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:
July 1, 2017

Date of Original Approval(s):
June 2015

Supersedes/Amends Policy dated:
June 2015

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). Where feasible, other means of communicating confidential information should be considered, such as the use of the University's MacDrive system administered by UTS or the MacDrop system administered by CSU. Unencrypted confidential information should not be shared through external systems (e.g. Dropbox, Google Docs).

Each user has an obligation to be aware of computer security and privacy concerns, and to 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 information includes patient or 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, financial records, citizenship, academic record, grades, accommodations in place, etc.

Confidential personal information and/or personal health information should not be sent over the e-mail system 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.

Exceptions:

- 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).
- 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).
- Health professionals within the circle of care of a patient may communicate with each other via the internal university email system, and without encryption or password protection of the message, provided that the email accounts of the sender and recipient are located on the secure Faculty of Health Sciences Exchange Server.
- A health professional within the circle of care of a patient may communicate to another health professional or healthcare institution at an outside email address with unencrypted PI/PHI within the body of the email provided that:
    - the use of the PI/PHI is permitted under PHIPA and the activities are within the duties of the professional and/or institution; and
    - the email address of the recipient is at a hospital or healthcare institution which provides a secure email platform (i.e., a participant in the OneMail program of eHealth Ontario or similar program); and
    - the email package is transmitted using TLS encryption.

To maintain security of e-mail communications, autoforwarding of email accounts will not be allowed if the e-mail account might be a recipient of confidential business information, personal information or personal health information.

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:

Information Security Policy
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