UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
PROCEDURE

Procedure:	**ACCESS AND PRIVACY**
Parent Policy:	Access and Privacy Policy
Effective Date:	June 23, 2015
Revised Date:	
Review Date:	June 23, 2025
Approving Body:	Vice-President (Administration)
Authority:	*The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA)
Responsible Executive Officer:	Vice-President (Administration)
Delegate:	
Contact:	Access and Privacy Officer
Application:	All Employees, All External Parties, Students

Part I
Reason for Procedure

1.1 Establish roles and responsibilities under *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA).

1.2 Establish procedures governing access to information, including general information, Personal Information and Personal Health Information, according to provisions of FIPPA and PHIA.

1.3 Establish procedures for the collection, use, disclosure, storage and disposal of Personal Information and Personal Health Information according to the provisions of FIPPA and PHIA.

1.4 Establish procedures for the reporting, investigation and remediation of Breaches of Privacy under FIPPA and PHIA.

1.5 The Access and Privacy Policy and Procedure are in addition to FIPPA and PHIA, and they do not supersede the Acts or any part of these Acts. If any part or

parts of the Procedures are found to be in conflict with either Act, the Act shall prevail.

Part II
Procedural Content

Roles and Responsibilities

2.1 For the purpose of this Procedure:

(a) **University-President** is the head of the public body under both FIPPA and PHIA.

(b) **Chief Access and Privacy Officer/Access and Privacy Officer** refer to the University of Manitoba employee(s) delegated by the President to act on behalf of the University in matters related to FIPPA and PHIA. The Chief Access and Privacy Officer receives all reports regarding Breaches of Privacy. The University's Vice-President (Administration) is the Chief Access and Privacy Officer. Other individuals may also be delegated specific responsibilities under the Acts.

(c) **Access and Privacy Office** means the University Office under the Office of Fair Practices and Legal Affairs that is tasked with the administration of FIPPA and PHIA at the University.

(d) **Unit Liaison** means a University staff member who has been appointed to represent their office or unit in matters relating to FIPPA, PHIA and Records Management.

2.2 Definitions

(a) **Access to Information** means the viewing or copying of a Record held in the custody or under the control of a public body or trustee.

(b) **Breach of Privacy** occurs when Personal Information, including Personal Health Information, is collected, accessed, used, disclosed, transported, transmitted, transferred or destroyed other than as authorized, or when the accuracy, confidentiality or integrity of the information is compromised.

(c) **Confidential Information** is information that is proprietary of the University and/or to Persons Associated with the University; that has not been authorized for release by the President or the President's duly designated representatives; and that falls into two general categories: University Records, which may include Personal Information; and Personal Information, which includes Personal Health Information.

(d) **Disclosure of Personal Information and Personal Health Information** means making the information known, revealing, exposing, showing, providing, selling or sharing the information with any person or entity outside of the University. FIPPA and PHIA permit disclosures of Personal Information and Personal Health Information for authorized purposes only and within limitations.

(e) **Personal Health Information** is Recorded Information about an identifiable individual that relates to:

(i) the individual's health, or health care history, including genetic information about the individual,

(ii) the provision of health care to the individual, or

(iii) payment for health care provided to the individual, and includes

(iv) the Personal Health Information Number ("PHIN") and any other identifying number, symbol or particular assigned to an individual, and

(v) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care;

(vi) any identifying personal information collected in the course of, and is incidental to the provision of healthcare or payment for health care

(f) **Personal Information** means Recorded Information about an identifiable individual, including:

(i) the individual's name,

(ii) the individual's home address, or home telephone, facsimile or e-mail number,

(iii) information about the individual's age, sex, sexual orientation, marital or family status,

(iv) information about the individual's ancestry, race, colour, nationality, or national or ethnic origin,

(v) information about the individual's religion or creed, or religious belief, association or activity,

(vi) personal health information about the individual,

(vii) the individual's blood type, fingerprints or other hereditary characteristics,

(viii) information about the individual's political belief, association or activity,

(ix) information about the individual's education, employment or occupation, or educational, employment or occupational history,

(x) information about the individual's source of income or financial circumstances, activities or history

(xi) information about the individual's criminal history, including regulatory offences,

(xii) the individual's own personal views or opinions, except if they are about another person,

(xiii) the views or opinions expressed about the individual by another person, and

(xiv) an identifying number, symbol or other particular assigned to the individual.

