ACADEMIC COUNCIL REPORT

SESSION: **ACTION REQUESTED:**

Public ☒ **Decision** ☐
Discussion/Direction ☒
Information ☐

Financial Impact ☐ **Yes** ☒ **No** **Included in Budget** ☐ **Yes** ☒ **No**

TO: **Academic Council**

DATE: **September 27, 2022**

PRESENTED BY: **Niall O'Halloran, Manager, Privacy & Policy**
Sara Gottlieb, General Counsel

SUBJECT: **Draft Personal Health Information Privacy Policy**

ACADEMIC COUNCIL MANDATE:

- Under the Policy Framework, and the University's Act, the Board of Governors has a "duty to consult" on "all academic, research, service and institutional policies".
- We are submitting this report and draft policy amendment to Academic Council to request discussion and comments on the draft Privacy Policy: Personal Health Information Collection, Use and Disclosure and related Procedure.

BACKGROUND/CONTEXT & RATIONALE:

- The University operates student services that are considered health care under the Personal Health Information Protection Act (PHIPA), including Student Mental Health Services and Athletic Therapy. PHIPA allows higher education institutions to chose the structure by which the personal health information associated with health-related student services is governed. Institutions can take on the role of "health information custodian" or they can assign that role to one or more employees or contractors.
- The new policy defines the University as a health information custodian and sets out roles and responsibilities, rights of privacy and access, consent for collection and use, disclosure, retention and disposal, correction of records, breach of privacy, safeguards for PHI, employee awareness and training and continuity of care. Adopting this policy will allow the university to improve student services by ensuring all staff involved in the provision of health care have the proper training to protect student privacy.

RESOURCES REQUIRED:

- External trainer will be engaged for staff who have obligations under PHIPA.

IMPLICATIONS:

- N/A

ALIGNMENT WITH MISSION, VISION, VALUES & STRATEGIC PLAN:

- This policy supports the university's culture of trust and belonging by ensuring there is a framework of responsibilities in place to ensure compliance with privacy law.

ALTERNATIVES CONSIDERED:

- N/A

CONSULTATION:

- The policy was drafted in consultation between the Privacy Office, Student Mental Health Services and Athletic Therapy. In order to ensure compliance with PHIPA, a draft was reviewed by external legal counsel.

- Policy Advisory Committee
- Academic Council
- Online Consultation
- Administrative Leadership Team
- Audit & Finance Committee
- Board of Governors

COMPLIANCE WITH POLICY/LEGISLATION:

- This policy supports compliance with PHIPA, and defines roles and responsibilities within the university to enable Ontario Tech to meet requirements. The General Counsel has been delegated the role of Chief Privacy Officer under this policy.

NEXT STEPS:

- Continue consultation and approval path outlined above

MOTION FOR CONSIDERATION:

- N/A

SUPPORTING REFERENCE MATERIALS:

- Privacy Policy: Personal Health Information Collection, Use and Disclosure and related Procedure)

Classification Number	LCG XXAB
Framework Category	Legal, Compliance and Governance
Approving Authority	Board of Governors
Policy Owner	General Counsel
Approval Date	DRAFT FOR CONSULTATION
Review Date	
Supersedes	

PRIVACY POLICY:

PERSONAL HEALTH INFORMATION COLLECTION, USE AND DISCLOSURE

PURPOSE

1. The purpose of this Policy is to establish a standard for privacy and confidentiality of Personal Health Information to ensure compliance with the University's obligations under Ontario's Personal Health Information Protection Act. As a health information custodian, the University is responsible for ensuring that Personal Health Information is protected and treated with respect and sensitivity at all times.

DEFINITIONS

2. For the purposes of this Policy the following definitions apply:

"Agent" means any person who is authorized by the University to perform services or activities in respect of Personal Health Information on the University's behalf and for the purposes of the University. An agent includes a Health Care Practitioner, or another University employee or volunteer who supports Practitioners, and any member of the University Counselling Team.

"Chief Privacy Officer" means the member of SLT with delegated responsibility for addressing compliance obligations related to applicable privacy law.

"Health Care" means any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that:

- is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition;
- is carried out or provided to prevent disease or injury or to promote health;
- is carried out or provided as part of palliative care, and includes:
- the compounding, dispensing or selling of a drug, a device, equipment or any other item to an individual, or for the use of an individual, pursuant to a prescription; and
- a community service that is described in subsection 2 (3) of the Long-Term Care Act, 1994 and provided by a service provider within the meaning of that Act.

