



Procedure Title:

Privacy Procedures

University Classification & Procedure Number:

TBD

Approval Body:

University Administration

Responsible Designate:

Vice-President, Finance and Administration

Established:

2016

Revised:

2023

Editorial Revisions:

Not applicable

Scheduled Review:

2028

1.0 Procedure Purpose

To implement the Privacy Policy at The University of Winnipeg, the Procedures outlined in this document shall be followed.

2.0 Definitions

The following definitions apply to terms as they are employed in this Procedure document:

2.01 Commercial Activity: any particular transaction, act, or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering, or leasing of donor, membership, or other fundraising lists.

2.02 Demographic or Eligibility Information: the following Personal Health Information about an identifiable individual as defined in *The Personal Health Information Act* (PHIA):

- name,
- signature,
- address,
- email,
- phone number,
- sex,
- date of birth,
- date of death,
- family associations,
- eligibility for Health Care coverage,
- jurisdiction of residence,
- Manitoba Health family registration number,
- Personal Health Identification Number (PHIN),
- a unique identifier equivalent to the PHIN assigned by another jurisdiction that pays for Health Care,

- a unique identifier – not including a social insurance number or, except as provided above, any other pre-existing identifier – assigned to an individual by a Trustee for its own purposes, when accessed by any Trustee, and
- a non-Canadian unique health identification number.

2.03 Department: a University faculty, department, office, centre, or other unit.

2.04 Electronic Health Information System: a computer system or systems delegated to host PHI.

2.05 Information Manager: an individual, corporate organization, business, or association that processes, stores, or destroys PI or PHI, or provides information management or information technology services to or on behalf of the University.

2.06 Integrity: the preservation of the content of PI or PHI throughout its storage, Use, transfer, and retrieval so that there is confidence that the information has not been tampered with or modified other than as authorized.

2.07 PIPEDA: *The Personal Information Protection and Electronic Documents Act S.C. 2000, c.5* as amended from time to time.

2.08 Privacy Breach: the Collection, Use, Disclosure, or destruction of PI or PHI in contravention of FIPPA, PHIA, or PIPEDA.

2.09 Record of User Activity: a Record about access to PHI maintained on an Electronic Health Information System, which identifies the following:

- individuals whose PHI has been accessed,
- persons who accessed PHI,
- when PHI was accessed,
- the Electronic Health Information System or component of the System in which PHI was accessed, and
- whether PHI that has been accessed is subsequently Disclosed under s.22 of PHIA.

2.10 Responsible Administrator: Department Heads including Vice-Presidents, Associate Vice-Presidents, Deans, Directors, and Managers.

2.11 Trustee: a university, health professional, Health Care facility, public body, or health services agency that Collects or maintains PHI as provided for under PHIA.

Additionally, all Definitions in the Privacy Policy are incorporated into these Procedures and shall apply as fully as if they had been set out verbatim herein.

3.0 Procedure Elements

3.01 Collection of Personal Information and Personal Health Information:

3.01.01 Collection must be authorized by a statute or alternatively where the information Collected relates directly to and is necessary for an existing service, program, or activity of the University.

3.01.02 PI or PHI shall be Collected in a manner and location that ensures the security, accuracy, Integrity, and confidentiality of the information, to the extent that it is reasonable to do so.

3.01.03 Collection shall be limited to only as much PI or PHI as is reasonably necessary to accomplish the purpose for which it is being Collected, and that a reasonable person would consider appropriate in the circumstances.

3.01.04 Whenever possible, PI or PHI shall be Collected directly from the individual to whom the information relates, unless a method of indirect Collection authorized under FIPPA or PHIA is necessary.

3.01.05 If Collecting PI or PHI directly from the individual to whom the information relates, they shall be provided with the purpose and the contact information of a University employee who can answer questions about the Collection, unless the University has recently provided the individual with this information about the Collection of the same or similar PI or PHI for the same or a related purpose.