(g) **Persons Associated with the University** means a staff, faculty, student, researcher or agent who is associated with the University by appointment, employment, contract, or agreement.

(h) **Record or Recorded Information** means a Record of information in any form, including information that is written, photographed, recorded or stored in any manner, on any storage medium, or by any means, including by graphic, electronic or mechanical means, in the custody or under the control of the University of Manitoba.

(i) **Records Authority Schedule (RAS)** refers to a document that identifies a series or group of records, establishes the period for which they must be retained and provides the authority for the final disposition of the records, which will result in either the destruction of the records or their transfer to the appropriate archives. Records Authority Schedules provide a high level inventory of the records held by the University of Manitoba.

(j) **Security** means the consistent application of controls and safeguards to protect the confidentiality and integrity of Personal Information and Personal Health Information at all stages and in all aspects of its collection, access, use, processing, disclosure, transmittal, transport, storage, retention and destruction.

(k) **Third Party**, in relation to a request for access to a Record or for correction of Personal Information, means any person, group of persons or organization other than

(i) the person who made the request, or

(ii) a public body

(l) **Unit Liaison** means a University staff member who has been appointed to represent their office or unit in matters relating to FIPPA, PHIA and Records Management.

(m) **University Health Care Unit** means a unit whose main function is the provision of health care by health professionals and whose function may include the education and training of students in the provision of health care.

(n) **University Office** means a faculty, department, division, unit, centre, program, service or other office of the University unless otherwise specified. University Office includes some offices that collect significant amounts of Personal Health Information.

(o) **Use** of Personal Information and Personal Health Information means accessing, viewing, gaining entry to, hearing, receiving, reproducing, transmitting, employing or otherwise dealing with the information within the University (e.g. between University Offices or employees of the University). Use of Personal Information and Personal Health Information must be for an authorized purpose of the University.

Access

2.3 Access to General Information and Personal Information (Excluding Personal Health Information)

(a) FIPPA allows any individual a right of Access to Information held in the custody or under the control of public bodies, subject to specific exceptions. This includes access to general information held by the University, as well as Personal Information about the individual requesting the Record(s). Requests for general information and access to an individual's own Personal Information may be made either informally to the holding office or formally to the Access and Privacy Office.

(b) A formal Access to Information request is required if the information concerns:

(i) Confidential Information,

(ii) Personal Information concerning an individual who is not named as a requestor,

(iii) the holding office has any doubts about whether that information should be released,

(iv) if the individual requesting the information is not satisfied with the information they receive informally, or

(v) Third Party business information.

(c) A formal Access to Information request must be submitted to the Access and Privacy Office, as described by Sections 8(2) and 8(3) of FIPPA. If the formal request is received by another University Office, it will be immediately forwarded to the Access and Privacy Office. All formal requests will be reviewed by the Chief Access and Privacy Officer or designates.

2.4 Access to Personal Health Information: The University will assist individuals in exercising their rights under Section 5(1) of PHIA to request to examine and receive a copy of his or her Personal Health Information maintained by the University.

(a) At the University, all requests for access to Personal Health Information shall be made first to the office where the individual believes the Records containing the Personal Health Information are held.

(b) No special form is required if the individual is making his or her own request. A written request must contain the name of the individual requesting the Record(s), address, phone number, signature and date of request. The request should be in writing, but verbal requests will be accepted in the event that writing a request causes undue harm or difficulty for the individual and the University Office is satisfied as to the rights of the individual to that information.

(c) (c)Prior to permitting an individual to examine or receive a copy of his or her Personal Health Information, the University Office or University Health Care Unit shall confirm the identity of the requester through photo or other appropriate identification.

(d) (d)Anyone seeking access to the Personal Health Information of another individual must submit a written request to the Access and Privacy Office.

