Research Involving Human Participants: Data Security Guideline

YU HUMAN PARTICIPANTS REVIEW COMMITTEE (HPRC) GUIDELINES

The privacy and confidentiality of data supplied by human research participants as a consequence of their participation in research projects is of paramount concern to both institutions and researchers alike. Under the Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans, researchers have an obligation to protect information from “unauthorized access, use, disclosure, modification, loss or theft.”[1] As a consequence, safeguards must be in place to protect the security of research-related data, in particular that data which contains personal identifiers. It is the responsibility of both researchers and institutions, therefore, to have the necessary physical, administrative and/or technical security measures in place to provide the protection that this data requires.

This guideline provides a framework of data security principles which researchers should address when conducting their research, and the context within which research ethics boards (REBs) should consider research ethics protocols.

Researcher Responsibilities

1. **Researchers shall develop and provide details to the REB regarding a data security and management plan.**

Researchers shall assess privacy risks and threats to the security of information for all stages of the research life cycle, and implement appropriate measures to protect information.[2]

Researchers shall provide full details to the REB regarding their proposed measures for safeguarding information, for the full life cycle of information: its collection, use, dissemination, retention and/or disposal.[3]

A researcher’s obligations for data security requirements are not limited to those of the TCPS. Discipline-specific measures as well as formal privacy impact assessments may also be required depending on the context. Researchers are required to adhere to all additional data privacy and protection standards.

2. **Researchers shall consider the full implications of the data collection, use, retention and destruction/archiving when developing data security and management plans.**

Data security measures should, at a minimum, take into account:

- The nature, type and state of data;
- The data's form (e.g., paper or electronic records);
- Content (e.g., presence of direct or indirect identifiers);
- Mobility (e.g., kept in one location or subject to physical or electronic transport);
- Vulnerability to unauthorized access (e.g., use of encryption or password protection).[4]

3. **Researchers shall ensure that the protection of the privacy of research participants is paramount.**

The privacy risks for research participants vary greatly in relation to the type of data collected, its use and its disclosure. Researchers are required to take considerable care in the methods used to collect, store, analyze, disseminate, archive and/or destroy data. Of particular concern is data which contains personally identifiable information. Ethical concerns regarding privacy decrease as it becomes more difficult to associate information with a particular individual.[5] Therefore, when collecting data, researchers shall assess the extent to which the data can be used to identify the participant(s):

- Anonymous information – data collected is anonymous; little or no risk of identification
- Anonymized information – data permanently stripped of all identifying information (no code; no potential for re-linkage); little or no risk of identification
- Coded information – data is stripped of identifying information and replaced with a code; risk of identification is low to moderate as there is a potential for researchers to re-identify participants
- Indirectly identifying information – information could reasonably identify an individual through a combination of indirect identifiers (demographic information; personal characteristics)
- Directly identifying information – personal identity directly revealed (name, health numbers, etc.)

Data Security Practices for Personally Identifiable Information in Research

Personally identifiable information in research should be protected from loss, destruction, or unauthorized access in compliance with legislation, university policy, and funding agency requirements. The following standards as they pertain to data security and privacy should be followed as appropriate throughout the research cycle:

Collection

1. Limit the collection of personally identifiable information wherever possible, and only as permitted by an approved research protocol.
2. De-identify personally identifiable information as soon as possible.

Use

3. If using coded information, keep the key separate from the data.
4. For field work, minimize the use of personal identifiers in field notes and maintain identifiable data in a secure fashion at all times in the field.
5. Only take personally identifiable hardcopy data offsite if absolutely necessary and only if permitted by HPRC approvals and research agreements. Take all necessary precautions to ensure hardcopy data taken offsite is secure (e.g., transported in a locked briefcase).
6. For personally identifiable electronic information, encrypt data when transporting on USB keys, laptops and other portable electronic data devices.
7. Encrypt personally identifiable electronic information which is used outside a secure server environment.
8. Send personally identifiable research data via University email (not via third-party email services such as hotmail, gmail, yahoo, etc.). Avoid Internet Cafés or kiosks when sending personally identifiable data via email.
9. When accessing personally identifiable information remotely, use VPN (virtual private network) or an encrypted remote desktop.

Disclosure / Dissemination

10. Do not disclose or disseminate personally identifiable information unless explicit approvals have been obtained from either the HPRC or the relevant institutional office, or required by law.

Storage and Retention

11. Store personally identifiable hardcopy information in a secure institutional setting with restricted access (e.g., locked filing cabinets in locked offices).
12. Store all personally identifiable electronic information on a secure server. Ensure that data is not cached or otherwise stored outside a secure server environment, such as on a desktop or laptop.
13. Where personally identifiable information must be stored on a non-secure server or on a personal computer or laptop, ensure the data is encrypted at all times.
14. Ensure all personally identifiable information is retained as long as required in accordance with University and funding agency policy.

Disposal

15. Where required, ensure personally identifiable data is destroyed in a secure and confidential manner (see Tip Sheet on Secure Destruction of Records Tip Sheet on Secure Destruction of Records).
16. Ensure all personally identifiable information is removed or deleted from decommissioned computers. Consult IT services to ensure all data has been wiped from memory.

General

17. If using cloud computing tools for any part of the research (e.g., data collection, processing, storage), ensure that a risk assessment has been conducted in accordance with University policies and guidelines.
18. Report any privacy breach or data loss immediately to the Information and Privacy Office (privacy@yorku.ca) and the Office of Research Ethics (acollins@yorku.ca).

[1] Introduction and Chapter 5, Tri-Council Policy Statement, *Ethical Conduct for Research Involving Humans*, 2nd Edition (2010) [hereafter TCPS2].

[2] Article 5.3 Application, TCPS2.

[3] Article 5.3, TCPS2.

[4] Ibid.

[5] Key Concepts, Chapter 5, TCPS2.