Data Security Standards for Personally Identifiable and Other Confidential Data in Research

Confidential information in research should be protected from loss, destruction or unauthorized access. Confidentiality arises from law, policy or practice, and covers personal or third party data, or information which is provided in confidence, for example by government.

The following principles, which are consistent with TAHSN policy principles for personal health information security in research, should be followed by all individuals in University research together with applicable requirements of all involved institutions, conditions in research agreements and other legal, policy and practice requirements:

1. Work with de-identified data at all times unless this is not possible for your work and you have explicit REB or other official University approval to work with identifiable data. Code data as early as possible and keep the key separate (in a physically separate space or in a separate electronic file) from the data.

If you work with identifiable or other confidential data:

2. Avoid using hard copy media for storing identifiable or confidential data if possible.

3. If you must use hard copy media for identifiable or confidential data, keep them in a secure institutional environment with restricted access and lockup capability.

4. Only take hard copy media with identifiable or confidential data offsite if absolutely necessary and permitted by REB approvals and research agreements.

5. If you must take hard copy media outside a secure institutional environment, take all reasonable security precautions consistent with protection of a high-value asset.

6. If collecting identifiable data in the field, maintain the minimum amount possible securely on your person until you return to a secure location. De-identify the data as soon as possible. As consent forms include personal information, verbal consent in some research situations may be preferable to protect research subjects. Please consult your REB.

For electronic data:

7. Keep data in a secure server environment. Only access it securely (virtual private network or encrypted remote desktop). Ensure that data are not cached or otherwise stored outside a secure server environment, for example on a desktop or laptop computer.

8. Keep any identifiable data which are outside a secure server environment encrypted at all times except to the extent that you need to decrypt them during use.

General requirements:

9. Do not store or disclose personally identifiable or confidential data other than as necessary for your research and consistent with explicit REB or other official University approval.

10. Keep an accurate and up-to-date log detailing your use of personally identifiable and/or confidential data and specific security and privacy protection measures that you apply.

11. Immediately report privacy concerns (like possible data loss) to the University FIPP Office.

12. Ensure that records are retained only as long as is required to accomplish research purposes and satisfy legal and policy retention requirements.

13. Ensure the secure destruction of all personally identifiable or confidential information at the end of applicable retention periods.

For details about security principles, see App.1; TAHSN "Principles for Development of Policy and Guidelines on Security of Personal Health Information Used for Research Purposes" (TAHSN Principles) and the University's General and Administrative Access and Privacy Practices. Certain specific details of the TAHSN Principles address *Personal Health Information Protection Act* and may not apply to all confidential data. The Information and Privacy Commissioner/Ontario (IPC) www.ipc.on.ca produces detailed materials on personal health information, security and privacy, including; "Safeguarding Personal Health Information" and "Encrypting Personal Health Information on Mobile Devices"