2.5 Responding to Access Requests

(a) When a University Office receives an informal request for Personal Information or Personal Health Information, the University Office shall review the Record(s). If the Record(s) is about the individual making the

request, and if it contains no Third Party Personal Information or Personal Health Information and no otherwise Confidential Information, the office may permit the requester to examine it and provide a copy of the Record to the requester. If the University Office is unsure about releasing the requested information, or is unable to release it, they shall contact the Access and Privacy Office or refer the individual to the Access and Privacy Office. The University Office will keep a Record of having provided access to requested information.

(b) If a University Office anticipates that search and preparation of the requested Records will require more than 2 hours, or if the requested Records exceed 50 pages, the University Office shall contact the Access and Privacy Office or direct the requester to make a formal request through the Access and Privacy Office.

(c) A University Office receiving a formal request via the Access and Privacy Office shall provide the Access and Privacy Office with copies of all the relevant Records to enable the Access and Privacy Office to process the request.

(d) The University will respond to a request as promptly as possible, but no later than the time frames established under FIPPA and PHIA.

(e) Fees may be charged to the applicant and will be assessed by the Chief Access and Privacy Officer, or designates, according to FIPPA or PHIA regulations.

Collection

2.6 Collection of Personal Information and Personal Health Information, may only take place under the authority of an Act, such as *The University of Manitoba Act*, for an authorized purpose and with proper notification.

(a) The University shall collect Personal Information and Personal Health Information about an individual only for a necessary purpose that is connected with an authorized function or activity of the University.

(b) Whenever possible, the University shall collect Personal Information and Personal Health Information directly from the individual that it is about, either verbally or in writing. If the information is collected verbally, it must be recorded by the person who is taking the information.

(c) Personal Information and Personal Health Information shall be collected in a manner and location that ensures the security and confidentiality of such information, to the extent that it is reasonable to do so.

(d) When Personal Information and Personal Health Information is collected directly, the University shall notify the individual of the purpose for collection and with whom the information may be shared.

(e) The University shall collect only as much Personal Information and Personal Health Information as is reasonably necessary to accomplish the purpose for which the information is collected.

Correction of Information

2.7 The University shall ensure the right of individuals to request, and make corrections to, their own Personal Information and Personal Health Information in accordance with FIPPA and PHIA.

(a) All requests for correction must be in writing. The request must include the following information:

(i) name,

(ii) address,

(iii) phone numbers,

(iv) correction requested,

(v) signature, and

(vi) date of signing.

(b) If an individual makes a written request for correction on his or her own behalf and the request is to a University Office, the University Office shall review the Record and if the existing information is inaccurate or incomplete, make the correction. The written request shall be placed in the file and form part of the file. Verbal requests will not be accepted. If the University Office is unsure or unable to make the correction, they shall direct the individual making the request to the Access and Privacy Office for resolution.

(c) Notify, where practicable, any other Public Body or Third Party to whom the Personal Information or Personal Health Information has been disclosed within the past year that the correction was made or the request for correction has been added to the Record.

(d) No fees are charged for the correction of Personal Information or Personal Health Information.

Use and Disclosure

2.8 Use and Disclosure of Personal Information and Personal Health Information by the University:

(a) are limited to the least amount that is necessary to accomplish an authorized purpose.

(b) are limited to the fewest employees possible, that is, to only those who need it to accomplish an authorized purpose.

(c) are only used or disclosed for the purpose for which it was collected, or for a closely related purpose or for certain other purposes allowed under FIPPA and/or PHIA.

(d) shall be only in the discharge of work responsibilities and duties (including reporting duties imposed by legislation) and based on the need to know. This applies to all Persons Associated with the University.

(e) for a different purpose than for which it was collected is only undertaken with consent from the individual the information is about, or from someone who is authorized to act on behalf of the individual.

2.9 Law Enforcement Disclosure: Personal Information and Personal Health Information collected and maintained by the University shall only be disclosed to the Winnipeg Police Service, or other law enforcement agency, in strict accordance with FIPPA and PHIA.

(a) All requests for Personal Information and Personal Health Information relating to a criminal investigation will require a University of Manitoba Law Enforcement Disclosure Form to be completed by the representative of the law enforcement agency making the request. A copy of the completed form is sent to and kept on file in the Access and Privacy Office and a copy is forwarded to the Director, Office of Risk Management.