3.01.06 If Collecting PI directly from the individual to whom the information relates, the individual shall also be provided with the legal authority under which the information is Collected, unless the University has recently provided the individual with this same information about the Collection of the same or similar PI for the same or a related purpose.

3.01.07 If Collecting PI or PHI in the course of Commercial Activity, the consent of the individual to whom the information relates is required, unless:

- a. Collection without consent is permitted under sections 7 to 7.4 of PIPEDA ([Hyperlink](#)),
- b. it is impossible or impractical to seek consent, or
- c. the PI or PHI is not sensitive and the individual to whom the information relates would reasonably expect that consent is implied.

3.02 Access to Personal or Personal Health Information

PI or PHI may only be accessed as required for authorized purposes.

3.03 Use and Disclosure of Personal or Personal Health Information

3.03.01 PI or PHI may only be Used and Disclosed as required for the purpose for which it was Collected or Disclosed unless the individual to whom the information relates has provided consent for other Use or Disclosure, or Use or Disclosure is otherwise authorized under FIPPA or PHIA as cited in Table 1 below:

TABLE 1

FIPPA	PHIA
s.43 or 45 (Hyperlink)	s.21 (Hyperlink)
s.44 (Hyperlink)	s.22 (Hyperlink)
s.47 or 48 (Hyperlink)	s.24 (Hyperlink)
s.44.1 (Hyperlink)	s.25 (Hyperlink)

3.03.02 PI may be Used or Disclosed for a consistent purpose in accordance with s.45 of FIPPA ([Hyperlink](#)).

3.03.03 The Use and Disclosure of PI or PHI shall be in a manner and location that ensures the security, accuracy, Integrity, and confidentiality of the information, to the extent that it is reasonable to do so.

3.03.04 The Use and Disclosure of PI or PHI shall be limited to the minimum amount of information necessary to accomplish the purpose for which the information is Used or Disclosed and that a reasonable person would consider appropriate in the circumstances.

3.03.05 PI or PHI shall not be Disclosed to any person, unless the individual to whom the information relates has provided consent for the Disclosure, or Disclosure is otherwise authorized under FIPPA or PHIA as cited in Table 1 above.

3.03.06 Before Using or Disclosing PI or PHI, UW Community Members shall take reasonable steps to ensure that the information is accurate, up-to-date, complete, and not misleading.

3.03.07 Disclosure to an Information Manager may only be made as permitted under s.44.1 of FIPPA ([Hyperlink](#)) or s.25 of PHIA ([Hyperlink](#)).

3.03.08 Disclosure for research may only be made as permitted under s.47 of FIPPA ([Hyperlink](#)) or s.24 of PHIA ([Hyperlink](#)) and in compliance with any applicable University Human Research Ethics Board-approved Protocol.

3.03.09 If Using or Disclosing PI or PHI in the course of Commercial Activity, the consent of the individual to whom the information relates is required, unless:

- a. Use or Disclosure without consent is permitted under sections 7 to 7.4 of PIPEDA ([Hyperlink](#)),
- b. it is impossible or impractical to seek consent, or
- c. the PI or PHI is not sensitive and the individual to whom the information relates would reasonably expect that consent is implied.

3.04 Consent for Collection, Use, and Disclosure of Personal or Personal Health Information

3.04.01 Where consent is required for the Collection, Use, or Disclosure of PI or PHI, that consent shall:

- a. be in writing or otherwise electronically or manually recorded;
- b. relate to the purpose for which the information is Used or Disclosed;
- c. be knowledgeable, so that it is reasonable to expect that an individual to whom the University's activities are directed would understand the nature, purpose, and consequences of the Collection, Use, or Disclosure of the PI or PHI to which they are consenting, including the implications of withdrawal of consent where applicable;
- d. be voluntary; and
- e. not be obtained through misrepresentation.

3.05 Administrative Safeguards

3.05.01 All PI and PHI shall be protected in accordance with the Information Security Policy and related Procedures.

3.05.02 The University may require employees to complete training focused on privacy and information security.

3.05.03 UW Community Members who regularly Collect, Use, Disclose, store, or destroy PHI shall complete privacy training offered through the University's Information and Privacy Office and sign the PHIA Pledge of Confidentiality (see Appendix "A" attached).

