POLICY ON THE HANDLING OF PERSONAL HEALTH INFORMATION (DRAFT)

Definitions:

Agent: a person, with the authorization of the health information custodian (HIC), acting for or on behalf of the HIC in respect of personal health information for the purposes of the HIC, and not the agent’s own purposes, whether or not the agent has the authority to bind the HIC, whether or not the agent is employed by the HIC and whether or not the agent is being remunerated.

Collect: to gather, acquire, receive or obtain personal health information by any means from any source, and "collection" has a corresponding meaning.

Data Classification Scheme: the university's schema for classifying data and information to ensure the level of information protection and privacy is commensurate with the sensitivity and value of that data.

Directory of Records (DoR): a list of the general classes or types of records prepared by or in the custody or control of the university.

Disclose: to make personal health information available or to release it to another health information custodian or to another person, but does not include to use the personal health information, and "disclosure" has a corresponding meaning.


Health Information Custodian (HIC): a person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's duties pertaining to the provision of health care. See the appendix for a list of Queen's University’s health information custodians.
**Personal Health Information (PHI):** identifying information about an individual, in oral or recorded form, if that information relates to the physical or mental health of the individual; relates to the provision of health care to the individual.

**Personal Information (PI):** recorded information about an identifiable individual.

**Personal Information Bank (PIB):** a collection of personal information that is organized and capable of being retrieved using an individual’s name or an identifying number or particular assigned to the individual.

**PHIPA:** the *Personal Health Information Protection Act*, Statutes of Ontario 2004, chapter 3.

**Privacy Impact Assessment (PIA):** an organizational risk management tool used to identify the effects of a given process or other activity on an individual’s privacy.

**Record:** as defined in PHIPA, a record of information in any form or in any medium, whether in written, printed, photographic, electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.

**Researcher:** a person who conducts research.

**Service Provider:** any third-party entity that provides services to the university, whether for compensation or for free.

**Use:** to view, handle or otherwise deal with personal health information.

**Purpose/Reason for Policy:**

The purpose of this policy is to:

- set out the responsibilities of the university’s health information custodians regarding the proper handling of personal health information in accordance with the *Personal Health Information Protection Act* ("PHIPA"); and

- ensure that personal health information in the university’s custody or control, including personal health information that has been transferred to a Researcher, an agent, or service provider, is handled and protected appropriately.

**Scope of this Policy:**

This policy applies to all university employees (including faculty, staff, and students employed by Queen’s) when handling personal health information on behalf of Queen’s University for a health care purpose.

This policy does not apply to the handling of health care or medical information for any purpose other than a health care purpose (e.g., academic or workplace accommodations). For such collections, see the policy on Access to Information and Protection of Privacy.
Policy Statement:

Queen’s University collects and receives personal health information for the limited purposes of providing health care and supporting its research and teaching mission, and is committed to protecting the privacy of the personal health information in its custody or under its control. Accordingly, the university will collect, use, disclose, retain, store, transfer, dispose of and protect personal health information in accordance with PHIPA and the following principles:\footnote{These ten principles are drawn from the Canadian Standards Association’s \textit{Model Code for the Protection of Personal Information} and are the basis for all of Canadian privacy statutes. Queen’s University’s policy is modelled on McMaster University’s “Policy on the Handling of Personal Health Information” (June 16, 2015).}

1. Accountability for Personal Health Information

   1.1 Ultimate accountability for compliance with PHIPA rests with the university Principal and Vice-Chancellor, although other individuals within Queen’s University departments and units are responsible for the implementation of local policies, procedures and guidelines regarding the handling of personal health information in alignment with this central policy.

   1.2 The university’s Chief Privacy Officer is delegated to act on behalf of the Principal and Vice-Chancellor with respect to privacy oversight and compliance across the university.

   1.3 Each department or unit is responsible for taking reasonable steps to protect the privacy of personal health information in its custody or control.

   1.4 Each department or unit that transfers personal health information to an agent or a service provider must ensure that the personal health information is protected through contractual or other means.

   1.5 Each department and unit that handles personal health information will establish and implement local policies, procedures and guidelines as necessary in alignment with PHIPA, this policy and with the university’s central policies, procedures and guidelines.

   1.6 Department and unit local policies, procedures and guidelines will be reviewed and approved by the Chief Privacy Officer, and where applicable, by the Information Security Officer.

2. Identifying Purposes for the Collection of Personal Health Information

   2.1 Each health information custodian will identify the purposes for which personal health information is collected at or before the time of collection.

   2.2 The purpose for the collection will be conveyed to the individual by means of a written public statement.

   2.3 A written public statement shall include:
• a general description of the health information custodian’s information practices;
• a description of how to contact the health information custodian;
• information on how an individual may obtain access to or correct a record of personal health information; and
• information on how to make a complaint to the health information custodian and to the Information and Privacy Commissioner under PHIPA.

