Policies, Procedures and Guidelines

Complete Policy Title: **Privacy Governance and Accountability Framework**	Policy Number (if applicable):
Approved by: **President**	Date of Most Recent Approval:
Date of Original Approval(s): **June 16, 2015**	Supersedes/Amends Policy dated:
The purpose of this 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 information or personal health information on behalf of the institution.

The purpose of this Policy is to set out the accountabilities for ensuring that all individuals involved in the planning, management and day-to-day operations of McMaster University are in compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), RSO, 1990 and with the *Personal Health Information Protection Act* (PHIPA), SO, 2004, their associated regulations and the privacy policies, procedures and practices set out by McMaster University.

The accountability for ensuring that entities and individuals associated with McMaster University comply with FIPPA and PHIPA, and all relevant regulations, policies, procedures, and guidelines is distributed as follows:

Entity	Overarching Accountability	Accountabilities	Day-to-Day Authorisation
McMaster University	President	Ensure that personal information in the University's custody or control is collected, used and disclosed in accordance with FIPPA and/or PHIPA and with University policy. Ensure that relevant information and training is provided to all faculty, staff and students. Ensure that McMaster University prepares an annual privacy report in respect of the University's operations. Ensure that McMaster University, in any agreement with a vendor in respect of Personal Information (PI) or Personal Health Information (PHI), includes provision to require the vendor to comply with the relevant legislation, regulations and policies, procedures and practices in respect of FIPPA and/or PHIPA.	Privacy Officer
Faculty of Health Sciences	Dean and Vice President, Faculty of Health Sciences	Ensure that McMaster University employees, contracted workers, volunteers, students and vendors in the Faculty of Health Sciences who have access to PHI in the course of their work, comply with PHIPA and with relevant policies, procedures, and practices of the University. Ensure in written agreements with affiliated organizations that their agents similarly comply with relevant legislation and policies, procedures and practices of the University.	Chief Operating Officer

Roles and responsibilities of individuals with delegated day-to-day authorisation to manage the privacy requirements of FIPPA and PHIPA in specific sectors of the University are outlined below:

Entity	Day-to-Day Authority	Roles and Responsibilities
McMaster University	Privacy Officer	To provide McMaster University with guidance and direction on privacy issues; review and provide input into privacy related policies and procedures for FIPPA and PHIPA; review privacy educational material and provide assistance with privacy training for faculty, staff and students as required; make privacy information and practices available to the public by keeping website and other communication materials up to date and accessible; lead the development of privacy training and education for University staff and agents with access to PI and/or PHI; facilitate initial and ongoing training for staff and agents; respond to privacy inquiries; lead breach management response, liaise with the Information and Privacy Commission on the adjudication of appeals.
Faculty of Health Sciences	Chief Operating Officer	To ensure compliance with University privacy policies within the Faculty of Health Sciences, specifically with respect to the requirements of PHIPA; to ensure agreements for PHI are in place with all organizations, vendors, or other agents that have been granted access to PHI.
Maternity Centre of Hamilton	Clinic Director, Maternity Centre of Hamilton	To ensure compliance with University privacy policies, specifically in relation to the requirements of PHIPA; to ensure agreements for PHI are in place with all organisations, vendors, or other agents that have been granted access to PHI.
David Braley Sports Medicine Clinic	Clinic Director, David Braley Sports Medicine Clinic	To ensure compliance with University privacy policies, specifically in relation to the requirements of PHIPA; to ensure agreements for PHI are in place with all organisations, vendors, or other agents that have been granted access to PHI.

Student Wellness Centre	Clinic Director, Student Wellness Centre	To ensure compliance with University privacy policies, specifically in relation to the requirements of PHIPA; to ensure agreements for PHI are in place with all organizations, vendors, or other agents that have been granted access to PHI.
Physical Activity Centre of Excellence (PACE)	Director, Physical Activity Centre of Excellence	To ensure compliance with University privacy policies specifically in relation to the requirements of PHIPA; to ensure agreements for PHI are in place with all organizations, vendors, or other agents that have been granted access to PHI.

