PROCEDURES: PRIVACY POLICY

AUTHORITY: University Administration

RESPONSIBILITY: Provost and Vice-President, Academic

Effective Date: April 1, 2016

PART 1

INTRODUCTORY PROVISIONS

Purpose:

To implement the Privacy Policy the procedures outlined in this document shall be followed.

Responsibility:

The Provost and Vice-President, Academic, on behalf of University Administration, is responsible for the development, administration, and review of this Policy.

Definitions:

"Commercial Activity" means: 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.

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

"Electronic Devices and Media" means: compact discs, computers, photocopiers, scanners, tablets, diskettes, tapes, hard drives, thumb or jump drives, phones, and all other moveable or removable devices and media that may be used for the Use, Disclosure, or storage of PI or PHI.

"Information Manager" means: 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.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

"Integrity" means: 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.

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

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

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

"Secured Place" means: a physical environment for the temporary or permanent storage of, or for the Use, processing, or communication of PI or PHI which physical environment has the following characteristics:

- is readily accessible to only Authorized Persons,
- is keyed or otherwise locked to allow entrance or access to Authorized Persons only,
- is protected by controls to protect against theft, vandalism, or accidental destruction or loss,
- is protected by controls to minimize loss, destruction, or deterioration caused by fire, water, humidity, or other hazards, and
- has proper containers and adequate labelling to reduce accidental loss or destruction.

"Social Media" means: websites and digital applications that enable users to create and share information, ideas, and similar content and create connections.

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

"University Human Research Ethics Board-approved Protocol" means: a protocol approved pursuant to the UHREB's Policies and Procedures (Hyperlink).

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.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

PART 2

COMMON REQUIREMENTS IN RESPECT OF PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION

Collection of Personal or Personal Health Information

1. Only Authorized Persons may Collect PI or PHI.
2. Collection must be authorized by a statute or alternatively where the information Collected relates directly and is necessary for an existing service, program, or activity of the University.
3. 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.
4. 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.
5. 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.
6. If Collecting PI or PHI directly from the individual to whom the information relates, he or she 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.
7. 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.
8. 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.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

Access to Personal or Personal Health Information

Only Authorized Persons may access PI or PHI and only as required for authorized, necessary purposes.

Use and Disclosure of Personal or Personal Health Information

1. Only Authorized Persons may Use and Disclose PI or PHI and only 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 and cited in Table 1 below.

TABLE 1

FIPPA	PHIA
s.43 or 45 (Appendix "A" attached)	s.21 (Appendix "B" attached)
s.44 (Appendix "C" attached)	s.22 (Appendix "D" attached)
s.47 or 48 (Hyperlink)	s.24 (Hyperlink)
s.44.1 (Hyperlink)	s.25 (Hyperlink)

2. PI may be Used or Disclosed for a consistent purpose in accordance with s.45 of FIPPA (see Appendix "A" attached).
3. 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.
4. 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.
5. The Use and Disclosure of PI or PHI shall be limited to the fewest persons necessary to carry out the purpose for which the information is Used or Disclosed.
6. 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 and cited in Table 1 above.
7. Before Using or Disclosing PI or PHI, Authorized Persons shall take reasonable steps to ensure that the information is accurate, up-to-date, complete, and not misleading.
8. Disclosure to an Information Manager may only be made as permitted under s.44.1 of FIPPA (Hyperlink) or s.25 of PHIA (Hyperlink).

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

9. 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 a University Human Research Ethics Board-approved Protocol.
10. 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.

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

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

1. be in writing or otherwise electronically or manually recorded,
2. relate to the purpose for which the information is Used or Disclosed,
3. 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,
4. be voluntary, and
5. not be obtained through misrepresentation.

Security of Personal or Personal Health Information

1. Responsible Administrators shall implement reasonable administrative, physical, and technical security safeguards that ensure the confidentiality, security, accuracy, and Integrity of the PI or PHI in their custody or under their control and protect against risks such as unauthorized access, Use, Disclosure, or destruction.
2. In determining the reasonableness of security safeguards, Responsible Administrators shall take into account the degree of sensitivity and medium of the PI or PHI to be protected.
3. Reasonable safeguards shall, at a minimum, include the safeguards outlined in these Procedures.