3.06 Privacy Breaches

3.06.01 Any complaint received about a Privacy Breach, or any knowledge of a Privacy Breach or a reasonable suspicion of a Privacy Breach, shall be immediately reported to the University's Senior Information and Privacy Officer and the Responsible Administrator.

3.06.02 The University's Senior Information and Privacy Officer, working with others as needed, shall determine whether the alleged Privacy Breach warrants investigation, taking into consideration factors such as:

- a. the length of time that has elapsed since the alleged Privacy Breach;
- b. whether the alleged Privacy Breach is trivial, or the complaint is not in good faith or frivolous; and
- c. whether the circumstances of the alleged Privacy Breach warrant investigation.

3.06.03 If a Privacy Breach warranting investigation is confirmed as a Privacy Breach under FIPPA, PHIA, or PIPEDA, the University's Senior Information and Privacy Officer shall, working with others as needed, take any steps reasonably necessary to contain the Privacy Breach and explore corrective procedures to address the Privacy Breach and lessen the likelihood of future Privacy Breaches.

3.06.04 The University's Senior Information and Privacy Officer shall generate a Record of the Privacy Breach and the subsequent investigation and shall report the matter to:

- a. the President or the President's delegate under section 81 of FIPPA or section 58 of PHIA, and
- b. the Ombudsman of Manitoba, the Privacy Commissioner of Canada, or law enforcement agencies as may be appropriate, in the case of Privacy Breaches that present a real risk of significant harm to the affected individuals.

3.07 Retention of Personal or Personal Health Information

PI or PHI Used to make a decision that directly affects the individual to whom the information relates shall be retained for a reasonable period of time in accordance with all applicable legislation, regulation, and University policy.

3.08 Requests for Access to Personal Information

Except only where there is an existing procedure for access to PI or where access is provided for under a collective agreement, individuals who wish to examine or receive a copy of their PI must submit a FIPPA request on the prescribed form to the University's Senior Information and Privacy Officer together with any fees that may be required.

3.09 Requests for Access to Personal Health Information

3.09.01 Individuals who wish to examine or receive a copy of their PHI must submit a request to the Department that retains the information or to the University's Senior Information and Privacy Officer.

3.09.02 The Department or the University's Senior Information and Privacy Officer shall make every reasonable effort to assist the individual making a request and to respond openly, accurately, completely, and without delay.

3.09.03 The Department or the University's Senior Information and Privacy Officer shall respond within 3 days of receiving a request for access, if the information refers to an individual who is currently receiving Health Care at the University, or within 30 days in any other case, unless the request is transferred to another Trustee.

3.09.04 If the time limit to respond to a request for access expires on a statutory holiday or a University closure day, the time limit is extended to the next day on which the University is open.

3.09.05 If a Department is unsure about releasing the requested information or anticipates that search and preparation of the requested Records will require more than 2 hours, or if the requested Records exceed 50 pages, the Department shall contact the University's Senior Information and Privacy Officer or direct the requester to make an application through the University's Senior Information and Privacy Officer.

3.09.06 Prior to permitting an individual to examine or receive a copy of their PHI, the Department or the University's Senior Information and Privacy Officer shall confirm the identity of the requester.

3.09.07 On request, the Department or the University's Senior Information and Privacy Officer shall provide the individual with an explanation of any term, code, or abbreviation Used in the PHI.

3.09.08 The Department or the University's Senior Information and Privacy Officer is not required to permit an individual to examine or copy their PHI in accordance with the exceptions outlined in subsection 11(1) of PHIA ([Hyperlink](#)).

3.09.09 A Department or the University's Senior Information and Privacy Officer who refuses to permit an individual to examine or receive a copy of their PHI pursuant to subsection 11(1) of PHIA ([Hyperlink](#)) shall, to the extent possible, sever, redact or otherwise remove the PHI that cannot be released, permit the individual to examine and receive a copy of the remainder of the information, and inform the individual of their right to complain to the Ombudsman of Manitoba about the refusal.

