

CATEGORY:	<b>INFORMATION TECHNOLOGY</b>
SUB-CATEGORY:	<b>APPROPRIATE TECHNOLOGY USE</b>
GROUP:	
DISTRIBUTION:	<b>ALL STAFF</b>
TITLE:	<b>COMMUNICATING CONFIDENTIAL INFORMATION VIA EMAIL</b>

**PURPOSE**

- To establish a framework for the appropriate use of Western Health’s email systems for communicating confidential information.
- To provide guidelines for the use of e-mail for communicating confidential information within specified parameters.

**POLICY**

[Policy 10-01-75 Communicating Personal Health Information](#) via email specifically addresses the communication of personal health information by email. This policy applies to all employees and agents of Western Health who communicate other forms of confidential information (e.g. other types of personal information or confidential business information) via email.

Western Health is committed to efficient secure communication and the protection and privacy of confidential information. All means of communication have inherent risks. An increasing amount of communication is being conducted using electronic mail. Internal email communication within Western Health is secure. When external email communication contains confidential information, it must be sent adhering to the Western Health [Email Acceptable Use policy \(10-01-50\)](#) and the guideline, [Sending an Encrypted Email Message](#).

Western Health recognizes the importance of efficient communication. Secure email is an efficient form of communication; however, email containing confidential information must follow security protocols. These include but are not limited to:

1. Communication within the Western Health secure network, i.e. from an address at westernhealth.nl.ca to another address at westernhealth.nl.ca.
2. Following the [Email Acceptable Use policy \(10-01-50\)](#) and guideline [Sending an Encrypted Email Message](#) when sending email external to Western Health that includes personal health information or any other confidential information.

*Only the electronic version of this policy is to be considered current. Paper copies may be outdated. This policy is uncontrolled when printed.*

3. Adhering to Western Health’s Disclosure of Information policies when disclosing confidential via email.
4. Including a visible privacy/confidentiality statement when confidential information is communicated via email.
5. Following the guideline, [Using Scan-to-Email on Western Health Multi-Function Printers](#), when using the scan-to-email feature on Western Health multi-function printers.

#### For Internal Email:

1. Communication to another individual or provider within Western Health must take place within the Western Health e-mail system.
2. Verify that the correct email address for the recipient is being used.
3. DO NOT include confidential information in the subject line.
4. Limit the amount of information sent via email to only that which is essential for the purpose of the communication.
5. Take care not to respond to or forward emails that, through the accumulation of information, cause confidential information to be inappropriately disclosed.

#### For External Email

1. Follow all the above steps.
2. All external non-Western Health email communication must take place by adhering to the [Email Acceptable Use policy \(10-01-50\)](#) and the guideline, [Sending an Encrypted Email Message](#).

#### Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing at Western Health. Allegations of misconduct will be addressed according to established procedures. Sanctions for inappropriate use on Western Health’s email system may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of email access;
2. Disciplinary action according to applicable Western Health policies;
3. Termination of employment; and/or
4. Legal action according to applicable laws and contractual agreements.

*Only the electronic version of this policy is to be considered current. Paper copies may be outdated. This policy is uncontrolled when printed.*

**GUIDELINES**

[Using Scan-to-Email on Western Health Multi-Function Printers](#)

[Sending an Encrypted Email Message](#)

**KEYWORDS**

Email  
 e-mail  
 email system  
 confidentiality  
 electronic mail  
 records

**TO BE COMPLETED BY STAFF IN QUALITY DEPARTMENT**

Approved By: Chief Executive Officer	Maintained By: Provincial Manager-Application Development, Solutions and Infrastructure
Effective Date: 14/December/2017	<input checked="" type="checkbox"/> Reviewed: 20/October/2020 <input checked="" type="checkbox"/> Revised: 30/June/2021
Review Date: 30/June/2024	<input type="checkbox"/> Replaces: <i>(Indicates name and number of policy being replaced)</i> OR <input checked="" type="checkbox"/> New

*Only the electronic version of this policy is to be considered current. Paper copies may be outdated. This policy is uncontrolled when printed.*