Related Documents:

Policy for Handling of Personal Health Information
Policy for Handling of Personal Information
Policy on Access to Personal Health Information
Policy on Correction of Personal Health Information
Background Check Policy
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

Collection of Personal Information

Personal information collection must comply with the *McMaster University Statement on Collection of Personal Information and Protection of Privacy (NOC)*. In addition, personal information collection must comply with the following:

- The information collected must be necessary to fulfill a legitimate University activity;
- The information collected must be the minimum amount necessary for the purpose;
- The information must be collected directly from the individual or if indirectly, with the clear knowledge and authority of the individual;
- The owner of the information must be advised (through a notice) as to the authority for the collection, the main purposes for the collection and whom to contact if there are any questions about the collection. If the information is collected on a form, this notice should be on the form or provided as a link;
- Personal information collections that do not comply with this Policy must be brought to the attention of the university's Privacy Officer.

Use or Disclosure of Personal Information

Personal information use and disclosure must comply with the. *Freedom of Information and Protection of Privacy Act* (FIPPA) and with University policy. In addition, personal information use and disclosure must comply with the following:

- Personal information should be used and/or disclosed only for the purpose for which it was collected, for established university functions, or with consent of the individual;
- Personal information should only be used and/or disclosed within the University to officers, employees and third parties who need the information to carry out their duties and if the disclosure is necessary and proper in the discharge of the University's functions;
- Personal information should not be disclosed outside of the University without clear legal authority or the permission of the owner to do so;
- When uncertain whether a use or disclosure of personal information is permitted, contact the University Privacy Office.

Safeguarding Personal Information

McMaster University is committed to the protection of personal 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, disclosure, or destruction.

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 – locking 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 information by using confidentiality agreements and by providing privacy education and privacy awareness campaigns.

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

Definitions

Collection means actively or passively acquiring, gathering or receiving personal information either directly or through a third party.

Consistent Purpose means one which is reasonably compatible or "consistent" with the original purpose of the collection as stated in the University's NOC or in the notice of collection provided at time of collection.

Disclosure means allowing access to personal information to others beyond the original collector for purposes that are consistent with the stated collection purpose or with permission of the individual or to comply with a law.

Employees means faculty, staff and students with official University records functions.

Informational (data) privacy means that an individual is the ultimate owner of his or her personal information and that the collection, use and disclosure of an individual's personal information should remain under the control of that individual to the greatest extent possible. Control implies knowledge of the purpose of the collection and either informed consent by the information owner for the collection or a legal authority for the collecting organization to collect.

Legal Authority means that the University has the right to collect the personal information under laws such as the *McMaster University Act* (1976); its related by-laws, rules, regulations and resolutions or other statutes granting powers to the University.

Notice of Collection (NOC) means the formal notice required by law to be given when personal information is collected. This notice consists of three items: 1) the legal authority for collection; 2) The purpose(s) of the collection and 3) contact information for someone who can answer questions about the collection.

Personal Information means any recorded information about an identifiable individual as defined by section 2 of the Freedom of Information and Protection of Privacy Act (FIPPA) which may also include personal health information defined in the Personal Health Information Protection Act (PHIPA). The information may relate to the identifiable individual either directly or indirectly. Under FIPPA, personal information must be kept for at least 1 year after last use unless permission for destruction has been granted by the individual to whom the information relates, or by the University Privacy Officer.

Third parties means outside groups such as contractors or authorized visitors.

Use means the active utilization of personal information to fulfill a legitimate University activity consistent with the law or stated collection purposes.

Related Documents:

Background Check Policy
Privacy Breach Protocol
Electronic Mail Protocol for Personal Information and Personal Health Information
Portable Storage Device Policy
Guideline for Verifying Identity
McMaster Statement of Information Practices

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, 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

Policies, Procedures and Guidelines

Complete Policy Title: **Privacy Breach Protocol**	Policy Number (if applicable):
Approved by: **President**	Date of Most Recent Approval:
Date of Original Approval(s): **June, 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*

Purpose

Under the *Freedom of Information and Protection of Privacy Act* (FIPPA) or *Personal Health Information Protection Act* (PHIPA), McMaster University has a responsibility to ensure that the personal information in its custody or control is properly safeguarded from those not entitled to have access.