"Health Care Practitioner" or **"Practitioner"** means:

- A person who is a member of a health care professions within the meaning of the *Regulated Health Professions Act, 1991* and who provides Health Care;
- A person who is registered as a drugless practitioner under the *Drugless Practitioners Act* and who provides Health Care;

- a person who is a member of the Ontario College of Social Workers and Social Service Workers and who provides health care; or
- any other person whose primary function is to provide health care.

"Health Care Unit" means a unit or service acting for or on behalf of the University to provide Health Care or retain and protect Personal Health Information.

"Personal Heath Information" means oral or written information that is collected, used or disclosed by the University or anyone acting on behalf of the University, about an identifiable individual if the information:

- Relates to the individual's physical or mental health, including family health history;
- Relates to the provision of Health Care, including the identification of a person as a provider of HealthCare to an individual;
- Is a plan of service for individuals requiring long-term care;
- Relates to payment or eligibility for Health Care or eligibility for coverage for Health Care;
- Relates to the donation of body parts or bodily substances or is derived from the testing or examination of such parts or substances;
- Is the individual's health number;
- Identifies an individual's substitute decision-maker; or
- Is included in a record containing Personal Health Information.

"Personal Information" means information about an identifiable individual**.**

"Privacy Breach" or **"Breach"** means an incident where Personal Information or Personal Health Information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws.

"Privacy Impact Assessment" or **"PIA"** means a risk management tool used to identify the actual or potential effects that a proposed University project/initiative may have on an individual's privacy or the University's information privacy and security practices/procedures.

"University Counselling Team" means advisors and counsellors from Student Mental Health Services, Student Accessibility Services, the Career Centre and Indigenous Student Services, as well as graduate –level student trainees (e.g. internship and practicum students) and administrative staff.

SCOPE AND AUTHORITY

3. This Policy applies to Health Care Units and services of the University that support Health Care Practitioners and/or collect, use and disclose Personal Health Information to fulfil their mandate.

4. The University is the Health Information Custodian for records containing Personal Health Information created by Heath Care Units.

5. This Policy does not apply to Health Care services contracted by the University from a third party to be directly provided by the third party. Any contracts for such third party services must nonetheless comply with the Personal Health Information requirements under PHIPA.

6. The General Counsel, or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of this Policy.

POLICY

The University is committed to the privacy and security of Personal Information and Personal Health Information it collects, uses and discloses. It maintains privacy in compliance with the Personal Health Information Protection Act, 2004 and its regulations (PHIPA).

7. Roles and Responsibilities

7.1. Chief Privacy Officer will:

a) Ensure that secure information practices are in place that comply with the requirements of PHIPA, and that all Health Care Units are informed of and receiving training on their duties under PHIPA.

b) Respond to requests of an individual for access to or correction of a record of Personal Health Information about the individual that is in the custody or under the control of the University.

c) Ensure compliance with reporting obligations under PHIPA.

d) Oversee the management and response to any potential or actual Privacy Breaches.

7.2. Agents will:

a) Conduct searches and review records in access to information requests involving clinical records related to their area of practice or duties on behalf of the University.

b) Understand and comply with information privacy practices established to safeguard records containing Personal Health Information and other sensitive information.

c) Report Privacy Breaches or situations that could lead to potential Privacy Breaches to the Privacy Office.

d) Maintain privacy and confidentiality of Personal Health Information created, collected or used in their role.

7.3. Privacy Office will:

a) Coordinate and respond to requests for access to records containing Personal Health Information under PHIPA and the Freedom of Information and Protection of Privacy Act (FIPPA) (see Access to Information and the Protection of Privacy Policy for the University's FIPPA practices and procedures, [link]).

b) Support compliance with PHIPA and FIPPA through education and advice on developing information practices that safeguard records containing Personal Health Information and other sensitive information.

c) Respond to inquiries from the public about the University's information privacy practices.

d) Investigate and respond to potential Privacy Breaches.

e) Ensure information is made publicly available regarding the University's privacy policies and practices.

f) Ensure compliance with reporting obligations under PHIPA and FIPPA.

g) Monitor compliance with this Policy and PHIPA by whatever means are appropriate to the circumstances.

