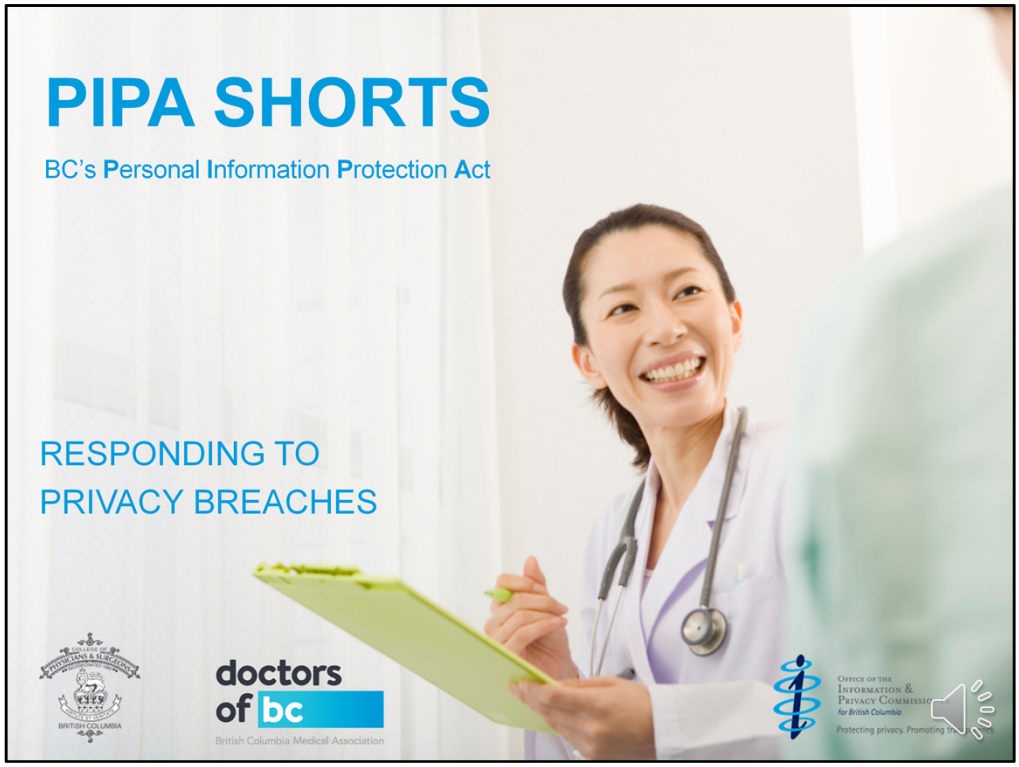
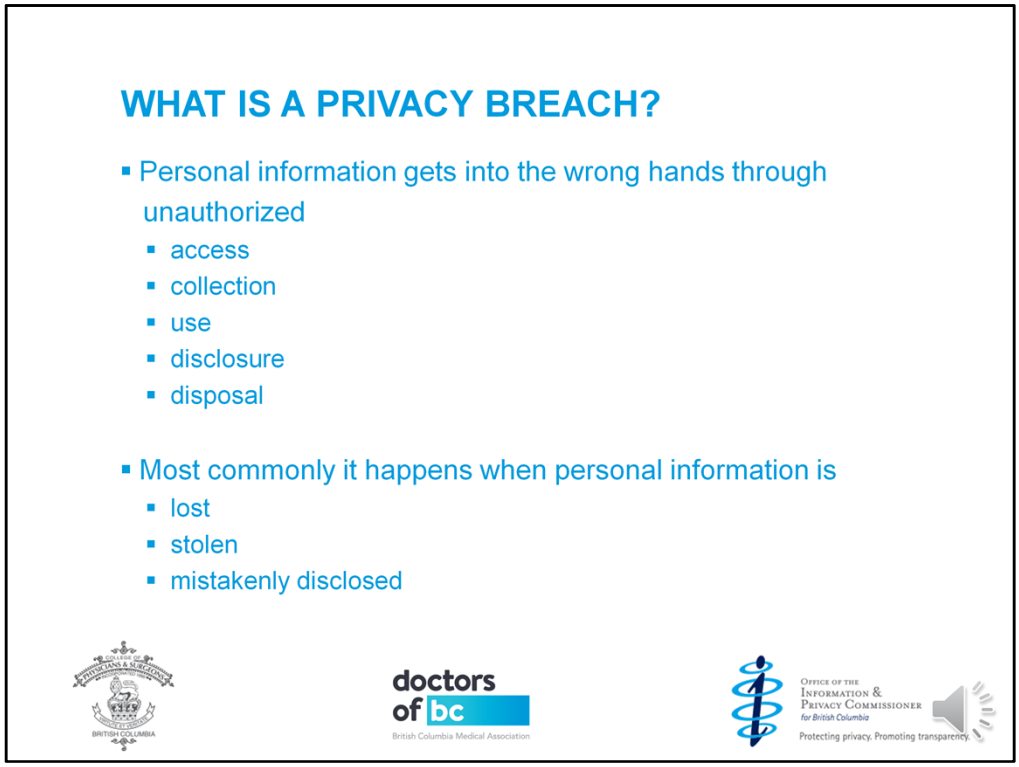
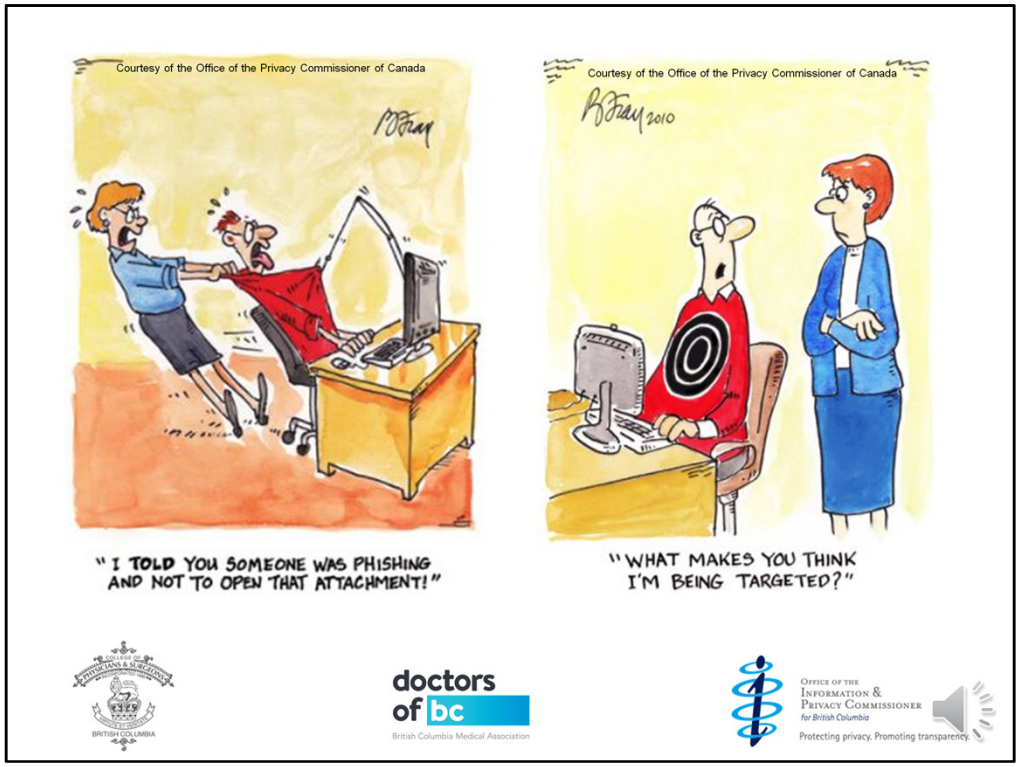


- Welcome to a webinar about understanding BC's Personal Information Protection Act or PIPA for short.
- If you're a physician or MOA working in a private practice, this webinar is for you.



