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

Approved by: President
Date of Original Approval(s): June 16, 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).

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