

Procedures for Stewardship of Research Records at the University of Saskatchewan

Members of the University [defined below] involved in research at the University of Saskatchewan must create and retain records in accordance with these procedures. The purpose of these procedures is to ensure that the authenticity of all data and other factual information generated in research can be verified and to ensure that any research records containing personal and personal health information about identifiable individuals are stored in a manner which protects the privacy of such personal and personal health information in accordance with the University's Freedom of Information and Protection of Privacy Policy¹ and the appropriate freedom of information and protection of privacy acts.

Research records must be recorded appropriately, archived for defined time periods or for reasonable longer periods [described below], and made available for review if required in the following situations:

- to ensure the appropriate use of human and animal participants in research and compliance with biosafety, radiation safety, environmental and other regulations or requirements;
- to ascertain compliance with research sponsorship terms;
- to protect the rights of students (undergraduate and graduate), postdoctoral fellows, staff, and other research team members, including rights to access records from research in which they participated as a researcher;
- to assist in proving and/or securing intellectual property rights;
- to enable investigations of allegations of academic misconduct or conflict of interest; and,
- to assist and enable other administrative or legal proceedings involving the University and/or researchers, or its/their interests, related to their research.

1.0 Application

These procedures apply to all members of the University involved in research, in any capacity whatsoever. Members of the University of Saskatchewan, include but are not limited to, faculty, professors emeriti, sessional lecturers, staff, trainees, clinical faculty, graduate and undergraduate students, adjunct professors, visiting professors, visiting scholars, professional affiliates, associate members, residents, and postdoctoral fellows (PDFs) at the University of Saskatchewan. Nothing in these procedures will limit or amend the provisions of any existing collective agreement at the University of Saskatchewan.

Research records are those documents and other records and materials recorded by or for a researcher that are necessary to document, reconstruct, evaluate, and validate research results and the events and processes leading to the acquisition of those results. Research records may be in many forms including but not limited to laboratory notebooks, survey documents, questionnaires, interview notes, transcripts, machine-generated data or performance outputs, recruitment materials, consent forms, correspondence, other documents, computer files, audio or video recordings, photographs including negatives, slides, x-ray films, samples of compounds, organisms (including cell lines, microorganisms, viruses, plants, animals) and components of organisms.

¹ http://www.usask.ca/university_secretary/policies/operations/Freedom-of-Information.php

2.0 Collection and Retention

The Principle Investigator² (PI) is responsible for the collection, maintenance, privacy, and secure³ retention of research records in accord with these procedures and applicable privacy legislation. The PI should also ensure that all personnel involved with the research understand and adhere to established practices that are consistent with these procedures.

Research records must be recorded or preserved in accordance with the highest standard of scientific and academic practice and procedures. Research records must be retained in sufficient detail to enable the University and the involved researchers to respond to questions about research accuracy, authenticity, compliance with pertinent contractual obligations, and University of Saskatchewan and externally imposed requirements and regulations governing the conduct of the research.

Human research ethics applications require a statement outlining the procedures researchers will use to securely store research records including the length of time the research records will be stored, the location of storage, the identity of the person responsible for storage of research records, and the procedures that will ensure secure storage. Research participants must be informed of the purpose, use and retention of the records as part of the information provided to them to make an informed decision about whether to consent to participate in the study. Research participants must also be informed about any potential for secondary use of research records.

Research record retention periods will vary depending on the research discipline, research purpose and type of records involved.

Research records must be retained for not less than:

- five (5) years after the end of a research project's records collection and recording period;
- five (5) years from the submission of a final project report;
- five (5) years from the date of publication of a report of the project research; or,
- five (5) years from the date a degree related to a particular research project is awarded to a student.

whichever occurs last.

Research records must be retained for longer periods:

- if required to protect intellectual property rights;
- if such research records are subject to specific federal or provincial regulations⁴ requiring longer retention periods;
- if required by the terms of a research sponsorship agreement; or,
- if any allegations regarding the conduct of the research arise, such as allegations of academic misconduct or conflict of interest.

² A Principal Investigator (PI) is a person responsible for performing, directing, or supervising research, or who signs a research sponsorship agreement in acknowledgement of the obligations of himself, herself, or the University.

³ Research records must be stored securely and protected with all the precautions appropriate to its sensitivity and privacy. Highly sensitive records may need to be held on computers not connected to networks and located in secured areas with restricted access. Secure storage may mean encryption of research records sent over the internet or kept on a computer connected to the internet; adherence to guidelines on data storage on mobile drives, digital recording devices or laptop computers; the use of computer passwords, firewalls, back-ups, and anti-virus software; off-site backup of electronic and hard-copy records; and other measures that protect research records from unauthorized access, loss or modification.

⁴ For example: Canada's *Food and Drug Regulations* require certain clinical trial records to be stored for twenty-five (25) years and research conducted in provincial hospitals may be subject to *The Hospital Standards Regulations, 1980* (Saskatchewan).

Research records may be retained for longer periods if retention is required for the continuity of scientific research or if the research records are potentially useful for future research by the PI or other researchers⁵.

The Tri-Councils place the following responsibilities on grant holders:

- The Social Sciences and Humanities Research Council (SSHRC) Policy on Data Sharing states that all research data collected with the use of SSHRC funds must be preserved and made available for use by others within a reasonable period of time⁶.
- Canadian Institutes of Health Research (CIHR) grantees must deposit bioinformatics, atomic and molecular coordinate data into the appropriate public database immediately upon publication of research results⁷.
- CIHR grantees must retain original data sets arising from CIHR-funded research for a minimum of five years after the end of the grant. This applies to all data, whether published or not⁸.
- Collections of animal, culture, plant or geological specimens, or archaeological artifacts (“collections”) collected by a grantee with Tri-Council grant funds are the property of the University⁹.

3.0 Destruction of Research Records and Materials

Destruction of research records must be carried out so that personal information cannot practicably be read or reconstructed¹⁰. In some cases it may be advisable to document the manner and time of destruction.

4.0 Leaving the University

When a researcher (including a student) involved in a research project leaves the University, she or he may take a copy of the research records related to her or his research.

If a PI leaves the University of Saskatchewan or a project is to be moved to another institution, the University must be notified of the location of the original research records. In some instances (e.g., where University of Saskatchewan intellectual property or other interests are involved), such transfer may not be permitted, and any such agreement may require diligent retention by the recipient and continued access by the University of Saskatchewan.

The obligations of researchers set out in these procedures continue to apply if an individual takes copies of research material to his/her new institution.

⁵ Future use of research records may be subject to the provisions of applicable privacy legislation and/or the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS) <http://pre.ethics.gc.ca/eng/policy-politique/tcps-epc/readtcps-lireeptc>

⁶ http://www.sshrc.ca/site/apply-demande/policies-politiques/edata-donnees_electroniques-eng.aspx

⁷ <http://www.cihr-irsc.gc.ca/e/34846.html#8>

⁸ http://www.nserc-crsng.gc.ca/Professors-Professeurs/FinancialAdminGuide-GuideAdminFinancier/Responsibilities-Responsabilites_eng.asp

⁹ http://www.nserc-crsng.gc.ca/Professors-Professeurs/FinancialAdminGuide-GuideAdminFinancier/Responsibilities-Responsabilites_eng.asp

¹⁰ Paper documents containing personal information should be burned, pulverized or shredded into very small shreds. Erasing electronic files from a computer will not remove the information in that file from the computer. Applications are available that provide for secure erasure and will remove the records. When a computer is decommissioned, the disks must be erased using a secure disk erasure application or physically destroyed.