2.4 When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless law requires the new purpose, the consent of the individual is required before information can be used for that purpose.

3. Consent for the Collection, Use and Disclosure of Personal Health Information

3.1 Consent is required for the collection of personal health information and the subsequent use or disclosure of this information. Each health information custodian will seek consent for the use or disclosure of the information at the time of collection.

3.2 In certain circumstances, personal health information may be collected, used and/or disclosed without the consent of the individual. Examples are legal or security reasons that may make it impracticable to seek consent.

3.3 Each health information custodian will make a reasonable effort to ensure that the individual is notified of the purposes for which the information will be collected, used or disclosed. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be collected, used or disclosed, and must be described in a notice that is likely to come to the individual’s attention.

3.4 Consent can be express or implied. Each health information custodian can assume that an individual’s request for treatment constitutes implied consent for corresponding purposes, unless the individual explicitly states otherwise.

3.5 Consent must be express where a health information custodian discloses personal health information to a unit or department or person that is not a health information custodian, or where the disclosure is not for the purposes of providing health care.

3.6 Consent may be sought in a variety of ways, depending on the circumstances and the type of information being collected. Consent may be given verbally or in writing. Where verbal consent is provided, the exchange is to be documented.

3.7 An individual may withdraw consent at any time, subject to legal restrictions and reasonable notice. Withdrawal of the consent will not be retroactive. Each health information custodian will inform the individual of the implications of such a withdrawal.
4. **Limiting Collection of Personal Health Information**

4.1 The amount and the type of personal health information collected is limited to that which is reasonably necessary for the purposes identified by each health information custodian.

4.2 Personal health information will be collected by fair and lawful means.

5. **Limiting Use, Disclosure and Retention of Personal Health Information**

5.1 Personal health information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual, as required by law, for law enforcement, to avoid the risk of serious bodily harm to a person or group of persons, for research, or for other purposes in accordance with the requirements of PHIPA.

5.2 In cases where disclosure of personal health information to external parties is authorized, only the least amount of information appropriate for the intended purposes will be disclosed.

5.3 Personal health information will be retained only as long as necessary for the fulfillment of its purpose as documented in the university’s authorized records retention schedules.

6. **Ensuring Accuracy of Personal Health Information**

6.1 Each health information custodian will take reasonable steps to ensure the personal health information is as accurate, complete and up to date as possible.

6.2 Individuals have the right to challenge the accuracy of the information and to request correction of a record of personal health information.

7. **Ensuring Safeguards for Personal Health Information**

7.1 Personal health information in all its forms (electronic, paper, verbal, or other) will be safeguarded throughout its lifecycle (creation, collection, use, disclosure, processing, distribution, storage and disposal) through reasonable measures of protection.

7.2 The measures of protection will include physical, administrative and technical controls as determined by the university’s information security policies, procedures and standards, and/or by external regulatory agencies.

7.3 The nature of the measures of protection will vary depending on the classification and categorization of the information in accordance with the university’s data classification scheme.

7.4 Each health information custodian will make its employees and agents aware of the importance of maintaining the confidentiality of personal health information by using confidentiality agreements and by engaging in privacy education and awareness campaigns.

7.5 Each health information custodian will take care in the disposal or destruction of personal health information to prevent unauthorized access to the information, and to ensure that it is destroyed in such a way that it cannot be reconstructed or retrieved.
7.6 If personal health information is lost, stolen, or used or disclosed without authority, the responsible health information custodian will report the breach to the Chief Privacy Officer as soon as possible and work cooperatively with the Chief Privacy Officer to respond as required by the legislation and regulatory agencies.

8. **Openness about Personal Health Information and Practices**

8.1 Queen’s University will make information about its privacy policies and practices readily available in a form that is generally understandable.

8.2 Queen’s University will make information on its policies and practices for the handling of personal health information available in a variety of other ways including through public websites.

8.3 Records of personal health information will be included in the university’s directory of records and, where appropriate, in its index of personal information banks.

9. **Individual Access to Own Personal Health Information**

9.1 Individuals have the right to access their own personal health information.

9.2 Health information custodians may provide access to individuals seeking their own personal health information on an informal basis in accordance with local procedures.

9.3 Individuals seeking formal access to their own personal health information will make such a request to the university’s central privacy office for processing in accordance with PHIPA and/or FIPPA.

9.4 Individuals seeking to formally correct their own record of personal health information will make such a request to the university’s central privacy office for processing in accordance with PHIPA and/or FIPPA.

10. **Challenging Compliance with Queen’s University Privacy Policies and Practices**

10.1 An individual is able to challenge compliance with the above standards by contacting the Chief Privacy Officer at Queen’s University.

