UBC

populationdata BC

A PLATFORM SUPPORTING RESEARCH ON
HUMAN HEALTH, WELL-BEING AND DEVELOPMENT.

Data Privacy and Information Security:

Researcher Checklist

Planning and Grant Writing Phase

□ 1. Allocate money and time in your project budget to ensure a team member is charged with responsibility for privacy and information security.

□ 2. Understand UBC's Access and Privacy Requirements and Information Security Policies, as well as the policies of any other institutions you are affiliated with.

□ 3. In addition to the Freedom of Information and Protection of Privacy Act, understand any other legislative requirements relevant to your research. These may include the Personal Information Protection Act (for physicians working in the private sector) and the E-Health Act (if you are accessing a Health Information Bank).

□ 4. Require all project team members to complete the Tri-Council Policy Statement Two Course on Research Ethics. See the Online Tutorial.

□ 5. Schedule regular project team meetings to conduct data privacy and information security training and require all members to sign a confidentiality pledge. Consider using Population Data BC's Confidentiality Pledge as a template.

□ 6. Understand UBC's procedures for Reporting Information Security Incidents and Handling Privacy Breaches, as well as the related procedures of any other affiliated institutions.

□ 7. Ensure all research involving human participants that is conducted under the auspices of your institution is approved by and overseen by a sanctioned Research Ethics Board.

Data Collection, Analysis and Storage Phase

□ 1. Clearly identify all methods of collection, use, storage, linkage and disclosure of personal information for research and evaluation purposes in your consent form. See Population Data BC's Consent Form Sample and Guidelines and the BC Clinical Research Informed Consent Form Guide and Template.

□ 2. Limit the amount of data you collect -- don't collect data you don't need "just in case".

□ 3. Say no to the Cloud! Be aware of the restrictions on storing personal information outside Canada. Do not use tools such as Dropbox, Gmail, Survey Monkey or Google Docs without appropriate consents in place.

□ 4. Store data on a secure, centralized system (such as the University's central servers, or the Workspace service) or consider Population Data BC's Secure Research Environment.

□ 5. De-identify data immediately. Segregate personal information from the other data collected. Encrypt your electronic file that correlates study ID to personal information.

□	6. Implement requirements for physical and information security controls of your office and/or datacentre including encryption controls, appropriate firewalls, update to software and patch management. The UBC Information Security Office can provide assistance.
□	7. Provide data access to project team members on a "need to know" basis.
□	8. Restrict user accounts and folder permissions and enable logging functions to audit access to data files.
□	9. 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.
□	10. Take proactive measures to prevent left or loss of mobile devices containing project data. Comply with UBC's Working Remotely standard. Never leave any mobile devices (laptop, phone, USB drive etc.) that may contain data unattended.

Data Retention and Destruction Phase

□	1. Monitor timelines for data retention and closure outlined in ethics approval, consent form and funding application. Complete REB project closure. Make appropriate plans for archiving your project data to meet UBC policy requirements for study data to be retained for at least 5 years within a UBC facility.
□	2. Ensure plans for final data destruction comply with the minimum standards set out in Clearing and Declassifying Electronic Data Storage Devices (ITSG-06).
□	3. Track and log disposal of all University-owned devices and electronic information.
□	4. Be prepared to provide a data destruction certificate upon request to a data steward.

This checklist is a simplified summary of complex privacy and security requirements; it will evolve over time as more standards are created. This checklist was prepared by Kaitlyn Gutteridge, Lead, Privacy and Governance, for Population Data BC, in consultation with Paul Hancock, Legal Counsel, Information and Privacy, Office of the University Counsel. They would be pleased to answer your questions.
An electronic version of the checklist can be found here: http://universitycounsel.ubc.ca/data-privacy-day/