What is a Privacy Breach?

A privacy breach is an incident involving unauthorised access to personal information (PI) or personal health information (PHI) in the custody or under the control of the University. The information can be either recorded or verbal.

Examples of unauthorised access:

- PI/PHI collected in error;
- PI/PHI used for a purpose not consistent with the original collection (e.g. given to someone else for some purpose other than those originally stated);
- lost or misplaced PI/PHI;
- stolen or lost laptops, data drives or disks containing unencrypted PI/PHI;
- accidental disclosure of PI/PHI to an unauthorised person or group (e.g. e-mailing information to the wrong person, loss of unencrypted devices containing PI/PHI);
- deliberate disclosure of PI/PHI to an unauthorised person or group (for fraudulent or other purposes);
- deliberate access of PI/PHI by an unauthorised person or group (for fraudulent or other purposes);
- PI/PHI is copied, modified or disposed of in an unauthorised manner;
- contravention of the privacy policies, procedures or practices of McMaster University;
- contravention of the privacy policies, procedures or practices or of the privacy provisions of any agreements pertaining to the Provincial Electronic Health Record.

What Should I do if a Privacy Breach Occurs?

Except in the Faculty of Health Sciences, when you discover or suspect a breach of personal information or personal health information has occurred, immediately inform the University Privacy Officer to determine how to proceed.

In the Faculty of Health Sciences, when you discover or suspect that a breach of personal health information has occurred, immediately inform the Chief Operating Officer of the Faculty to determine how to proceed.

Assess and Record

You can help by identifying and recording to the extent possible, the following information:

- How did you discover the incident?
- When did you discover the incident and when did it likely occur?
- Where did you discover the incident?
- What happened?
    - is it likely a one-time or on-going occurrence;
    - who is affected;
    - what is the scope of the breach (internal/external);
    - the number of individuals affected;
    - what type of information is involved (identify all specific data types);
    - what format such as email, laptop, hard copy is involved; and
    - any suspicion of criminal activity.

Next Steps

The Privacy Officer will work together with University officials in the areas affected to:

Contain

- Stop the breach or minimise it as far as possible

Inform

- Contact all relevant units to ensure they are appropriately informed (eg. UTS, Security).

Notify

- Alert the persons whose information has been affected whenever it is possible.

Prevent

- A privacy breach should result in a review of current privacy practices to determine whether changes should be made to reduce the risk of a future occurrence.

Additional information on the handling of a privacy breach is available on the University's Privacy website.

McMaster University

Policies, Procedures and Guidelines

Complete Policy Title:
Electronic Mail (E-mail) Protocol for Personal Information and Personal Health Information

Policy Number (if applicable):

Approved by:
President

Date of Most Recent Approval:

Date of Original Approval(s):
June 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*

Purpose

To identify the standards, responsibilities and processes that apply in the use of e-mail accounts for transmission of Personal Information (PI) and Personal Health Information (PHI).

Policy

General principles

The McMaster University e-mail systems are to be used by authorized users to transmit business information. In some circumstances, confidential PI/PHI may be transmitted by email if appropriate safeguards are undertaken.

Standards and Expectations

All McMaster University e-mail users are expected to use e-mail in a responsible and informed way in keeping with University policies related to confidentiality and work ethics (see *Policy on Electronic Communications*).

Each user has an obligation to be aware of computer security and privacy concerns, and guard against viruses. E-mail is not encrypted, and as such, does not provide a secure platform for transfer of confidential data (e.g. student information, personal information, health information).

The sender of the e-mail is responsible for disclosure of all content contained as part of the e-mail. It is advisable to start a new e-mail discussion with a new subject line when the subject matter in an e-mail thread changes.

Care is to be taken in addressing e-mail messages to ensure they are not inadvertently sent to outsiders or to the wrong internal user.

NOTE*: When using McMaster University distribution lists, the user should ensure that all addressees included are appropriate recipients of the information.*

Confidential personal health information or personal information includes patient/client care information, information regarding an individual's identity, treatment and diagnosis, personal information regarding individuals' salaries, benefits, performance reviews, health records, personnel records, disciplinary action, management plan including financial records, citizenship, academic record, grades, accommodations in place, etc.