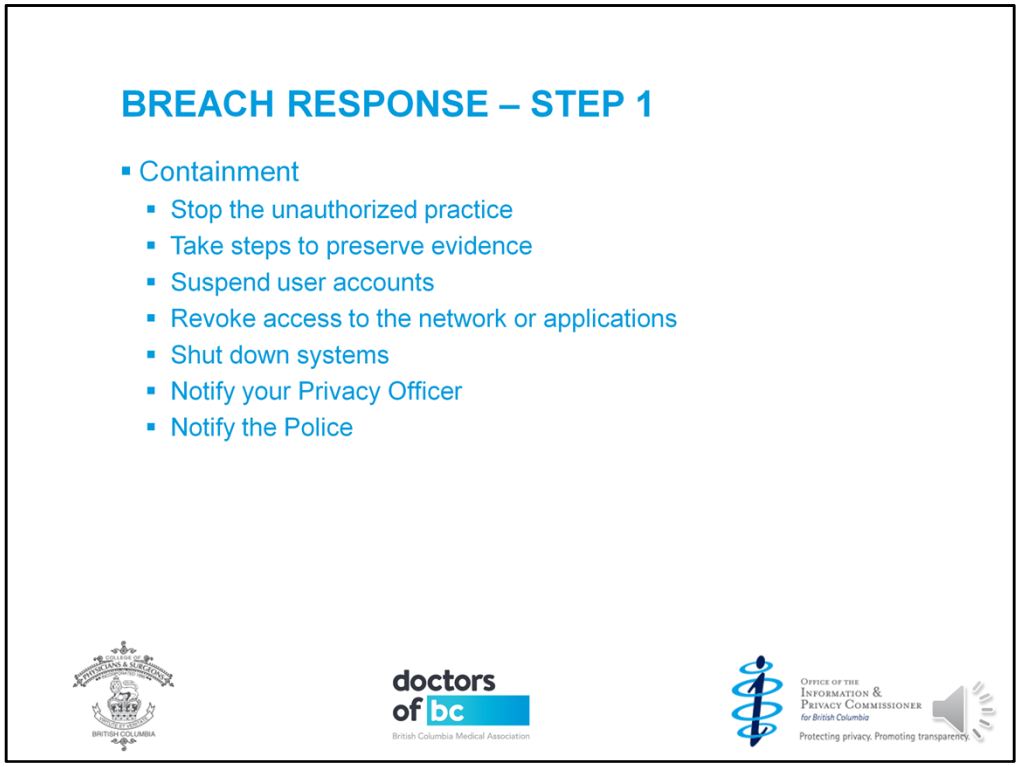
- Breaches happen when personal information gets into the wrong hands through unauthorized
    - access
    - collection
    - use
    - disclosure or
    - disposal
- The most common privacy breaches happen when personal information of your patients or employees is
    - lost
    - stolen or
    - mistakenly disclosed



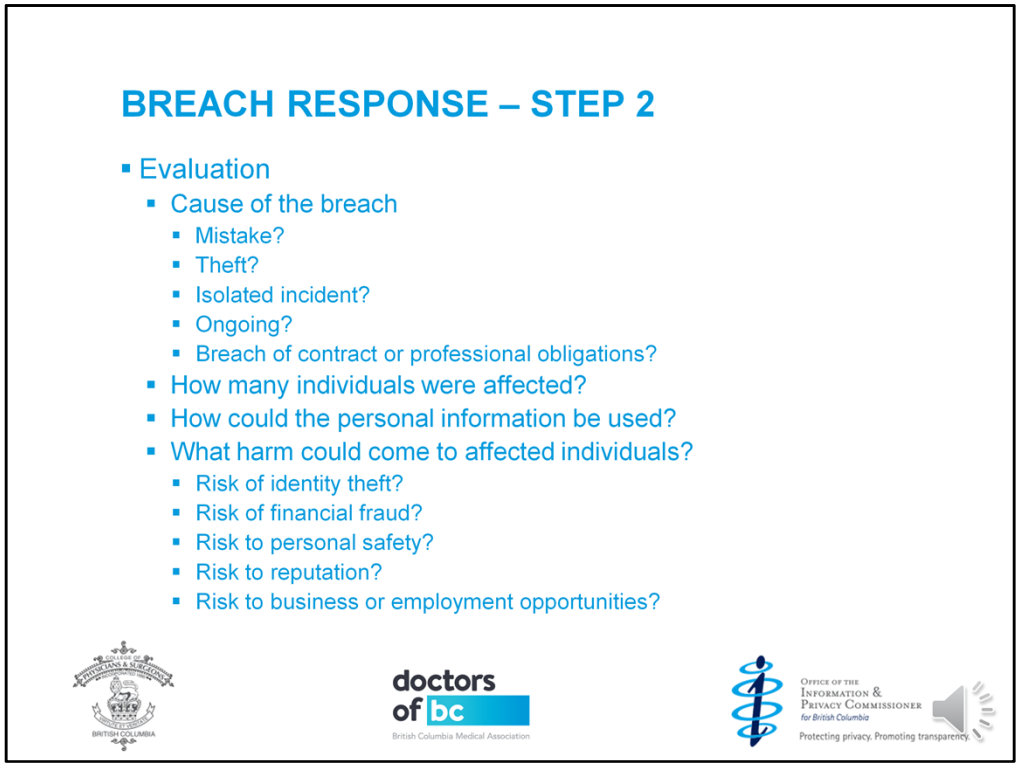
The fact that it occurred doesn't necessarily mean the practice has contravened PIPA, especially in cases of sophisticated cybercrime like phishing and ransomware.

