



- Welcome to a webinar about understanding BC's Personal Information Protection Act or PIPA for short.
- If you're a physician or MOA working in a private practice, this webinar is for you.

## EMAIL RISKS

- Mistakes
  - Sending to the wrong email address (procedures)
  - Using a distribution list (not using BCC)
  - Delays in response time and care
- Misunderstandings
  - Misinterpretation of content
  - Poor writing skills
- Mishandling
  - Saved on unsecured backup servers
  - Subject to improper access and retention rules
  - Personal information leaves Canada



OFFICE OF THE  
INFORMATION &  
PRIVACY COMMISSIONER  
for British Columbia



Protecting privacy. Promoting transparency.

There are lots of risks involved in using email to communicate with patients

- Mistakes happen
- Sometimes an email is sent to the wrong recipient – you need to have procedures documented on how to respond
  - For example,
    - 1) asking the recipient to confirm they have destroyed any printed copies and permanently deleted the email received in error and
    - 2) Informing the patient about
      - a) what happened
      - b) that you have confirmation of destruction and permanent deletion from the accidental recipient
      - c) that you don't believe there is any real risk of significant harm to them as a result of the error and
      - d) an apology for the inconvenience
- If you send to a distribution list and don't put all the recipient email addresses in the BCC, you've had a breach because you've exposed email addresses of other individuals
- Delays could negatively impact a patient's care if timeliness is critical
- Misunderstandings can happen with
  - one-way communications and two-way is always better
  - or if the sender has poor writing skills but has better verbal skills
- Mishandling can occur if information is
  - Saved on unsecured backup servers
  - Subject to improper access and retention rules and

- Personal information can often leave Canada

## EMAIL RISKS

- Interception when sent from an unsecured network
  - publicly accessible computer
  - home computer
  - over a public Wi-Fi network
  - through an ISP shared with other third parties
- Generally not encrypted and could be
  - intercepted or
  - altered
- Crime
  - Attachments with viruses or malware
  - Phishing attempts
  - Ransomware links



OFFICE OF THE  
INFORMATION &  
PRIVACY COMMISSIONER  
for British Columbia

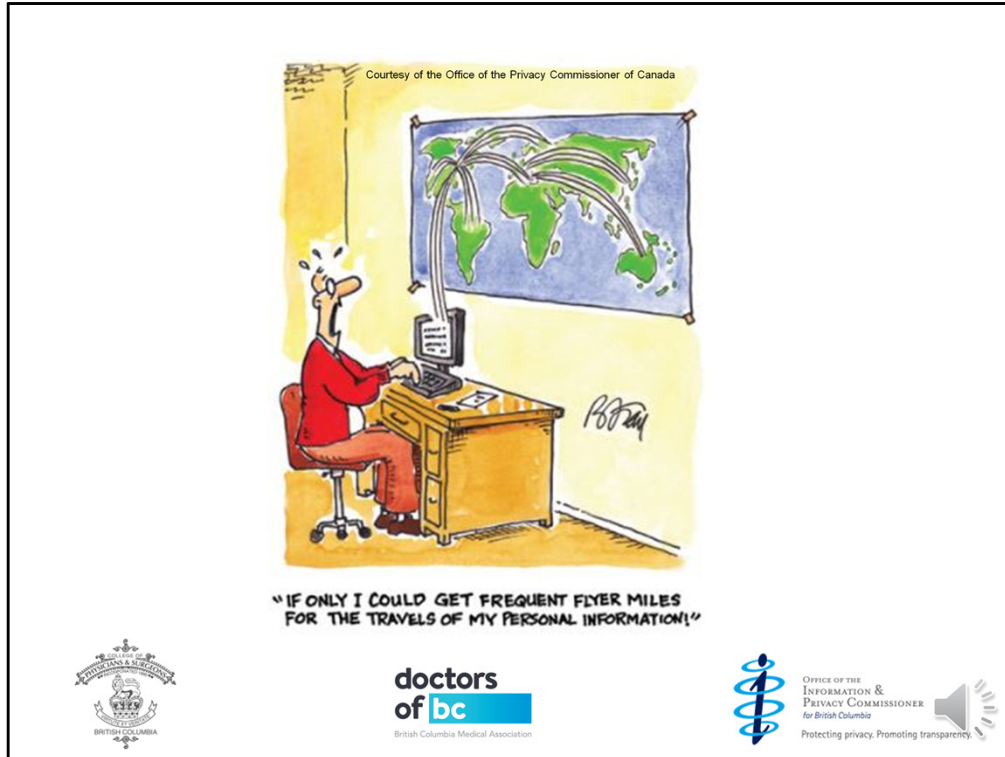


Protecting privacy. Promoting transparency.

Other risks include

- The potential for the email to be intercepted if it's sent from an unsecured network like
  - a publicly accessible computer,
  - home computer
  - over a public Wi-Fi network or
  - through an ISP shared with other third parties
- Email is generally not encrypted and could be
  - intercepted or
  - altered
- Crime needs to be considered as
  - attachments may contain viruses or malware
  - hackers could have obtained access to a patient's email and be on a phishing expedition or
  - ransomware links could be present

You need to take reasonable steps to protect personal information under your control



Here's an example of how email travels

If you include personal health information in an email, it will very likely leave Canada  
This may make it subject to laws in other jurisdictions that have inadequate or no  
protections

## WHERE DO YOU START?

- Inform patients of
  - the potential risks
  - precautions (anonymization)
  - alternatives (encryption, postal mail, courier)
  - their right to withhold or withdraw consent
  
- Policies and Procedures
  - acceptable use, verification and email etiquette
  - removing sensitive personal information and diagnosis/prognosis
  - managing the email component of medical records
  - password protecting attachments or encrypting emails
  - retention and destruction
  
- Employee training



OFFICE OF THE  
INFORMATION &  
PRIVACY COMMISSIONER  
for British Columbia



Protecting privacy. Promoting transparency.