Security of Personal or Personal Health Information – Administrative Safeguards

1. Only Authorized Persons may have access to PI or PHI.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

2. University employees shall regularly attend privacy training offered by the University's Information and Privacy Officer or complete other training as may be required by the University.
3. Authorized Persons who may Collect, Use, Disclose, store, or destroy PHI shall complete PHIA training and sign the PHIA Pledge of Confidentiality (see Appendix "E" attached).
4. As may be required, specific, Department-level policies and procedures regarding the Collection, Use, Disclosure, and protection of PI or PHI according to its sensitivity, shall be implemented, and copies provided to the University's Information and Privacy Officer.

Security of Personal or Personal Health Information – Personal Safeguards

1. Physical access to PI or PHI shall be limited to Authorized Persons only.
2. Authorized Persons shall not discuss others' PI or PHI in the presence of those who are not authorized to know the information, and therefore shall not discuss others' PI or PHI in public, unsecured, or open places where those who are not authorized to know the information are likely to be or have access.
3. Paper files and Electronic Devices and Media containing PI or PHI shall be stored in a Secured Place at all times other than when being Used as a necessary function of work.
4. PI or PHI shall not be transported or otherwise removed from a Secured Place unless necessary.
5. If transporting or otherwise removing PI or PHI from a Secured Place, only the minimum amount of information necessary may be transported and it must be secured in a briefcase or similar closed, opaque container and under the care and control of an Authorized Person
6. Whenever practicable, PI or PHI shall be de-identified before removing it from a Secured Place.
7. PI or PHI should not be left unattended or stored in a vehicle.
8. Where file folders, records storage boxes, Electronic Devices and Media, and other storage containers contain PI or PHI, labelling or other means of identification shall only reveal the minimum amount of information that is necessary for identification and Use.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

Security of Personal Health Information – Technical Safeguards

1. Access to PI or PHI maintained in electronic form shall be limited to Authorized Persons.
2. Software, hardware, or operating system access controls such as strong passwords shall be used to prevent against unauthorized Use, Disclosure, or destruction of PI or PHI.
3. Display screens shall be cleared without delay.
4. Computers shall be logged off or shut down when not in use.
5. If communicating PI or PHI through the mail or by fax, telephone, email, or Social Media, Authorized Persons shall consult the *Guidelines for the Communication of Personal and Personal Health Information* (Hyperlink) and take appropriate action.
6. Password protection/encryption (Hyperlink) shall be used if transporting PI or PHI on Electronic Devices and Media.
7. The Use and Disclosure of PI or PHI shall be audited and tracked within the resources available.
8. When Electronic Devices and Media are disposed of or used for another purpose, all PI or PHI shall be completely and effectively removed or destroyed by overwriting deleted information, reformatting the electronic storage medium, or physically destroying the electronic storage medium.

Security of Personal or Personal Health Information – Destruction

PI or PHI shall be destroyed in a manner that takes into account the sensitivity of the information and protects the security, accuracy, Integrity, and confidentiality of the individual's information, including at a minimum:

1. shredding of all paper Records, and
2. effective and complete deletion of the information on all Electronic Devices and Media.

Security of Personal or Personal Health Information – Shared Network Drives

1. Where a Department utilizes a shared network drive to maintain PI or PHI, the Responsible Administrator shall:
    a. ensure that access to PI or PHI is restricted to Authorized Persons only,
    b. maintain a Record of the persons authorized to access PI or PHI, and
    c. regularly review the authorizations and update as required.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

Privacy Breaches

1. 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 Information and Privacy Officer and the Responsible Administrator.
2. The University's Information and Privacy Officer and the Responsible Administrator shall determine whether the alleged Privacy Breach warrants investigation, taking into consideration:
    a) the length of time that has elapsed since the alleged Privacy Breach,
    b) if the alleged Privacy Breach is trivial, or the complaint is otherwise not in good faith or frivolous, and
    c) if the circumstances of the alleged Privacy Breach warrant investigation.
3. If a Privacy Breach warranting investigation is confirmed as a Privacy Breach under FIPPA,PHIA, or PIPEDA, the University's Information and Privacy Officer and Responsible Administrator shall:
    a) take steps to contain the Privacy Breach, and
    b) implement corrective procedures to address the Privacy Breach and lessen the likelihood of future Privacy Breaches.
4. The University's 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) in the case of serious Privacy Breaches or Privacy Breaches in the course of Commercial Activity, the Ombudsman of Manitoba, the Privacy Commissioner of Canada, or law enforcement agencies as may be appropriate.