7.4. Managers/Supervisors of Health Care Units will:

a) Ensure awareness and enforcement of, and compliance with, applicable privacy policies, laws, procedures, protocols and practices.

b) Ensure University staff and Agents are up to date and have completed appropriate privacy training and education.

c) Immediately report all actual or suspected Privacy Breaches to the Privacy Office.

d) At the request of, and in coordination with the Policy Office, support investigations into suspected Privacy Breaches.

e) Assist the Privacy Office in responding to privacy queries and complaints.

f) Receive and implement recommendations from the Privacy Office regarding necessary actions and/or remedial measures following a Breach, including actions to prevent a reoccurrence.

g) Receive and implement recommendations from the Privacy Office regarding necessary actions following a Privacy Impact Assessment.

h) In consultation with Human Resources, take appropriate remedial and/or disciplinary action to ensure incidents are addressed and not repeated.

i) Where requested, assist with client/patient or an individual's requests for access and correction and withdrawal of consent to the collection, use or disclosure of their Personal Health Information/Personal Information.

8. Application to members of regulated health professions

8.1. This Policy applies to members of regulated health professions acting on behalf of the University, while they are performing within the scope of practice set out by enabling legislation, as well as performing authorized acts that constitute Health Care.

8.2. Employees whose duties include acts that are not within their regulated scope of practice are not considered Practitioners while they are performing those duties, but are still bound by any applicable privacy and confidentiality requirements associated with the records and information used in performing those duties, including this Policy.

8.3. Individual Health Professionals must differentiate between Health-Related Acts and other activities for the purpose of fulfilling obligations under PHIPA and their regulatory college. This determination will be made based on the Health Professional's understanding of their obligations, guidance from the regulatory college, and the scope of practice as defined by the enabling legislation.

9. Right to Privacy and Access

9.1. Individuals have a right to privacy and a right to control how their Personal Health Information is collected, used, disclosed, retained and disposed of, subject to limited exceptions in PHIPA.

9.2. Individuals have a right of access to their own Personal Health Information.

10. Consent for collection and use of Personal Health Information

10.1. The University will provide a notice of collection that describes the information it will collect or create, the purposes for collecting Personal Health Information or creating records, the uses for those records and how that information will be shared. The notice will include any exceptions to the expectation of confidentiality.

10.2. Consent from individuals receiving Health Care will be obtained in writing at or before the time information is collected.

11. Disclosure of Personal Health Information

11.1. Disclosure of Personal Health Information to an individual who is not an Agent will only be done with express consent of the individual to whom the Personal Health Information relates, except as permitted or required by legislation.

12. Retention and Disposal of Personal Health Information

12.1. Records containing Personal Health Information will be retained and securely destroyed in accordance with the University's Records Classification and Retention Schedule. Record destruction will occur in a manner that is in compliance with PHIPA and protects information until it is permanently destroyed.

13. Access and Correction to Record

13.1. Individuals have a right to be informed of the existence, use and disclosure of their Personal Health Information. Under PHIPA, individuals can make a formal request to access their records, or to request a correction to their record.

14. Safeguards for Personal Health Information

14.1. The University will establish appropriate technical and administrative safeguards to ensure secure storage and maintain confidentiality of Personal Health Information.

14.2. Access rights to information systems with Personal Health Information will be granted only to authorized personnel. Access rights will be based on the role of the individual, and the level of access required to fulfil that role.

15. Breach of Privacy

15.1. The University will investigate and respond to any potential or actual breach of privacy or loss of Personal Health Information in compliance with PHIPA.

16. Employee Awareness and Training and Mandatory Confidentiality Agreements

16.1. Agents are expected to be knowledgeable of and abide by this policy and related privacy and security practices.

16.2. The University will make its employees aware of the importance of maintaining the confidentiality of Personal Health Information.

16.3. Health Care Unit Managers/Supervisors, in collaboration with the Privacy Office, will identify Health Care Practitioners and employees who support Health Care services and maintain a roster of Agents. Agents must sign the University confidentiality agreement and are subject to mandatory privacy training requirements.

17. Continuity of care

17.1. To ensure the continuity of care and support for all individuals receiving Health Care, Agents may consult with each other. This occurs on a need-to-know basis, meaning that Personal Health Information will only be shared when warranted or required to provide support. Personal Health Information will be held in confidence, and will only be released with individual consent, or in accordance with applicable law.

MONITORING AND REVIEW

18. This Policy will be reviewed as necessary and at least every three years. The General Counsel, or successor thereof, is responsible to monitor and review this Policy.

