collect survey data, anonymize the data stored on the cloud server. Do NOT collect directly identifiable data (names, ID numbers, email addresses, etc.). Use a securely stored identification key to match a unique identification code with a participant (for the purposes of avoiding duplicate data entry).

5. Ensure that data collected through cloud-based applications can only be accessed by approved members of the research team. Do NOT use open link sharing for data files. ONLY share access directly with approved team members.
6. As soon as possible, download data collected through cloud-based applications to a secure, password-protected device. Once data integrity has been verified for the downloaded file, delete the source file from the cloud storage space.
7. When using Internet-based applications to conduct data collection (i.e., interviews, etc.), be sure to use a secure meeting space that can only be accessed by approved participant(s) and members of the research team.

Location of Data Servers

- Nova Scotia public bodies are bound by the Personal Information International Disclosure Protection Act (PIIDPA). This legislation provides additional protection to personal privacy and applies to CBU as a public body. PIDPA requires that personal information to be housed on Canadian servers.
- If data will be housed outside of Canada, legislation requires that participants must be informed in the letter of consent that their information will be stored in another country where it is under the auspices of that country's legislation and access.
- The REB may deem the use of internationally stored data inappropriate for sensitive research topics.
- CBU One Drive is located on Canadian servers. Data stored here (using Office 365 such as Forms) will be saved on Canadian servers.
- Data stored on Microsoft Teams (such as recordings from Teams that are uploaded on Stream) are housed on US servers.

Please review the sample language provided below, quoted from the UBC REB and shared by MSVU's REB. You may model and/or adapt this language to use in your consent form when data will be stored internationally:

Sample One

This online survey company is hosted by a web survey company located in the USA and as such is subject to U.S. laws, in particular, the US Patriot Act which allows authorities access to the records of internet service providers. If you choose to participate in the survey, you understand that your responses to the survey questions will be stored and accessed in the USA. The security and privacy policy for the web survey company can be found at the following link: _____.

Sample Two

Data collected using the conferencing platform [insert] can be stored in Canada or the United States of America (USA) . Data stored in the USA is subject to American laws, including the Patriot Act, which allows US authorities to access the records of internet service providers. If you choose to participate in this study, you understand that the information you provide may be stored and accessed in the USA. The security and privacy policy for Zoom can be found at the following link: _____