2.10 All other requests for Access to Information under FIPPA and PHIA related to Law Enforcement or Security Services, including surveillance camera recordings not relating to criminal investigations, are required to be processed as a formal access request, facilitated by the Access and Privacy Office.

Protection of Information

2.11 Protection (Security) of Personal Information and Personal Health Information

(a) Personal Information and Personal Health Information shall be protected by the University during its collection, access, use, disclosure, retention, storage, transportation, transmission, transfer and during its destruction.

(b) All Persons Associated with the University are responsible for protecting Personal Information and Personal Health Information that is collected, heard, handled, viewed or processed in the discharge of their duties and responsibilities with the University.

(c) All Persons Associated with the University who are dealing with Personal Information and Personal Health Information in any manner shall take all reasonable precautions to protect the Personal Information and Personal Health Information from fire, theft, vandalism, deterioration, accidental destruction or loss and any other hazards.

(d) Reasonable administrative, technical and physical safeguards shall be taken by the University to ensure the confidentiality, integrity and security of Personal Information and Personal Health Information, and to prevent the unauthorized collection, access, use, disclosure, transport, transmission, transfer and destruction of Personal Information and Personal Health Information.

(i) Administrative safeguards include, but are not limited to, training, contracts containing appropriate protective clauses, security clearances, designated and restricted access to certain Records, offices or areas and sanctions.

(ii) Electronic safeguards include, but are not limited to, the use of passwords, defined and restricted electronic access, encryption and firewalls.

(iii) Physical security safeguards include, but are not limited to, locked offices, locked filing cabinets, lock-boxes and other barriers separating the Personal Information and Personal Health Information from those who do not need, and should not have, access to the information.

(e) To protect the privacy of Personal Information and Personal Health Information, Persons Associated with the University should not discuss others' Personal Information and Personal Health Information (in their absence) in the presence of those who are not entitled to such information. Personal Information and Personal Health Information should not be discussed in public places such as cafeterias, elevators, lobbies, hallways, classrooms, unsecured or open offices.

(f) Personal Information and Personal Health Information stored in electronic form on a fixed computer server or terminal shall be properly secured from unauthorized access. Personal Information and Personal Health Information stored on electronic media and mobile devices shall be kept in a secured place at all times and shall be used only by authorized personnel having access to a protected system.

(g) Additional safeguards must be taken for the protection of Personal Health Information maintained by electronic information systems, including a Record of User Activity, which documents the following:

(i) individuals whose Personal Health Information has been accessed,

(ii) individuals who accessed Personal Health Information,

(iii) when Personal Health Information was accessed,

(iv) the electronic information system or component of the system in which Personal Health Information was accessed, and

(v) whether Personal Health Information that has been accessed is subsequently disclosed under Section 22 of the Act.

(h) A Record of User Activity should be maintained for 3 years and then destroyed according to these procedures.

(i) The University shall ensure that at least one audit of a Record of User Activity is conducted before the Record is destroyed.

(i) Personal Information and Personal Health Information can only be removed from University premises/systems for an authorized and approved purpose.

(j) If authorized to remove Personal Information and Personal Health Information from University premises, security precautions must be taken, including the following:

(i) all Personal Information and Personal Health Information moved from a secure location shall be recorded in a tracking system,

(ii) only the least possible Personal Information and Personal Health Information necessary to accomplish the task may be removed,

(iii) Personal Information and Personal Health Information should be secured according to these procedures,

(iv) if Personal Health Information is held in electronic format, it must be encrypted or otherwise secured, and

(v) the Person Associated with the University should carry the file/electronic media with them at all times. If this is not possible, and the information is left unattended, the Person Associated with the University must ensure secure storage at all times by following reasonable security standards.

Retention and Destruction

2.12 Retention of Personal Information and Personal Health Information

(a) All Personal Information and Personal Health Information collected or maintained by University Offices or University Health Care Units must have Records Authority Schedules in place outlining the retention and destruction of the information. This information will be retained only as long as reasonably required for authorized purposes, and destroyed securely according to destruction guidelines approved for the University.

(b) The Personal Information and Personal Health Information of all Persons Associated with the University shall be maintained in a secure environment and shall be protected by administrative, technical, physical and electronic safeguards that are appropriate to the sensitivity of the information.

