SAINT MARY'S UNIVERSITY SINCE 1802

One University. One World. Yours.

Name:	**Research Ethics Board – Data Storage Guidelines**
Policy Number:	9-1002
Origin:	Research Ethics Board
Approved:	November 23, 2007
Issuing Authority:	Research Ethics Board
Responsibility:	Research Ethics Board
Revision Date(s):	n/a
Effective Date:	November 23, 2007

Guiding Principles

Issues around data retention are addressed in an interpretive guide published by the Tri-Council and available at http://pre.ethics.gc.ca/english/pdf/interpretations/Retention_of_Research_Data_April_2005.pdf. The interpretation states in part "

> *Under the TCPS, REBs typically apply guiding principles and/or address issues relevant to data retention, such as respect for free and informed consent (Section 2); respect for privacy and confidentiality, and principles for the secondary use of data (Section 3); and respect for applicable laws and regulations. The "legal context for research involving human subjects is constantly evolving, and varies from jurisdiction to jurisdiction." (TCPS, i.8).*
>
> *The TCPS underscores the importance of considering data retention by research ethics boards (REBs) in their reviews of studies that collect identifiable personal information about research participants: "Researchers shall secure REB approval for obtaining identifiable personal information about subjects. Approval for such research shall include such considerations as… (c) Limits on the use, disclosure and retention of the data…" (TCPS article 3.2 [c]). This is to ensure that the appropriate safeguards for security and confidentiality of the collected information are in place.*
>
> *The TCPS does not specify a required length of time for retention of research data. Data retention periods tend to vary depending on the research discipline, research purpose and kind of data involved.*
>
> *Under the TCPS, REBs typically apply guiding principles and/or address issues relevant to data retention, such as respect for free and informed consent (Section 2); respect for privacy and confidentiality, and principles for the secondary use of data (Section 3); and respect for applicable laws and regulations. The "legal context for research involving human subjects is constantly evolving, and varies from jurisdiction to jurisdiction." (TCPS, i.8).*

Guidelines

Two pragmatic issues regarding data storage and retention are paramount – [a] where the data are to be stored during and after the study and [b] how long the data are to be retained after the conclusion of the study. Although it is not possible to provide definitive standards in these areas, it is possible to articulate several guiding principles.

a) Researchers should be cognizant of the fact that any guarantees made to research participants during the consent process (e.g., limited access to the data, anonymity, confidentiality etc.) remain in force after the study concludes and throughout the data storage process. It is the researcher's responsibility to ensure secure storage of the data that maintains these guarantees and to demonstrate to the satisfaction of the REB that these guarantees are being met throughout the conduct of the study and the data storage period.

   As a guideline, the REB prefers that data are stored

   - on campus in a secure location (i.e., in a locked cabinet, in the University archives or on university computers/electronic media that have limited access)

   Researchers have a special obligation for maintaining secure storage of sensitive data, data containing identifiers[i] or data that may be linked to individuals. In these cases the REB recommends that data be stored:

   - on campus in a locked cabinet in a locked room. Data should be "de-identified" and, identifiers should be stored in a separate location. If stored electronically, data should be stored on a password protected hard drive.
   - off campus, electronic data should be stored on a password protected and encrypted device. Hard copies of the data should be stored in a locked location, under the personal control and supervision of the researcher or to which only the researcher has access.

b) Data Retention after the conclusion of the study should be for a specified period of time, after which the data should be destroyed. Data (either hard copy or electronic) should not be maintained in perpetuity. The sensitivity of the data and the reasons for maintaining the data should be the primary factors determining the length of retention. Recognizing that there are also disciplinary differences, and barring other concerns, the REB recommends a storage/retention period of five years after the completion of the project. Researchers may choose to implement an alternate policy with regard to their data but should justify this choice on application for review.

---

[i] In this context the identifiers include

1. Names
2. Postal address information, other than town or city, province, and postal code
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social insurance numbers.
7. Medical record numbers.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.

11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints and voiceprints.
16. Full-face, oblique or full-profile photographic images and any comparable images.
17. Any other unique identifying number, characteristic, or code.
18. University ID numbers or login.

The following can be identifiers in certain situations:

1. Date of Birth
2. Occupation
3. Ethnicity
4. Gender
5. First three digits of the postal code.

The determination of when and if data are sufficiently de-identified must be decided on a case-by-case basis, since the decision is so context dependent.
http://www.uoguelph.ca/research/humanParticipants/PDF/policies/4%20-%20Administrative/4-G-016.pdf