Research Ethics Matter. Big Time.

Got REB?

breb.ok.ubc.ca

UBC Okanagan

Behavioural Research Ethics Board

UBC Okanagan BREB

Research Data Storage and Security

Research data storage and security is a key part of any research project. It is crucial to ensure the safety of your data. Replacing it could be time-consuming, costly, or even impossible. Planning ahead to back up your files will make the process simple and can ensure you don't experience an avoidable disaster! It will also ensure that your data can be used by other researchers in the future. Three copies of your data are recommended: the original, a copy kept on a local external device, and a copy kept on a remote external device. Planning the security of your data prevents unwanted damage or modification, theft, breaches of confidentiality or privacy, releasing your data before it is ready. In addition, Protecting your valuable research data from physical damage is just as important as garnering against possible tampering, loss, or theft. The four links to the right provide information regarding data storage/ security and other related items. If you aren't familiar with them—take a look!

Security is necessary, but not necessarily easy. However, it is easier to protect than to explain a breach or loss of data

Tips for data Privacy and Security

**taken from the Research Checklist: Data Privacy; access the link from the right for the complete list of tips*

- **Encrypt all devices** used to store, access, disclose or transfer personal information including backups, working copies and any transmissions. You may wish to use UBC's Encryption Services.
- Limit the amount of data you collect -- don't collect data you don't need "just in case".
- Say no to the Cloud! Be aware of the restrictions on storing personal information outside Canada. Do not use tools such as Dropbox, Gmail, Fluid Surveys, Survey Monkey or Google Docs without appropriate consents in place.
- Store data on a secure, centralized system (such as the University's central servers, or the Workspace service) .
- De-identify data immediately. Segregate personal information from the other data collected. Encrypt your electronic file that correlates study ID to personal information.
- Try not to use USBs, even if encrypted, especially if this is the only copy of the information as they are not that reliable for long term storage of data.
- Take proactive measures to prevent theft or loss of mobile devices containing project data. Comply with UBC's Mobile Access standard. Never leave any mobile devices (laptop, phone, USB drive etc.) that may contain data unattended.

Data Storage and Security : Section 8 of the BREB Application

All electronic files and devices containing personal information about an identifiable individual collected for research purposes must be encrypted. Please confirm in the application that this will be done. For further information around UBC's encryption requirements and for resources on how to do this, see the **UBC Security Standards** link at the right.

All hard copies of your research materials, including audio/video tapes, should be kept in a locked cabinet in an secure room. To safeguard confidential information, electronic data should be stored on an encrypted, password protected computer or storage device, which are also kept in a secure location. Please clarify how your research data will be protected.

Websites to Add to your Favorites:

Research Data Management

http://researchdata.library.ubc.ca/

Privacy Impact Assessments

http://universitycounsel.ubc.ca/access-and-privacy/pia/

UBC Security Standards

http://cio.ubc.ca/security-standards-home/information-security-policy-standards-and-resources

Checklist : Data Privacy—*Check it out!!*

http://universitycounsel.ubc.ca/files/2014/01/Checklist-for-Privacy-in-Research-2014.pdf

UBC O BREB Contacts:

Co-Chairs:

Carolyn Szostak
Carolyn.Szostak@ubc.ca

Wendy Klassen
Wendy.Klassen@ubc.ca

Associate Manager, BREB
Lisa Shearer
250.807.8289
Lisa.Shearer@ubc.ca

IT Contact
Wade Klaver
Wade.Klaver@ubc.ca