2.13 Disposal of Personal Information and Personal Health Information

(a) Personal Information and Personal Health Information shall be considered Confidential Information for the purposes of disposal and/or destruction.

(b) Control procedures shall be developed and implemented in all University Offices and University Health Care Units to segregate Confidential Information from non-confidential information and other waste streams.

(c) Confidential Information shall be disposed of by secure shredding or another confidential method of destruction.

Research

2.14 Research

(a) Research involving the use or disclosure of Personal Information and Personal Health Information held by the University requires:

(i) Formal approval by an appropriate institutional research ethics board. In reviewing the request, the appropriate research ethics board shall ensure that security and confidentiality conditions meet or exceed those described in Section 24 of PHIA.

(ii) The appropriate research ethics board shall ensure that the researcher enters into an agreement with the University as per Section 24(4) of PHIA.

(iii) The researcher and all agents and associates coming into contact with Personal Health Information must complete the University of

Manitoba Personal Health Information Act Training and sign the University's Personal Health Information Confidentiality Pledge.

Audit of Personal Health Information

2.15 The University shall conduct an audit of security safeguards at least every two (2) years. This audit shall be an overall audit that encompasses electronic, administrative, technical and physical safeguards employed to protect Personal Health Information held by the University, and will be conducted by Audit Services, or an authorized individual assigned by the University.

Breach of Privacy

2.16 A Breach of Privacy occurs when Personal Information, including Personal Health Information, is collected, accessed, used, disclosed, transported, transmitted, transferred or destroyed other than as authorized, or when the accuracy, confidentiality or integrity of the information is compromised. Breaches may include, but are not limited to, the viewing of Confidential Information by unauthorized individuals, the access, theft or loss of University Records and the unauthorized destruction of such information by deliberate means or by human or natural accident.

(a) Any Person Associated with the University who becomes aware of a possible or actual Breach of Privacy, shall immediately report the possible or actual Breach of Privacy to the head of the University Office or University Health Care Unit, who shall take immediate steps to contain the Breach.

(b) The head of the University Office or University Health Care Unit shall report the possible or actual Breach of Privacy to the dean, director or unit head of that University Office or University Health Care Unit and to the Access and Privacy Office.

(c) All Breaches of Privacy will be investigated by the Access and Privacy Office.

(d) The Access and Privacy Office will make recommendations for immediate and long-term corrective measures as necessary to protect the confidentiality, integrity and security of all Personal Information and Personal Health Information.

(e) If it is determined that a Breach of Privacy has occurred, appropriate remedial action shall be taken by the University. Such action may include disciplinary action, which will be implemented pursuant to and in accordance with the relevant collective agreement, University policies or by-laws.

(f) The Access and Privacy Office will act as a resource for all Persons Associated to the University regarding appropriate action to be taken following a Breach of Privacy.

Part III
Accountability

3.1 The Office of Legal Counsel is responsible for advising the President that a formal review of these Procedures is required.

3.2 The Chief Access and Privacy Officer of the University is responsible for the communication, administration and interpretation of these Procedures.

3.3 All supervisors and employees are responsible for complying with these Procedures and all Secondary Documents.

Part IV
Review

4.1 Governing Document reviews shall be conducted every ten (10) years by the Vice-President (Administration). The next scheduled review date for these Procedures is June 23, 2025.

4.2 In the interim, these Procedures may be revised or repealed if:

(a) the Approving Body deems it necessary or desirable to do so;

(b) the Policy is no longer legislatively or statutorily compliant;

(c) the Policy is now in conflict with another Governing Document; and/or

(d) the Parent Policy is revised or repealed.

Part V
Effect on Previous Statements

5.1 These Procedures supersede all of the following:

(a) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and

(b) all previous Administration Governing Documents on the subject matter contained herein.

Part VI
Cross References

6.1 These Procedures should be cross referenced to the following relevant Governing Documents, legislation and/or forms:

(a) Access and Privacy Policy

(b) PHIA Training and Pledge of Confidentiality Procedure

(c) Records Management Policy

(d) Closed Circuit TV (CCTV) Monitoring Policy