Retention and Disposition of Personal or Personal Health Information

1. 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.
2. PI or PHI identified for destruction shall be destroyed in a manner that prevents unauthorized access, Use, or Disclosure, as set out in this Policy

Research Involving Personal or Personal Health Information No person shall Collect, Use, or Disclose PI or PHI for research except as permitted by a University Human

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

Research Ethics Board-approved Protocol and in accordance with FIPPA (Hyperlink) or PHIA's (Hyperlink) requirements.

Requests for Access to Personal Information

1. Excepting 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 Information and Privacy Officer together with any fees that may be required to pay.

Requests for Access to Personal Health Information

1. 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 Information and Privacy Officer.
2. The Department or the University's 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. The Department or the University's 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.
4. 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.
5. 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 Information and Privacy Officer or direct the requester to make an application through the University's Information and Privacy Officer.
6. Prior to permitting an individual to examine or receive a copy of his or her PHI, the Department or the University's Information and Privacy Officer shall confirm the identity of the requester.
7. On request, the Department or the University's Information and Privacy Officer shall provide the individual with an explanation of any term, code, or abbreviation used in the PHI.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

8. The Department or the University's Information and Privacy Officer is not required to permit an individual to examine or copy his or her PHI pursuant to subsection 11(1) of PHIA (Hyperlink).
9. A Department or the University's 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.

Requests for Correction of Personal or Personal Health Information

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

Exercising Rights of Another Person

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

PART 3

ADDITIONAL REQUIREMENTS IN RESPECT OF PERSONAL HEALTH INFORMATION

Definitions:

"Demographic or Eligibility Information" means: PHI about an identifiable individual as defined in PHIA, including the individual's:

- 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.

"Electronic Health Information System" means: a computer system or systems delegated to hosting PHI for access by Authorized Persons.

"Record of User Activity" means: 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 (see Appendix "D" attached).

Requirements

Security of Personal Health Information – Electronic Health Information Systems

1. 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 Information and Privacy Officer.
2. A Record of User Activity may be generated manually or electronically.
3. 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 an Authorized Person 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.

Audit of Personal Health Information Security Safeguards

1. 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.
2. If an audit identifies deficiencies in the University's security safeguards, the University's 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. The University's Information and Privacy Officer shall document the findings of the audit along with any recommendations to monitor and ensure compliance under PHIA.

Notice of Right to Access Personal Health Information

1. Departments that retain PHI must use 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 ss. 11(1) (Hyperlink).
2. 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 individuals' attention.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

PART 4

REVIEW

Review:

These Procedures shall be reviewed in conjunction with the Policy review at least once every five years or more frequently as required to reflect changes in legislation or to related University policies, procedures, and processes.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

APPENDIX "A"

RESTRICTIONS ON USE OF PERSONAL INFORMATION

The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175

Use of personal information

43 *A public body may use personal information only*
(a) for the purpose for which the information was collected or compiled under subsection 36(1) or for a use consistent with that purpose under section 45;
(b) if the individual the personal information is about has consented to the use; or
(c) for a purpose for which that information may be disclosed to the public body under section 44, 47 or 48.

Consistent purposes

45 *For the purpose of clauses 43(a) and 44(1)(a), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure*
(a) has a reasonable and direct connection to that purpose; and
(b) is necessary for performing the statutory duties of, or for delivering an authorized service or program or carrying out an activity of, the public body that uses or discloses the information.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

APPENDIX "B"

RESTRICTIONS ON USE OF PERSONAL HEALTH INFORMATION

The Personal Health Information Act, C.C.S.M. c. P33.5

Restrictions on use of information

21 *A trustee may use personal health information only for the purpose for which it was collected or received, and shall not use it for any other purpose, unless*
(a) the other purpose is directly related to the purpose for which the personal health information was collected or received;
(b) the individual the personal health information is about has consented to the use;
(c) use of the information is necessary to prevent or lessen a serious and immediate threat to
(i) the health or safety of the individual the information is about or another individual, or
(ii) public health or public safety;
(c.1) the information is demographic information about an individual, or his or her PHIN, and is used to
(i) confirm eligibility for health care or payment for health care, or
(ii) verify the accuracy of demographic information or PHIN;
(c.2) the information is demographic information about an individual and is used to collect a debt the individual owes to the trustee, or to the government if the trustee is a department;
(d) the trustee is a public body or a health care facility and the personal health information is used
(i) to deliver, monitor or evaluate a program that relates to the provision of health care or payment for health care by the trustee, or
(ii) for research and planning that relates to the provision of health care or payment for health care by the trustee;
(e) the purpose is one for which the information may be disclosed to the trustee under section 22; or
(f) use of the information is authorized by an enactment of Manitoba or Canada.