## WHERE DO YOU START?

- Inform your patients of
  - the potential risks of using email
  - precautions you need to take to anonymize their personal information
  - alternatives available such as encryption, postal mail or courier and the impacts of using those alternatives and
  - their right to withhold or withdraw consent
- Make sure your policies and procedures cover
  - acceptable use, verification and email etiquette
  - removing sensitive personal information and diagnosis or prognosis as this should be done in a face to face meeting
  - managing the email component of medical records
  - password protecting attachments or encrypting emails and
  - rules for retention and destruction
- Most importantly, make sure your employees are trained

## IDENTIFICATION

- How do you confirm the:
  - identity of the patient when email is received?
  - email address before an email is sent?

Multiple patients may have the same name  
Email addresses may be cryptic

- Controls
  - Visual verification
  - Automation

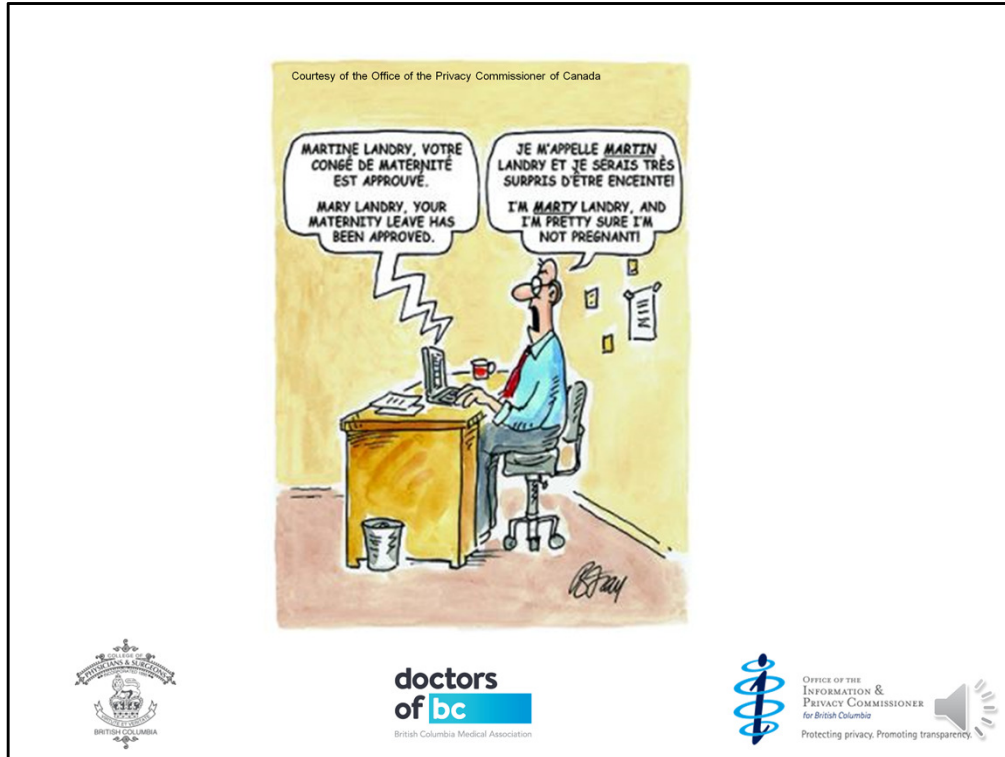


OFFICE OF THE  
INFORMATION &  
PRIVACY COMMISSIONER  
for British Columbia



Protecting privacy. Promoting transparency.

- Think about how you confirm the
  - identity of the patient when email is received
  - or the email address before an email is sent
    - when you might have multiple patients with the same name
    - or the email address is cryptic and doesn't contain the patient's name
- There are a number of controls that can be used
  - Visual verification is a manual, administrative control where the email address is confirmed by referring to a patient's electronic or paper records
  - There are several automated tools that can be used to authenticate email addresses
    - For example, your email software should be set up to display the full name of the patient which could help if it's unique



Here's an example of an email being sent to the wrong patient

All of your outgoing emails should contain a disclaimer

Check out the Tools Tab in the Privacy Toolkit for the wording you can use



## WEBINAR RESOURCES

- College Standards and Guidelines  
<https://www.cpsbc.ca/for-physicians/standards-guidelines>
- Doctors of BC Privacy Toolkit and webinar notes (PDF)  
<https://www.doctorsofbc.ca/privacy-toolkit-webinars>
- Office of the Information & Privacy Commissioner for BC:
  - Guide to PIPA
  - Privacy Breach Tools and Resources
  - Accountability Tips
  - Getting Accountability Right
  - Self-Assessment Tool for Securing Personal Information
  - Cloud Computing Guidelines
  - Guidance Document: Information Sharing Agreements<https://www.oipc.bc.ca/guidance/guidance-documents/>



OFFICE OF THE  
INFORMATION &  
PRIVACY COMMISSIONER  
for British Columbia



Protecting privacy. Promoting transparency.

Links to these Resources are in a PDF document on the Webinars page of the Privacy Toolkit

- College Standards and Guidelines
- Doctors of BC Privacy Toolkit and webinar notes
- and Privacy Commissioner guides, tips and resources



# PIPA SHORTS

BC's Personal Information Protection Act

**QUESTIONS?**  
[privacyofficer@doctorsofbc.ca](mailto:privacyofficer@doctorsofbc.ca)



**doctors  
of bc**  
British Columbia Medical Association



Protecting privacy. Promoting trust.

Let us know if you have any questions about complying with PIPA