Carleton UNIVERSITY
Canada's Capital University

Policy Name	Personal Health Information Processing (PHIP)
Originating/Responsible Department	Office of the General Counsel
Approval Authority	Senior Management Committee
Date of Original Policy	January 2013
Last Updated	September 2019
Mandatory Revision Date	September 2024
Contact	Manager, Privacy & Access to Information

Purpose

The purpose of this Policy is to ensure that Personal Health Information (PHI) in the University's custody or control is collected, used and disclosed in accordance with the relevant legislation. Carleton is committed to protecting the privacy, confidentiality and security of all PHI that has been entrusted to us. Carleton provides this protection, in part, by complying with Ontario's *Personal Health Information Protection Act* (PHIPA), enacted on November 1, 2004. PHIPA establishes rules concerning the collection, use and disclosure of PHI.

Scope

This Policy applies to all Carleton University faculty, staff and students processing PHI on behalf of the institution.

Definitions

The terms noted below will appear throughout this policy and based on legal definitions under sections 2, 3 and 4 of *PHIPA*:

> **"Agent"**, in relation to a health information custodian (HIC), means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.
>
> **"Collect"**, in relation to personal health information, means to gather, acquire, receive or obtain the information by any means from any source, and "collection" has a corresponding meaning.
>
> **"Disclose"**, in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning.
>
> **"Health Information Custodian, or HIC"** as defined in PHIPA s.3, is 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.

"Identifying information," means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual**.**

"Personal health information, or PHI" subject to certain exceptions, means identifying information about an individual in oral or recorded form, if the information,

a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
c) is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
f) is the individual's health number, or
g) identifies an individual's substitute decision-maker.

"**Record"** means a record of information in any form or medium, whether written, printed, photographic, digital imaging, electronic form or otherwise. It does not include computer programs or other mechanisms that produce records.

"Use" in relation to personal health information in the custody or under the control of a health information custodian or a person, means to view, handle or otherwise deal with the information, but does not include to disclose the information, and "use", as a noun, has a corresponding meaning.

Principles

The following principles apply to the processing of PHI within the custody and control of Carleton.

1. Accountability for Personal Health Information

Ultimate accountability for compliance with privacy principles rests with the President, although other individuals within Carleton are responsible for the day-to-day collection and processing of personal health information.

Carleton's General Counsel is delegated to act on behalf of the President with respect to the oversight and compliance of privacy across the University. Each business unit is responsible to protect the privacy of patient/client health information in its custody or control. PHI transferred to an agent of Carleton must be protected using contractual or other means.

Carleton has implemented procedures and guidelines to give effect to this Policy and the principle of accountability.

2. Identifying Purposes for the Collection of Personal Health Information

Each business unit will identify the purposes for which PHI is collected at or before the time of collection. The purpose is conveyed to the client/patient by means of a Statement of Information,

poster, brochure, public web site or by direct contact with the Carleton University's Privacy Office (the Privacy Office) or Health and Counselling Services.

Primarily, PHI is collected for the purpose of delivery of direct client care, the administration of the health care system, research, teaching, statistics, and the meeting of legal and regulatory requirements as described in PHIPA. When PHI 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 client/patient is required before information can be used for that purpose.

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

Consent is required for the collection of PHI and the subsequent use or disclosure of this information. Each business unit will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances PHI 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.

Each business unit will make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. In obtaining consent, the reasonable expectations of the individual are also relevant. Each business unit can assume that an individual's request for treatment constitutes consent for specific purposes, unless the client explicitly states otherwise.

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 a verbal consent is provided, this exchange is to be documented. A client/patient may withdraw consent at any time, subject to legal restrictions and reasonable notice. Withdrawal of the consent will not have a retroactive effect. Each business unit will inform the individual of the implications of such a withdrawal. Further information on the withdrawal of consent is provided later in the Policy.

4. Limiting Collection of Personal Health Information

The amount and the type of PHI collected is limited to that which is necessary for the purposes identified by each business unit. PHI will be collected by fair and lawful means.

5. Limiting use Disclosure and Retention of Personal Health Information

PHI will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the client or as required by law. In cases where disclosure/release of information to external sources is authorised, the least amount of information appropriate for the intended purposes is disclosed. PHI is retained only as long as necessary for the fulfillment of its purpose.

6. Ensuring accuracy of Personal Health Information

Each business unit will take practical steps to ensure the PHI is as accurate, complete and up to date as possible and necessary to minimise the possibility that inappropriate information may be used to make clinical decisions about the client/patient. Clients/patients have the right to challenge the accuracy of the information.

7. Ensuring safeguards for Personal Health Information

Carleton is committed to the protection of client/patient PHI in all its forms (electronic, paper, verbal, or other) throughout its life cycle (creation, use, distribution, storage and disposal) for authorised access, modification, destruction or disclosure. The nature of safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage.

