**Research Ethics Data Security Recommendations**

Researchers and research staff who are responsible for safeguarding personal information (PI) and personal health information (PHI) must ensure that all reasonable steps are taken to protect this information from unauthorized access throughout the full life cycle: collection, use, dissemination, retention, and/or disposal. For additional information regarding Privacy and Confidentiality, refer to [Chapter 5](http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter5-chapitre5/#toc05-1) of the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2 2014).

For Queen’s University policies regarding data security, refer to:

1. [Electronic Information Security Policy Framework](http://www.queensu.ca/secretariat/policies/senate/electronic-information-security-policy-framework)
2. [Data Security and Encryption: Handling Confidential & Personal Information](https://qshare.queensu.ca/Groups/USEC/Legal/WebDocs/Published/Fact%20Sheet%20-%20Data%20Security%20and%20Encryption.pdf)
3. [Best Practices in Security and Safe Computing](http://www.queensu.ca/its/security/best-practices/)
4. [Mobile Device Security](http://www.queensu.ca/its/security/best-practices/mobile-device-security)
5. [Encryption Service](http://www.queensu.ca/its/security/encryption-service)
6. [Research Data Manag ement at Queen’s University](http://guides.library.queensu.ca/rdm)