RELEVANT LEGISLATION

19. Personal Health Information Protection Act, 2004, S.O. 2004, as amended

RELATED POLICIES, PROCEDURES & DOCUMENTS

20. Access to Information and the Protection of Privacy Policy

Health Record Access and Release Procedure

Records Management Policy

Records Disposition Procedure

Records Classification and Retention Schedule

Classification	LCG XXAB.1
Parent Policy	Legal, Compliance and Governance
Framework Category	Board of Governors
Approving Authority	General Counsel
Policy Owner	DRAFT FOR CONSULTATION
Approval Date	
Review Date	
Supersedes	

PROCEDURE FOR RELEASE OF PERSONAL HEALTH INFORMATION

PURPOSE

1. The purpose of these Procedures is to outline a process for responding to requests for Personal Health Information consistent with applicable legislation.

DEFINITIONS

2. For the purposes of these Procedures the following definitions apply:

"Health Care" means any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that:

- is carried out or provided to diagnose, treat or maintain an individual's physical or mental condition;
- is carried out or provided to prevent disease or injury or to promote health; or
- is carried out or provided as part of palliative care, and includes:
- the compounding, dispensing or selling of a drug, a device, equipment or any other item to an individual, or for the use of an individual, pursuant to a prescription; and
- a community service that is described in subsection 2 (3) of the Long-Term Care Act, 1994 and provided by a service provider within the meaning of that Act.

"Health Care Practitioner" or **"Practitioner"** means:

- A person who is a member within the meaning of the *Regulated Health Professions Act, 1991* and who provides Health Care;
- A person who is registered as a drugless practitioner under the *Drugless Practitioners Act* and who provides Health Care;
- a person who is a member of the Ontario College of Social Workers and Social Service Workers and who provides health care; or
- *any other person whose primary function is to provide health care for payment.*

"Health Care Unit" means a unit or service acting for or on behalf of the University to provide Health Care or retain and protect Personal Health Information.

"Personal Heath Information" means oral or written information that is collected, used or disclosed by a Custodian, about an identifiable individual if the information:

- Relates to the individual's physical or mental health, including family health history;

- Relates to the provision of health care, including the identification of persons providing care;
- Is a plan of service for individuals requiring long-term care;
- Relates to payment or eligibility for health care;
- Relates to the donation of body parts or bodily substances or is derived from the testing or examination of such parts or substances;
- Is the individual's health number; or identifies an individual's substitute decision-maker.
- Is included in a record containing Personal Health Information.

"Requester" means a person who makes a request for Personal Health Information from the University.

SCOPE AND AUTHORITY

3. These Procedures apply to all requests for Personal Health Information in the custody and control of the University.

4. The General Counsel, or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of these Procedures.

PROCEDURES

5. Request for record transfer

5.1. A client of a University Health Care Unit may request the transfer of some or all of their records. The intended recipient will dictate the process to be followed.

5.2. **Transfers to another Health Care Practitioner** require the client to submit a consent form [LINK] to the Health Care Unit, requesting records be transferred to the other Health Care Practitioner. Consistent with PHIPA section 38 (1), personal health information about an individual may be disclosed when it is reasonably necessary for the provision of health care. Prior to making a disclosure, University Health Care Unit staff will ensure there is no notice of instruction in the client's file that limits disclosure

5.3. **Transfers to an internal Ontario Tech unit** require the client to submit a consent form [LINK] to the Health Care Unit describing the type of record sharing allowed with the internal Ontario Tech unit.

5.4. **Transfers to an external entity or individual other than a Health Care Practitioner** will follow the process for Formal request for access to Personal Health Information.

6. Formal request for access to Personal Health Information

6.1. All requests for Personal Health Information in the custody and control of the University will be formal requests made in writing to the Health Care Unit or Privacy Office using the form provided and submitted by mail or in person.

a) When submitting a formal access request, sufficient detail must be provided to enable an experienced employee, with a reasonable effort, to identify the personal information being sought.

b) Requests for Personal Health Information must be accompanied by a $5.00 application fee. The application fee may be made by cheque or money order.

6.2. Requests for Mixed Records or requests for a complete file made directly to a Health Care Unit will be forwarded to the Privacy Office for processing. Other requests may also be forwarded to the Privacy Office at the Director or Manager's discretion.

6.3. Requests will be processed in accordance with the *Personal Health Information Act* and/or *Freedom of Information and Protection of Privacy Act*, as applicable.

7. Request for a Record Search

7.1. If the Privacy Offices receives a formal request, either directly from a requester or from a Health Care Unit, the Chief Privacy Officer or delegate will prepare and send a search memo to the applicable Health Care Unit. The original request and any signed consent forms will be included to allow the identity of the Requester to be verified.

8. Search for Personal Health Information

8.1. Before initiating a search, the Health Care Unit will verify the signed consent of the Requester, and initiate a tracking form with the identity of the patient. If necessary, additional distinguishing identifiers will be verified, such as health card number, address, date of birth.

