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

Top Ten Tips for Privacy in Research

1. **Plan for privacy in advance**

Just as you spend a lot of time before a project working out the protocol, grant opportunities and data available, you should spend time to consider privacy in advance as well. Privacy controls work best when they are preventative rather than when used as a remedy for a weakness you've discovered. Make sure you will have the funds and resources to adequately protect the data you will be using. Hire a project team member with privacy experience. Put money aside in your grant proposals to resource privacy controls and scans, such as a Privacy Impact Assessment. Don't wait until it's too late to think about privacy – when you do it almost always means you've experienced a data privacy or security incident.

2. **Encrypt everything**

Privacy Commissioners and experts are increasingly recommending that encryption be mandatory for any devices storing, accessing, using, disclosing or transferring personal information. There is no excuse for not encrypting data at every point of its use. That includes back ups, working copies and during transfer. If there is a hole in any other part of your system make sure that the data is useless if accessed inappropriately.

3. **Limit the amount of data you collect**

This is one of the most important principles of privacy. Don't collect data you don't need "just in case". Only request the data that is necessary to answer your research questions. Use data that has been de-identified wherever possible to make the data less sensitive. The more you limit how much information you have the less data may be compromised in the case of an incident. It will also ensure that you aren't using the data for purposes other than that for which you collected it.

4. **Limit the amount of people accessing the data**

Only give data access to project team members who will be analyzing it. Don't give access to data just because it's in the same folder as outputs or papers. Keep the data segregated and provide access based on peoples' roles. The fewer people have access the fewer opportunities there are for error.

5. Don't proliferate the data, keep it central

The more copies that exist of the data, the higher the likelihood that it will be inadvertently disclosed or accessed, whether through loss or theft. It's also harder to track access and usage to ensure that all the project team members are using the data for the original purpose of the collection. The best case scenario for data storage is a central server with remote VPN access for authorized users. An examples of such a system can be found at Population Data BC, which offers Secure Research Environment rental opportunities even if you haven't coordinated your project through their Researcher Liaison Unit. Guidelines, instructions and suggestions for creating your own secure central server can also be found online.

6. Know the rules, read the agreements

Ignorance is not bliss! Look at the legislation governing the use of your data. If you are working with a public body look at the Freedom of Information and Protection of Privacy Act of BC. Doctors or others working in the private sector must be compliant the Personal Information Protection Act of BC. If you're accessing a Health Information Bank you need to ensure you are compliant with the E-health Act as well. Legislation is only one piece of the puzzle though. Make sure that you have read and understood your research agreement, confidentiality pledge and other services agreements, terms of use or other documents you've been asked to sign. Know what you are responsible for, and if you have questions ask them early on.

7. Train your team, pass on the knowledge

Quite often a Principal Investigator (PI) will sign an agreement that no one else on the team will see. This agreement may have requirements for everyone. Make sure these obligations are communicated, and make sure that all the members of the team who are accessing data learn about privacy and the rules surrounding their access to the data. It is the PI's responsibility to train their project team members.

8. Build on existing privacy resources

The Office of the Information and Privacy Commissioner (OIPC) and Office of the Chief Information Officer (OCIO) are resources for those interested in privacy - ask their offices for templates, guidelines and other documents that will help you develop a privacy program for your project. Talk to other researchers about what tools they used and if they can share them. Perhaps you can pool resources as well! Contact your privacy officer, or the University's Access and Privacy Manager if you have questions. Or, if you don't have the resources to manage your own security and privacy use PopData's Secure Research Environment. If you're using secondary, administrative data they can also manage your data access request with you.

9. Don't cut corners, invest in privacy

It's more expensive to clean up after a privacy incident than it is to invest in privacy at the outset. For example, if you are a research institution you may wish to invest in a privacy officer who can ensure you are compliant with legislation, that you proactively embed privacy in the design of your research projects, and that trains your researchers. You'd be surprised how much of a PI's time can be freed up if they don't need to struggle through a Privacy Impact Assessment on their own.

10. Pay attention to how you transfer data.

NEVER EMAIL DATA. There is no reason to email data given the ease of securely transferring information using SFTP. Make sure that you don't use US companies however, as in BC most personal information cannot be disclosed outside of Canada. Even if you are in Canada, use of a US company constitutes disclosure outside of Canada.