McMaster University

Policies, Procedures and Guidelines

Complete Policy Title: **Policy for the Handling of Personal Health Information**	Policy Number (if applicable):
Approved by: **President**	Date of Most Recent Approval:
Date of Original Approval(s): **June 16, 2015**	Supersedes/Amends Policy dated:
Responsible Executive: **University Privacy Officer**	Enquiries: **University Secretariat**

DISCLAIMER: *If there is a Discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails*

Scope and Purpose

This Policy applies to all McMaster University faculty, staff and students when handling personal health information on behalf of the institution.

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

At McMaster University, Personal Health Information is to be collected, used and disclosed in accordance with the following principles:

Principle I - Accountability for Personal Health Information

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

The University's Privacy Officer is delegated to act on behalf of the University 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. Personal health information that has been transferred to an agent of McMaster University must be protected through the use of contractual or other means.

McMaster University has implemented policies and guidelines to give effect to this Policy and the principle of accountability.

Principle II - Identifying Purposes for the Collection of Personal Health Information

Each business unit will identify the purposes for which personal health information 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 McMaster University's Privacy Officer.

Primarily, personal health information 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 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 client/patient is required before information can be used for that purpose.

Principle III - Consent for the Collection Use and Disclosure of Personal Health Information

Consent is required for the collection of personal health information 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 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.

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 the 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.

Principle IV - Limiting Collection of Personal Health Information

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

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

Principle V – Limiting use Disclosure and Retention of Personal Health Information

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 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.

Personal health information is retained only as long as necessary for the fulfillment of its purpose.

Principle VI – Ensuring accuracy of personal health information

Each business unit will take practical steps to ensure the personal health information 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.

Principle VII – Ensuring safeguards for personal health information

McMaster University is committed to the protection of client/patient personal health information in all its forms (electronic, paper, verbal, or other) throughout its life cycle (origination, entry, processing, 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;
- Organisational measures – confidentiality agreements;
- Technological measures – passwords, secure computer networks and audits.

McMaster University makes its employees aware of the importance of maintaining the confidentiality of personal health information by using confidentiality agreements, by providing privacy education and privacy awareness campaigns.

Care will be taken in the disposal or destruction of personal health information to prevent unauthorised access to the information.

Principle VIII – Openness about Personal Health Information and Practices

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

McMaster's Statement of Information Practices makes available the following information:

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

McMaster University may make information on its policies and practices for the handling of personal health information available in a variety of other ways, including brochures or through public web sites.

Principle IX – Individual Access to own Personal Health Information

McMaster University supports the right of clients/patients to access their personal health information as per legislation (See Access Policy for further information).

Principle XI – Challenging compliance with McMaster 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 Officer at McMaster University. 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 personal health information. The McMaster University's Privacy Officer 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.

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 personal health information 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 personal health information (for example, a particular diagnosis);

- not to collect, use or disclose the contents of their entire record of personal health information;

- not to disclose their personal health information 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 personal health information.

Although it is up to the individual to whom the information relates to decide what personal health information to lock, if any, and to whom the lock should apply, a Health Information Custodian may discuss with the individual how locking personal health information might affect the individual's health care and why a Health Information Custodian may need more personal health information 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 according to the *McMaster Lock-box Protocol*, available on the Privacy Office website.

Policy Breach

A Health Information Custodian is to take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorised use or disclosure and to ensure that the records containing the information are protected against unauthorised copying, modification or disposal.

A Health Information Custodian that has custody or control of personal health information about an individual is to notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorised persons.

An agent of a Health Information Custodian is to notify the custodian at the first reasonable opportunity if personal health information handled by the agent on behalf of the custodian is stolen, lost or accessed by unauthorised persons.

If the Health Information Custodian uses or discloses personal health information about an individual without the individual's consent the custodian is to:

inform the individual of the uses and disclosures at the first reasonable opportunity, unless, the individual does not have a right of access to a record of the information.

If the Health Information Custodian is a researcher who has received the personal health information from another health care custodian, the researcher is not to notify the individual that the information is lost, stolen or accessed by unauthorised persons unless the Health Information Custodian first obtains the individual's consent to having the researcher contact the individual and informs the researcher that the individual has given the consent.

Procedure Breach

Employees, volunteers, students, medical staff and contract workers, researchers, agents, or sub-contractors are to report suspected or known breaches of privacy, confidentiality and security to the McMaster University's Privacy Officer or to the Faculty of Health Sciences Chief Operating Officer as outlined in the University's Privacy Breach Protocol.

Definitions

PHI – Personal Health Information is defined in PHIPA s.4 as identifying information about an individual in either oral or recorded form that relates to the physical or mental health of the individual; relates to the provision of healthcare to the individual, including the identification of a provider of healthcare to the individual;

PHIPA – *Personal Health Information Protection Act* - means the 2004 SO Ontario Act and the regulations made there under;

HIC – Health Information Custodian as defined in PHIPA s.3 is a person or organisation who has custody or control of personal health information as a result of or in connection with performing the person's or organisation's duties;

Agent – in relation to a Health Information Custodian, means a person who, with the authorisation 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;

Record - means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record;

Use - as defined in PHIPA s.2, in relation to personal health information in the custody or under the control of Health Information Custodian or a person, means to handle or deal with the information.

Related Documents:

Policy on Access to Personal Health Information
Policy on Correction of Personal Health Information
Privacy Breach Protocol
Electronic Mail Protocol for Personal Information and Personal Health Information
Portable Storage Device Policy
McMaster Lock-box Protocol
Guideline for Verifying Identity
Guideline on Withdrawal of Consent
McMaster Statement of Information Practices