The methods of protection will include:

- Physical measures – locked filing cabinets and restricted access to offices;
- Administrative measures – confidentiality agreements;
- Technological measures – passwords, secure computer networks and audits.

Carleton makes its employees aware of the importance of maintaining the confidentiality of PHI by using confidentiality agreements, by providing privacy education and privacy awareness campaigns.

Carleton makes its employees aware of their records management obligations towards PHI records in order to prevent unauthorized access to the information; from creation, retention, and final disposal (archival deposit or secure destruction).

8. Openness about Personal Health Information and Practices

Carleton makes information about its privacy policy practices readily available in a form that is generally understandable.

Carleton's privacy policies makes available the following information:

- Provides a general description of University information practices
- Describes how to contact the Privacy Office
- Describes how an individual may obtain access to and/or make a correction request for a record of PHI
- Describes how a client/patient may file a complaint with the Privacy Office or with the Information and Privacy Commissioner of Ontario.

Carleton may make information on its policies and practices for the processing of PHI available in a variety of other ways, including brochures or through public web sites.

9. Individual Access to own Personal Health Information

Carleton supports the right of clients/patients to access their PHI as per legislation.

- Individuals wishing to access their PHI or Personal Information held by Health and Counselling Services please contact Health and Counselling Services at 613-520-6674**.**

- Individuals wishing to access their PHI or Personal Information held by any other business unit please contact the Privacy Office at 613-520-2600, extension 2047.

10. Challenging compliance with University Privacy Policies and Practices

A client/patient or substitute decision maker is able to challenge compliance with the above standards by contacting the Privacy Office. The University has procedures in place to receive and respond to complaints and/or inquiries about the policies and practices relating to the privacy and

security of PHI. The Privacy Office will investigate the complaints. If the complaint is judged to be valid, the University will take appropriate measures, including, if necessary, amending the policies and procedures.

If you are not satisfied with the outcome of our investigations, or if you would like to challenge our compliance with applicable legislation, please contact the Information and Privacy Commissioner of Ontario at 1 (800)-387-0073*.*

Withdrawal of Consent

Section 20(2) of PHIPA makes it clear that individuals may withhold or withdraw their consent to the collection, use or disclosure of their PHI by Health Information Custodians for the purposes of providing or assisting in providing health care. Further, under PHIPA, individuals may provide express instructions to health information custodians not to use or disclose their personal health information for health care purposes without consent in the circumstances set out in sections 37(1) (a), 38(1)(a) and 50(1)(e) of PHIPA.

These provisions have come to be referred to as the "lock-box" provisions, although lock-box is not a defined term in PHIPA. The withholding or withdrawal of consent or the express instructions cited above may take various forms, including communications from individuals to health information custodians:

- not to collect, use or disclose a particular item of information contained in their record of PHI (for example, a particular diagnosis);
- not to collect, use or disclose the contents of their entire record of PHI;
- not to disclose their PHI to a particular Health Information Custodian, a particular agent of a Health Information Custodian or a class of Health Information Custodians or agents (e.g. physicians, nurses or social workers); or
- not to enable a particular Health Information Custodian, a particular agent of a Health Information Custodian or a class of Health Information Custodians or agents (e.g. physicians, nurses or social workers) to use their PHI.

Although it is up to the individual to whom the information relates to decide what PHI to lock, if any, and to whom the lock should apply, a Health Information Custodian may discuss with the individual how locking PHI might affect the individual's health care and why a Health Information Custodian may need more PHI to provide the best possible care. Withholding or withdrawal of consent, or the express instructions cited above, will be processed by the receiving Health Information Custodian.

Notification and Reporting

Business units must take steps that are reasonable in the circumstances to ensure that PHI in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

Employees, volunteers, students, medical staff and contract workers, researchers, agents, or sub-contractors must report suspected or known breaches of privacy, confidentiality and security to the Manager, Privacy & Access to Information as outlined in the University's Privacy Breach Incident Plan.

Compliance

Violations of this Policy may result in disciplinary action.

Contacts

For questions related to PHI in Health and Counselling Services, please contact the Director, Health and Counselling Services at 613-520-6674**.**

For questions related to PHI in all other business units, or for questions related to the administration of this statement, please contact the Privacy Office by phone at 613-520-2600 extension 2047 or by e-mail at university_privacy_office@carleton.ca.

Related Legislation

- *Freedom of Information and Protection of Privacy Act*
- *Personal Health Information Protection Act*, 2004

Related Policies:

- Corporate Records and Archives Policy
- Data and Information Classification and Protection
- FIPPA Policies
- Information Security Incident Response
- Information Technology (IT) Security
- Mobile Technology Security
- Password Policy for Information Systems