Confidential personal information should not be sent over the internal e-mail system i.e. from one McMaster University account to another, within the body of an e-mail message, but may be attached to the message in a password-protected or encrypted file. Information regarding the password or encryption key must be communicated separately (either in a separate e-mail or by telephone or text message) and should never be included in the same e-mail message as the file.

Similarly, PI/PHI sent to an external recipient(s) must be de-identified, encrypted, or password-protected.

Exceptions:

- An authorized healthcare provider or designate may communicate with an individual through e-mail to support that individual's care if specific conditions are met, and consent is obtained (see *Guideline on Obtaining Consent re Personal Health Information to be Transmitted via E-mail*). Students may receive confidential communications via e-mail if they have been informed of the inherent risks and have consented in writing (see *Guideline on Obtaining Consent re Personal Information to be Transmitted via E-mail*).

Inappropriate use of e-mail can result in penalties that range from having e-mail privileges revoked to formal disciplinary action up to and including termination of employment as per the Code of Conduct set out in the *McMaster Computers and Networks Policy*.

Related Documents:

Policy for Handling of Personal Health Information
Policy for Handling of Personal Information
Portable Storage Device Policy
McMaster Computers and Networks Policy
Policy on Electronic Communications
Guideline on Obtaining Consent re Personal Health Information to be Transmitted via E-mail Guideline on Obtaining Consent re Personal Information to be Transmitted via E-mail

McMaster University

Policies, Procedures and Guidelines

Complete Policy Title: **Portable Storage Device Policy**	Policy Number (if applicable):
Approved by: **President**	Date of Most Recent Approval:
Date of Original Approval(s): **June 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*

Purpose

The purpose of this Policy is to ensure that personal information, personal health information and other sensitive information in the University's custody or control is properly safeguarded from those not entitled to have access as well as protecting University systems from the introduction of malicious software. Information contained on portable storage devices (PSD) is subject to the same policies and laws as other University information. However, because of their size and portability they are easily lost or stolen and therefore present increased privacy and security risks when sensitive or personal information is stored on the device.

Security of Personal Information (PI) and Personal Health Information (PHI)
Personal information and personal health information are both classified as "Confidential" under the UTS *Information Classification Matrix Policy Statement*.

All University employees must ensure that PI/PHI in the University's custody or control is protected against theft, loss and unauthorised use or disclosure and ensure that the records containing the information are protected against unauthorised copying, modification or disposal.

Minimum guidelines when using a mobile device.

- PI/PHI should not be stored on mobile devices. However, in the event that there is no alternative to local storage, all such information must be encrypted using approved encryption techniques and/or password protected.
- PI/PHI must not be transmitted via wireless communication to or from a mobile device unless approved wireless transmission protocols along with approved encryption techniques are utilised.
- All remote access to McMaster University information resources must use an approved communication mechanism.

- All mobile devices must have approved virus and spy ware detection/protection software along with personal firewall protection (where applicable).

User Responsibilities and Procedures

Password-protect your Mobile Device:
Physical security is a major concern for mobile devices, which tend to be small and easily lost or misplaced. If your mobile device is lost or stolen, a device password may be all that stands in the way of someone reading your E-mail or PI/PHI of another individual(s).

- Choose a strong password. Strong login passwords are comprised of at least eight characters with 14 or more being ideal. These should include a combination of upper and lower case letters, numbers and symbols. DO Not use passwords that are predictable i.e. Birthday.

Verify Encryption Mechanisms:

Any PI/PHI must be encrypted**.** On its own, password protection is not sufficient should the mobile device become lost or stolen.

Protect your passwords and encryption key by:

- Not writing them down or storing them on the device
- Not using the same password to log into your computer and to unlock encrypted files.

Enable Auto Lock Feature:
Enable the automatic lock feature of your device after five minutes or less of idle time.

Use Antivirus Software:
If you have PI/PHI on your mobile device then at a minimum you should have personal firewall, anti-virus and anti-spyware programs that are up-to-date with the latest security patches.

