

EMAIL GUIDELINES

GUIDELINES ON EMAILING PERSONAL INFORMATION

We have a shared accountability to protect personal information. Therefore, the purpose of this document is to provide guidelines for PHC staff and physicians that will help ensure we protect and maintain the privacy and integrity of personal information received and transmitted by email.

GENERAL GUIDELINES:

- Personal information should be sent by the most secure method of communication.
 - Only email personal information where urgency is required, and email is the only timely way to send this information.
 - Keep emails brief, factual and objective. Email may be released under FIPPA.
 - All messages are the property of Providence Health Care and may be monitored.
 - As a general rule, do not communicate with patients/residents via email. Where a patient/resident prefers to communicate by email, explain to them the risks and get their consent. Then, ask the patient/resident to send the initial email to initiate the communication. If PHC Staff need to send the initial email, the first message should only ask the recipient to reply and confirm it is the correct email address. Call the recipient and verify if still unsure.
-

WHEN YOU HAVE TO EMAIL PERSONAL INFORMATION:

- Remove personal identifiers wherever possible. Consider the use of unique identifiers or codes to protect the identity of the individual(s) involved.
- Encrypt and password protect any email attachment containing personal information, and do not share the password via email; rather communicate it by phone.
- Avoid sending highly sensitive personal information.
- Keep personal information to a minimum.
- Send only to those that “need to know”.
- Verify email addresses with recipients. Double check the email address(es) prior to sending.
- Never use email distribution lists.
- Confirm delivery with the recipient, where possible.
- Never **forward**, **reply to**, or **reply all** if the email contains personal information; create a new email containing only the information that needs to be sent.
- Delete emails containing personal information from your **inbox**, **sent box**, **delete box** as soon as possible after the email has been received or sent.
- Never email personal information to an external email account.
- Attach a written notice to an email containing personal information:
This email message, including any attachments, contains confidential information and is intended solely for the use of the individual or entity to whom it is addressed. Any distribution, copying, disclosure, or other use is strictly prohibited. If you have received this email in error, please notify the sender immediately and permanently delete this message. Thank you.
- Immediately notify your manager and the Information Access & Privacy Office if an email is misdirected. If you think your email account has been compromised, immediately contact the Service Desk.
- If you have any questions about emailing personal information, contact the Information Access & Privacy Office at 604-806-8336 or privacy@providencehealth.bc.ca.