APPENDIX "C"

RESTRICTIONS ON DISCLOSURE OF PERSONAL INFORMATION

The Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175

Disclosure of personal information

44(1) A public body may disclose personal information only

(a) for the purpose for which the information was collected or compiled under subsection 36(1) or for a use consistent with that purpose under section 45;

(b) if the individual the information is about has consented to its disclosure;

(c) in accordance with Part 2;

(d) for the purpose of complying with an enactment of Manitoba or Canada, or with a treaty, arrangement or agreement entered into under an enactment of Manitoba or Canada;

(e) in accordance with an enactment of Manitoba or Canada that authorizes or requires the disclosure;

(f) to a minister or an elected official of the public body, if the information is necessary to carry out his or her responsibilities;

(f.1) to an officer or employee of a public body, for the purpose of delivering a common or integrated service, program or activity, if the information is necessary to deliver the service, program or activity and the officer or employee to whom the information is disclosed needs the information to carry out his or her responsibilities;

(g) for the purpose of managing or administering personnel of the Government of Manitoba or the public body;

(h) to the Auditor General or any other person or body for audit purposes;

(i) to the Government of Canada in order to facilitate the monitoring, evaluation or auditing of shared cost programs or services;

(j) for the purpose of determining or verifying an individual's suitability or eligibility for a program, service or benefit;

(j.1) for the purpose of

(i) evaluating or monitoring a service, program or activity of the Government of Manitoba or the public body, or

(ii) research and planning that relates to a service, program or activity of the Government of Manitoba or the public body;

(k) for the purpose of enforcing a maintenance order under The Family Maintenance Act;

(l) where necessary to protect the mental or physical health or the safety of any individual or group of individuals;

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

(m) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information or with a rule of court that relates to the production of information;
(n) for use in providing legal advice or legal services to the Government of Manitoba or the public body;
(o) for the purpose of enforcing a legal right that the Government of Manitoba or the public body has against any person;
(p) for the purpose of
(i) determining the amount of or collecting a fine, debt, tax or payment owing by an individual to the Government of Manitoba or to the public body, or to an assignee of either of them, or
(ii) making a payment;
(q) for use in existing or anticipated legal proceedings to which the Government of Manitoba or the public body is a party;
(r) for law enforcement purposes or crime prevention;
(s) if the public body is a law enforcement agency and the information is disclosed to
(i) another law enforcement agency in Canada, or
(ii) a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;
(t) for the purpose of supervising an individual in the custody of or under the control or supervision of a correctional authority;
(u) where disclosure is necessary for the security of a correctional institution;
(v) by transfer to the Archives of Manitoba or to the archives of the public body for records management or archival purposes;
(w) to an officer of the Legislature, if the information is necessary for the performance of the duties of that officer;
(x) to an expert for the purposes of clause 24(b);
(x.1) if the personal information is information of a type routinely disclosed in a business or professional context, and the disclosure
(i) is limited to the individual's name, position name or title, business address, telephone number, facsimile number and e-mail address, and
(ii) does not reveal other personal information about the individual or personal information about another individual;
(y) for the purpose of
(i) contacting a relative or friend of an individual who is injured, incapacitated or ill,
(ii) assisting in identifying a deceased individual, or
(iii) informing the representative or a relative of a deceased individual, or any other person it is reasonable to inform in the circumstances, of the individual's death;

(z) to a relative of a deceased individual if the head of the public body reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy;
(aa) to an information manager in accordance with section 44.1;
(bb) when the information is available to the public;
(cc) in accordance with section 47 or 48; or
(dd) if the public body is an educational institution and the disclosure is for the purpose of fundraising activities of the educational institution, but only if

(i) the disclosure is of information in the alumni records of the educational institution and is reasonably necessary for the fundraising activities, and
(ii) the educational institution and the persons to whom the information is disclosed have entered into a written agreement that complies with subsection (1.1).

