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.
WHAT IS WI-FI?

- Wi-Fi technology enables devices to conveniently connect wirelessly to
  - home or office networks
  - wireless speakers
  - online payment services

- It requires your device to broadcast a unique identifier so that it can
  - be identified on a network
  - permit passive tracking

- Wi-Fi technology enables devices to conveniently connect wirelessly to
  - home or office networks
  - wireless speakers and
  - online payment services

- It requires your device to broadcast a unique identifier so that it can
  - be identified on a network and
  - permit passive tracking
• It allows hardware devices to communicate using radio frequencies to transmit data. It doesn’t require the physical cable connections used within a controlled wired environment so it’s an inherently open method of communication. Attackers have specially equipped devices that can detect weak or no security so it’s important to take security measures.

• When you have Wi-Fi on, your movements around the city or through a store can be tracked. Over time, this can, for example, provide a retailer with a detailed understanding of the areas you frequent in a store or your visits to a shopping centre. To prevent this, consider disabling Wi-Fi when it’s not in use. You can easily do this through the drop-down options or settings menus on your devices.
WHERE DO YOU START?

- Security
  - Mandatory strong passwords
  - Encrypted access points

- Policies and procedures
  - Acceptable use
  - Never using public Wi-Fi
  - Process for lost or stolen devices
  - PIN to PIN messaging
  - Secure storage and disposal procedures

- Employee Training

WHERE DO YOU START?
- Implement security so that
  - strong passwords are required for access
    For example,
    a combination of upper and lower case, numbers and symbols
    with a minimum password length and
    requirement to change at least every 90 days
  - and industry-standard encryption for access points
- Make sure you have policies and procedures documented for
  - acceptable use
  - never using public Wi-Fi
  - the process for reporting lost or stolen devices (including contacting vendors to
    disable services and wipe data)
  - never sending personal information when using PIN to PIN messaging (because
    it’s not secure)
  - securely storing devices pending disposal and having secure disposal procedures
    (more about this is in the webinar called How Can It Be Destroyed)
- and most importantly, make sure your employees are trained
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/

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