Storage:
Portable storage devices should be used for the temporary storage of information only and must not be used as permanent document repositories to store University information. Confidential data or personal information contained on portable storage devices may only be a copy of data stored on a secure University system.

Data Erasure and Disposal of PSDs:
Confidential and personal data held on PSDs must be erased sufficiently to prevent information recovery using tools normally available on the university system. Simple deletion or erasure of the files or reformatting does not clear the portable storage device, because commands such as undelete or un-format may permit the recovery of the information. Contact University Technology Services for additional information

Promptly Report a Lost or Stolen Device:
If your mobile device has been lost or stolen promptly report this to the McMaster University Security Services. Additionally, advise the Privacy Officer if the device has any PI/PHI on it.

Storage Case:
Ensure that the case does not bear any visible identification of the University. Include an "if found, return by calling [phone number]" card inside the case with no other identifying information.

Related Documents:

Policy for Handling of Personal Health Information
Policy for Handling of Personal Information
UTS Information Classification Matrix Policy Statement
Information and Privacy Commission – Fact Sheet on Health-Care Requirement for Strong Encryption
Information Privacy Commissioner - Safeguarding Privacy in a Mobile Workplace
Privacy Breach Protocol

McMaster University

Policies, Procedures and Guidelines

Complete Policy Title: **Policy on Access to Personal Health Information**	Policy Number (if applicable):
Approved by: **President**	Date of Most Recent Approval:
Date of Original Approval(s): **June, 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*

Policy

A client/patient has a right of access to a record of personal health information about themselves that is in the custody or under the control of McMaster University.

The right of access does not extend to the following types of health records:

- The record or its contents are subject to a legal privilege;
- Another Act or court order prevents the access;
- The information was collected or created in anticipation of a proceeding;
- The information was collected or created in the course of an inspection, investigation or authorised by law;
- Granting access would result in a risk of serious harm to the treatment or recovery of the individual or another person.

Role of Substitute Decision-Maker

A substitute decision-maker may request access on a client's/patient's behalf as the right of access exists whether or not a client/patient has capacity. Substitute decision-makers will follow the same process to obtain access to the personal health records as the client/patient.

Request for Access

Requests for access are to be directed to the client/patient care team. Clients/patients may request access to their personal health records orally or in writing. The client's/patient's identity or the substitute decision-maker's authority needs to be verified prior to granting the access.

Providing Access

Clients/patients are provided access by way of viewing the original record or by obtaining a copy of their record.

If access is provided by way of viewing the original records, such access should be provided in the presence of a representative of McMaster University.

Timeframe to Respond

The health information custodian has thirty (30) days from the date of the request to respond to the request for access. If additional time is required, the client/patient must be provided with a written notice of an extension. The extension request should identify when a response might be expected and why an extension is needed.

An extension is only permitted if:

- Replying to the request within thirty (30) days would unreasonably interfere with activities since the search in locating the personal health records is complex; or
- The time required to undertake the necessary consultations would make it impractical to reply within thirty (30) days.

If there is no response to a request for access within a sixty (60) day time period, the request for access is deemed to have been refused.

Urgent Request

Where a client/patient satisfies the University that he or she needs the record on an "urgent basis" within a period of less than thirty (30) days, the University is obliged to make every reasonable effort to comply with this request.

Fees for Providing Access

A fee for providing access may be charged to the client/patient if an estimate of the fee is provided.

The fee cannot exceed a prescribed amount, or if no amount is prescribed, the amount of the fee cannot exceed the amount of a reasonable cost recovery (see Guideline on Fees).

A fee may be waived in total or in part, if it is deemed appropriate to do so.

Refusing a Request for Access

Should the request for access be refused, reasons for such refusal must be provided to the client/patient.

Filing a Complaint

The client/patient can complain to the McMaster University Privacy Officer or to the Information Privacy Commission/Ontario about a refusal of a request for access.