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

APPENDIX "D"

RESTRICTIONS ON DISCLOSURE OF PERSONAL HEALTH INFORMATION

The Personal Health Information Act, C.C.S.M. c. P33.5

Disclosure without individual's consent

22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is

(a) to a person who is or will be providing or has provided health care to the individual, to the extent necessary to provide health care to the individual, unless the individual has instructed the trustee not to make the disclosure;

(b) to any person if the trustee reasonably believes that the disclosure is necessary to prevent or lessen a serious and immediate threat to

(i) the health or safety of the individual the information is about or another individual, or

(ii) public health or public safety;

(c) for the purpose of

(i) contacting a relative or friend of an individual who is injured, incapacitated or ill,

(ii) assisting in identifying a deceased individual, or

(iii) informing the representative or a relative of a deceased individual, or any other person it is reasonable to inform in the circumstances, of the individual's death;

(d) to a relative of a deceased individual if the trustee reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy;

(e) required for

(i) the purpose of peer review by health professionals,

(ii) the purpose of review by a standards committee established to study or evaluate health care practice in a health care facility or health services agency,

(iii) the purpose of a body with statutory responsibility for the discipline of health professionals or for the quality or standards of professional services provided by health professionals, or

(iv) the purpose of risk management assessment;

(f) in accordance with subsection 22(2.2) (disclosure to another government), section 23 (disclosure to patient's family), section 23.1 (disclosure to religious organization), section 23.2 (disclosure for fundraising), section 24 or 24.1 (disclosure for health research) or section 25 (disclosure to an information manager);

(g) for the purpose of

(i) delivering, evaluating or monitoring a program of the trustee that relates to the provision of health care or payment for health care, or

(ii) for research and planning that relates to the provision of health care or payment for health care by the trustee;

(g.1) to another trustee who requires the information to evaluate or monitor the quality of services the other trustee provides;

(g.2) for the purpose of determining or verifying the individual's eligibility for a program, service or benefit, if the information disclosed is limited to the individual's demographic information;

(g.3) to another trustee for the purpose of de-identifying the personal health information;

(h) to a computerized health information network established by a body specified in subsection (2.1), in which personal health information is recorded for the purpose of

(i) providing health care,

(ii) facilitating the evaluation or monitoring of a program that relates to the provision of health care or payment for health care, or

(iii) facilitating research and planning that relates to the provision of health care or payment for health care;

(i) to the government, another public body, or the government of another jurisdiction or an agency of such a government, to the extent necessary to obtain payment for health care provided to the individual the personal health information is about;

(i.1) for the purpose of collecting a debt owed by the individual to the trustee, or to the government if the trustee is a department, if the information disclosed is limited to demographic information;

(j) to a person who requires the personal health information to carry out an audit for or provide legal services to a trustee, if the trustee reasonably believes that the person will not use or disclose the personal health information for any other purpose and will take appropriate steps to protect it;

(k) required in anticipation of or for use in a civil or quasi-judicial proceeding to which the trustee is a party, or to which the government is a party if the trustee is a department;

(k.1) required in anticipation of or for use in the prosecution of an offence;

(l) required to comply with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of the personal health information, or with a rule of court concerning the production of the personal health information;

(l.1) required by police to assist in locating an individual reported as being a missing person, if the information disclosed is limited to demographic information;

(m) for the purpose of

(i) an investigation under the enforcement of an enactment of Manitoba respecting payment for health care, or

(ii) an investigation or enforcement respecting a fraud relating to payment for health care;

(n) for the purpose of complying with an arrangement or agreement entered into under an enactment of Manitoba or Canada; or

(o) authorized or required by an enactment of Manitoba or Canada.

Computerized health information network

22(2.1) For the purpose of clause (2)(h), a computerized health information network may be established by

(a) the government or a government agency;

(b) the Government of Canada or of another province or territory or any agency of such a government;

(c) an organization representing one or more governments; or

(d) a trustee that is a public body specified in the regulations.

Disclosure by minister to another government

22(2.2) The minister or his or her designate may disclose an individual's personal health information to the government of another jurisdiction in Canada, or an agency of such a government, without the individual's consent, if

(a) the individual the information is about normally resides in the other jurisdiction;

(b) the information is about health care he or she received in Manitoba; and

(c) the government of the other jurisdiction requires the information for the purpose of monitoring or evaluating the extra-jurisdictional provision of health care to its residents.

Limit on disclosure

22(3) A trustee may disclose information under subsection (2), (2.1) or (2.2) only to the extent the recipient needs to know the information.

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy

APPENDIX "E"

PHIA PLEDGE OF CONFIDENTIALITY

I acknowledge that I have completed personal health information (PHI) training offered through the University of Winnipeg (the University). I have read and understood 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 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 of Authorized Person: _____
*Signature:*_____
*Date:*_____
Witness: _____

Approved: March 29, 2016
Revised:
Cross Reference:
Privacy Policy