8.2. The Health Care Unit will designate a member of staff to track and manage ongoing access request files. The designate will verify the request and consent for completeness and specific request details. Requests may be made for:

a) a full file; or

b) specific date range; and/or

c) specific content.

8.3. The designate will arrange to have the necessary content extracted from the file (i.e. specific date of lab reports, results or specific physician notes, or full file) and copied as necessary. Records will be provided to the Practitioner who treated the patient along with a clear statement about what release is requested.

8.4. The Practitioner reviews the documents for the purpose of compliance with Section 52 of PHIPA, in context of the specific content requested for release. The Practitioner completes the tracking form and identifies any concerns with release.

9. Concern for Release of Personal Health Information

9.1. When a Practitioner identifies a concern with the release of the medical file during their review, the Practitioner will meet with the Director or Manager to discuss the concerns, and whether the concerns can be addressed by having the Practitioner meet with the patient to discuss the content and context of the file before direct release. The Director or Manager will review the concerns in the context of Sections 51 and 52 of PHIPA.

9.2. The Director or manager will determine whether:

- Information will be redacted as per Section 54 of PHIPA; or
- The Practitioner will meet with the patient who has requested the file before direct release.
- FIPPA exemptions may apply to the records.

9.3. If the request was initiated by a search memo to the Health Care Unit, the Director or Manager will respond to the Chief Privacy Officer to explain the concern, and whether:

a) Information will be redacted as per Section 54 of PHIPA; or

b) The Practitioner will meet with the patient who has requested the file before direct release.

9.4.

9.5. When no concern is identified by the Practitioner, the Director or Manager will review the materials.

10. Review of Personal Health Information

10.1. The Director or Manager reviews the materials signed off by the Practitioner(s) to:

a) Confirm that all documents required to fulfill the request have been identified and signed off.

b) Confirm that all files meet note-taking standards.

c) Identify any terminology which may be unfamiliar to non-health professionals and to provide explanations for same in a covering document to be included with the file.

10.2. For requests to the Campus Health Centre, where it is determined that FIPPA exemptions do not apply, the Director signs off on the request, and provides a written summary of the records provided including an explanation of any redactions according to Section 54 of PHIPA.

10.3. For requests initiated by a formal search memo to the Health Care Units, or where FIPPA exemptions may apply, the Director or Manager will release the Records to the Chief Privacy Officer for a review and determination of any exemptions to be applied prior to releasing records to the Requester.

11. Fees for Record Search and Preparation

11.1. For requests to the Campus Health Centre, the clerk completes the "Record of Requests for Access to Personal Health Information" form and invoices for the services required to release the file, as outlined in section 10.3.

11.2. For requests to other Campus Health Units, Campus Health Unit staff complete the Records Search Form. Privacy Office Staff calculate the fees for the services required to release the file, as outlined in section 10.3.

11.3. Charges are calculated at the current suggested Ontario Medical Association rates and include photo copying, time to complete the request, and delivery charges. The invoice will be included with the records and provided to the patient or representative who has filed the request by the Ontario Tech Chief Privacy Officer or Campus Health Centre, as applicable.

12. Release of Records

12.1. For requests to the Campus Health Centre, the Campus Health Centre will keep a copy of all records released and notify the Chief Privacy Officer of the release of records relating to any patient who is a student of the University.

12.2. For requests initiated by a search memo, or where FIPPA exemptions may apply, the Privacy Office will keep a copy of all records released.

12.3. Records may be released:

a) In person if the patient comes in to physically pick up the file. The patient will be asked to show photo identification and may be asked to meet with a health professional as per section 8.2 b).

b) Through delivery by registered mail, courier or secure electronic means with signature or secure access code required by recipient named in the request for release.

13. Reporting

13.1. Each year, the Campus Health Centre will report to the University on all files of patients who are students of the University over the course of the year and will file statistical reporting with the Information and Privacy Commissioner on those releases of information.

13.2. The Privacy Office will file statistical reporting with the Information and Privacy Commissioner on requests initiated by a search memo.

MONITORING AND REVIEW

14. These Procedures will be reviewed as necessary and at least every three years. The Chief Privacy Officer, or successor thereof, is responsible to monitor and review these Procedures.

RELEVANT LEGISLATION

15. Personal Health Information Protection Act

Freedom of Information and Protection of Privacy Act

RELATED POLICIES, PROCEDURES & DOCUMENTS

16. Personal Health Information Access and Privacy Policy

Access to Information and the Protection of Privacy Policy