Related Documents:

Policy for Handling of Personal Health Information
Policy on Correction of Personal Health Information
McMaster Lock-box Protocol
Guideline for Verifying Identity
Guideline on Fees
McMaster Statement of Information Practices

Policies, Procedures and Guidelines

Complete Policy Title: **Policy on Correction of Personal Health Information**	Policy Number (if applicable):
Approved by: **President**	Date of Most Recent Approval:
Date of Original Approval(s): **June, 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*

Policy

A capable client/patient or their Substitute Decision-Maker (SDM) may request that incorrect information, contained in their health record and having an impact on their healthcare, be corrected under PHIPA.

Purpose

To provide individuals with a right of access to personal health information about themselves and a right to request correction or amendment of personal health information about themselves.

To provide for independent review and resolution of complaints with respect to personal health information and to provide effective remedies for contraventions of the *Personal Health Information Protection Act*, 2004 (PHIPA).

If a Health Information Custodian has granted an individual access to a record of his or her personal health information and if the individual believes that the record is inaccurate or incomplete for the purposes for which the custodian has collected uses or has used the information, the individual may request in writing that the custodian correct the record.

Duty to correct

The Health Information Custodian is to grant a request for a correction, if the individual demonstrates, to the satisfaction of the custodian, that the record is incomplete or inaccurate for the purposes for which the custodian uses the information and gives the custodian the information necessary to enable the custodian to correct the record.

Information deemed to be incorrect may be handled by: labeling the information as incorrect, severing the incorrect information from the record, storing it separately from the record and maintaining a link in the record that enables a person to trace the incorrect information. If it is not possible to record the correct information in the record, there is to be a process ensuring that there is a practical system in place to inform a person who accesses the record that the information in the record is incorrect and to direct the person to the correct information.

Informal request

If the individual makes an oral request that the Health Information Custodian correct the record, nothing in the Act prevents the custodian from making the requested correction.

Procedure for Requests for Correction

After a client/patient has accessed their personal health information (PHI) and determined that there are what they believe to be inaccuracies in the document(s) that may have an impact on their healthcare they may complete a formal Correction Request Form and submit this to the McMaster University Privacy Officer.

The McMaster University Privacy Officer upon receipt of the completed correction request form, will verify the identity of the client/patient or if applicable, the SDM using a standard protocol (see Guideline on Verifying Identity)

Once satisfied as to the identity of the requester, the University Privacy Officer will process the request for correction in accordance with Schedule A, s.55 of PHIPA.

Related Documents:

Policy for Handling of Personal Health Information
Policy on Access to Personal Health Information
McMaster Lock-box Protocol
Guideline for Verifying Identity
Guideline on Withdrawal of Consent
McMaster Statement of Information Practices

Policies, Procedures and Guidelines

Complete Policy Title:
Background Check Policy

Policy Number (if applicable):

Approved by:
President

Date of Most Recent Approval:

Date of Original Approval(s):
June 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*

Purpose:
The purpose of this Policy is to outline clearly the limits within which the University will respond to a request for the personal information of a student/alumnus in relation to a background check.

McMaster University regularly receives requests from third parties conducting background checks for records in respect of its students or alumni. As an institution subject to the *Freedom of Information and Protection of Privacy Act,* RSO 1990, McMaster takes seriously its responsibilities regarding the disclosure of personal information in response to such requests. While these requests are normally accompanied by a consent form, such forms are often broadly drafted and do not describe records with sufficient specificity.

Policy:
Absent the specific and express identification of a particular record within the written consent from the person to whom the personal information relates, McMaster University presumes that a general form of consent is intended to only allow for the release of the following student records and information: *Student Code of Conduct* and *Residence Code of Conduct*.

McMaster will neither confirm nor deny the existence of any other records relating to the individual subject of the background check. Such other records include, but are not limited to, Security Reports and Academic Integrity Policy records.

Requests for student transcripts[1] are outside the scope of this Policy and are to be addressed by a student or alumnus to the Office of the Registrar.

McMaster may, at its sole discretion and without advising a third party requester, contact the party to whom personal information relates to confirm the scope of any individual consent.

---

[1] Student transcripts may contain notations for sanctions under the *Academic Integrity Policy* or *Student Code of Conduct*. The removal of these notations is governed by the *Transcript Notation – Removal Process.*