10.2 The university’s Chief Privacy Officer will investigate any complaints. If the complaint is judged to be valid, the university will take appropriate measures, including, if necessary, amending the policies and procedures.

**Responsibilities:**

The Chief Privacy Officer will:

- develop policies, procedures and guidelines and other user-friendly tools to support implementation of this policy;

- work cooperatively with the Information Security Officer to develop IT security standards for personal health information;
• review for approval all local policies, procedures and guidelines for alignment with this policy and central policies, procedures and guidelines;

• provide training and advisory services to employees of the university so that the policy and procedures are understood and applied;

• maintain a network of appropriate contacts across university departments and units for the purpose of information-sharing, feedback, and continuous program improvement; and

• where, in the opinion of the Chief Privacy Officer, the collection of records containing personal health information creates significant risks of privacy invasion, require the appropriate department or unit to conduct a privacy impact assessment concerning that collection.

Health information custodians will:

• develop, document and publish local policies, procedures and guidelines as appropriate in alignment with this policy and central policies, procedures and guidelines, including IT security standards;

• take reasonable measures to ensure that records containing personal health information collected or received in accordance with this policy are protected from unauthorized access or modification, and inappropriate use or disclosure, whether intentional or unintentional;

• report privacy breaches of personal health information to the Chief Privacy Officer as soon as possible;

• report security breaches relating to personal health information to the Information Security Officer;

• conduct a privacy impact assessment as directed by the Chief Privacy Officer;

• ensure employees in their department or unit are aware of this policy and appropriately trained; and

• ensure all other individuals who are engaged by, or work with, their department or unit are aware of the requirements of this policy and appropriately trained.

All university employees (including faculty, staff, and students employed by Queen’s) and any other individuals who handle personal health information on behalf of the university will:

• ensure that personal health information which has come into their custody or control in accordance with this policy is handled according to this policy and the Queen’s University data classification scheme;

• consult, as needed, the Chief Privacy Officer about the collection, use, disclosure, retention, transfer and disposal of personal health information;
• consult, as needed, the Information Security Officer about IT security standards for personal health information;

• cooperate with the Chief Privacy Officer, when required, in fulfilling formal access requests;

• report privacy breaches to their supervisor and the Chief Privacy Officer as soon as possible;

• report security breaches to their supervisor and the Information Security Officer as soon as possible; and

• comply with this policy and any procedures issued in accordance with it.

<table>
<thead>
<tr>
<th>Contact Officer</th>
<th>Chief Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date for Next Review</td>
<td>2022/02/01</td>
</tr>
</tbody>
</table>

|---------------------------------------------|----------------------------------------------------------|---------------------------|-------------------------------------------|

<table>
<thead>
<tr>
<th>Policies Superseded by This Policy</th>
<th></th>
<th></th>
</tr>
</thead>
</table>

## Appendix: Queen’s University Health Information Custodians

<table>
<thead>
<tr>
<th>Health Information Custodian</th>
<th>Operational Authority for Compliance with this Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Department of Family Medicine</strong></td>
<td>Clinic Manager</td>
</tr>
<tr>
<td>School of Medicine</td>
<td></td>
</tr>
<tr>
<td>Faculty of Health Sciences</td>
<td></td>
</tr>
<tr>
<td><strong>The Physical Therapy Clinic at Queen’s</strong></td>
<td>Clinic Manager</td>
</tr>
<tr>
<td>School of Rehabilitation Therapy</td>
<td></td>
</tr>
<tr>
<td>Faculty of Health Sciences</td>
<td></td>
</tr>
<tr>
<td><strong>Psychology Clinic at Queen’s University</strong></td>
<td>Clinic Director</td>
</tr>
<tr>
<td>Department of Psychology</td>
<td></td>
</tr>
<tr>
<td>Faculty of Arts and Science</td>
<td></td>
</tr>
<tr>
<td><strong>Student Wellness Services</strong></td>
<td>Executive Director</td>
</tr>
<tr>
<td>• Health Services</td>
<td></td>
</tr>
<tr>
<td>• Counselling Services</td>
<td></td>
</tr>
<tr>
<td>Division of Student Affairs</td>
<td></td>
</tr>
<tr>
<td><strong>Regional Assessment and Resource Centre</strong></td>
<td>Clinical Director</td>
</tr>
<tr>
<td>Division of Student Affairs</td>
<td></td>
</tr>
<tr>
<td><strong>Athletic Therapy Services</strong></td>
<td>Coordinator</td>
</tr>
<tr>
<td>Athletics and Recreation</td>
<td></td>
</tr>
<tr>
<td>Division of Student Affairs</td>
<td></td>
</tr>
</tbody>
</table>