3.10 Requests for Correction of Personal or Personal Health Information

Individuals may submit a request for correction of PI or PHI in writing to the University's Senior Information and Privacy Officer.

3.11 Exercising Rights of Another Person

Any right or power conferred on an individual by this Policy may be exercised by another person pursuant to s.79 of FIPPA ([Hyperlink](#)) or s.60 of PHIA ([Hyperlink](#)).

3.12 Electronic Health Information Systems

3.12.01 Where a Department utilizes an Electronic Health Information System to maintain PHI, the Responsible Administrator shall:

- a. create and maintain, or have created and maintained, a Record of User Activity for at least three years;
- b. ensure that at least one audit of the Record of User Activity is performed to detect Privacy Breaches before the Record is destroyed; and
- c. provide a copy of the completed audit to the University's Senior Information and Privacy Officer.

3.12.02 A Record of User Activity may be generated manually or electronically.

3.12.03 A Record of User Activity is not required:

- a. if the PHI is limited to, or qualifies or further describes, Demographic or Eligibility Information, or
- b. if PHI is accessed or Disclosed while a UW Community Member is generating, distributing, or receiving a statistical report, as long as the Responsible Administrator:
 - i. maintains a Record of the persons authorized to generate, distribute, and receive such reports, and
 - ii. regularly reviews the authorizations.

3.13 Audit of Personal Health Information Security Safeguards

3.13.01 The University shall conduct an audit of administrative, physical, and technical security safeguards employed to protect PHI in the custody or under the control of the University at least every two years.

3.13.02 If an audit identifies deficiencies in the University's security safeguards, the University's Senior Information and Privacy Officer shall make recommendations to the Responsible Administrator to take steps to correct the deficiencies as soon as is practicable to do so.

3.13.03 The University's Senior Information and Privacy Officer shall document the findings of the audit along with any recommendations to monitor and ensure compliance under PHIA.

3.14 Notice of Right to Access Personal Health Information

3.14.01 Departments that regularly retain PHI must display a sign, poster, brochure, or other similar type of notice to inform individuals of their rights to examine and receive a copy of their PHI and to authorize another person to examine and receive a copy of the PHI subject to the right of the University to refuse as set out under PHIA s. 11(1) ([Hyperlink](#)).

3.14.02 The sign, poster, brochure, or similar type of notice must be prominently displayed in as many locations and in such numbers as the Responsible Administrator reasonably considers adequate to ensure that the information is likely to come to the individual's attention.

4.0 Relevant Legislation

- *The Freedom of Information and Protection of Privacy Act (FIPPA)*
- *The Personal Health Information Act (PHIA)*
- *Criminal Code of Canada*

5.0 Related Policies, Procedures and Institutional Documents

- Information Security Policy
- University Records Policy

APPENDIX "A"

PHIA PLEDGE OF CONFIDENTIALITY

I acknowledge that I have completed personal health information (PHI) training offered through The University of Winnipeg ("University"). I have been provided an opportunity to read and understand the Privacy Policy and Procedures governing the collection, use, disclosure, retention, disposition, and security of PHI, which is in accordance with The Personal Health Information Act (PHIA) and Regulation.

I understand that unauthorized use or disclosure of PHI may result in a disciplinary action up to and including termination of employment / contract / association / appointment with the University, the imposition of fines under PHIA, and, where appropriate, a report to my professional regulatory body.

I further understand that my obligations concerning the collection, use, disclosure, retention, disposition, and security of PHI relate to all PHI acquired through my employment / contract / association / appointment with the University.

I hereby agree that I will not, during or after my employment / association / contract / appointment with the University, collect, use, disclose, retain, or dispose of any PHI except as may be required in the course of my duties and responsibilities and in accordance with the University Privacy Policy and Procedures and any applicable legislation and University policies governing the collection, use, disclosure, retention, disposition, and security of PHI.

Name: _____

Signature: _____

Date: _____

Witness: _____