CATEGORY:	**INFORMATION TECHNOLOGY**
SUB-CATEGORY:	**APPROPRIATE TECHNOLOGY USE**
GROUP:	
DISTRIBUTION:	**ALL STAFF**
TITLE:	**COMMUNICATING PERSONAL HEALTH INFORMATION VIA EMAIL**

PURPOSE

- To establish a framework for the appropriate use of Western Health's email systems for communicating client/patient/resident information.
- To provide guidelines for the use of e-mail for communicating client/patient/resident information within specified parameters.

POLICY

This policy applies to all employees and agents of Western Health who communicate client/patient/resident information via email.

Western Health is committed to efficient secure communication and the protection and privacy of personal health 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 personal health 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*.

Personal health information collected through email becomes part of the client/patient/resident record.

Western Health recognizes that efficient communication positively affects client/patient/resident care and service delivery. Secure email is an efficient form of communication; however, email containing client/patient/resident 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 *Secure Send an Encrypted Email Message* when sending email external to Western Health that includes personal health information or any other confidential information.

3. Adhering to Western Health's Disclosure of Information policies when disclosing personal health information via email.

4. Including a visible privacy/confidentiality statement when client/patient/resident 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 client/patient/resident information in the subject line.

4. Clearly identify the client/patient/resident in the body of the email.

5. Limit the amount of information sent via email to only that which is essential for the purpose of the communication.

6. Take care not to respond to or forward emails that, through the accumulation of information, cause identifiable client/patient/resident information to be inappropriately disclosed.

7. When client/patient/resident information on service delivery of care is communicated via email, place the email in the client/patient/resident record with additional positive patient identifiers to ensure accurate filing. Write a brief summary of the correspondence in the progress/service notes.

8. Save attachments containing client/patient/resident information in PDF format, when possible, and place in the client/patient/resident record.

9. Delete the email once the required documentation is complete.

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*.

Communicating with Patients/Residents/Clients via Email:

Email is an acceptable means of communicating with clients or, where applicable, clients' substitute decision–makers provided that this practice is approved by the management in the clinical area. However, it is important that the client or substitute decision-maker understand the risks inherent in email communication and their responsibilities in protecting their own privacy. The following message may be used at the outset of any new email correspondence with a client or substitute decision-maker to help establish this understanding:

> *Before we begin to talk through email, I am required to make sure that you are OK with a few things:*
> - *Anything we write in emails becomes part of Western Health's official records, the same as if I print it off and put it in a file.*
> - *Western Health's email is very secure because we have staff who take care of that, but we can't ensure the security of the email system that you use. You have to be comfortable with that.*
> - *We both need to be very careful about sending and replying to each other's messages to make sure that we don't accidentally send one to the wrong person.*
>
> *Are you OK with all of this?*

If the client consents to communicating about his or her care by email, either verbally or by some other means, the consent must be reflected in the client/patient/resident record.

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 systems and services 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.

GUIDELINES

Using Scan-to-Email on Western Health Multi-Function Printers

Secure Send 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: Regional Director – Information Management
Effective Date: 14/December/2017	❒ Reviewed: ☑ Revised: 30/June/2021
Review Date: 30/June/2024	❒ Replaces: *(Indicates name and number of policy being replaced)* OR ☑ New