- A breach incident may be brought to your attention by
    - an employee
    - a patient
    - the public
    - the Information and Privacy Commissioner's office or
    - detective monitoring through audits and system alerts
- There is a great tool on the Office of the Information and Privacy Commissioner website that you can use when responding to a breach
- Here's the link

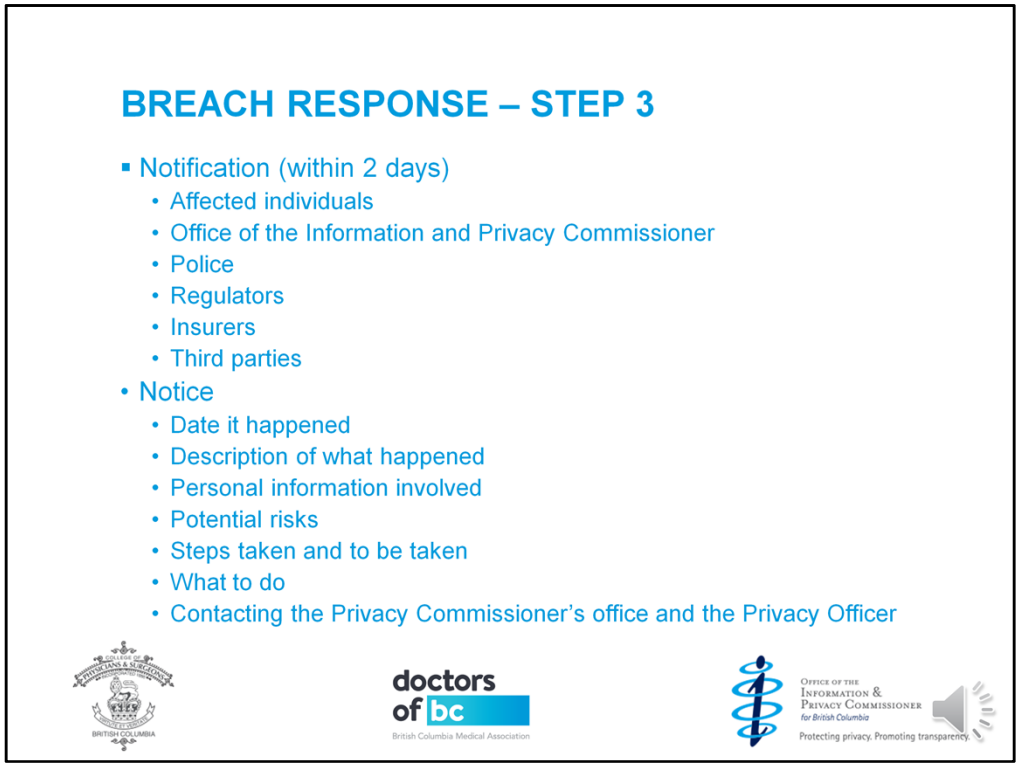
Their staff are excellent at providing guidance if you have any questions



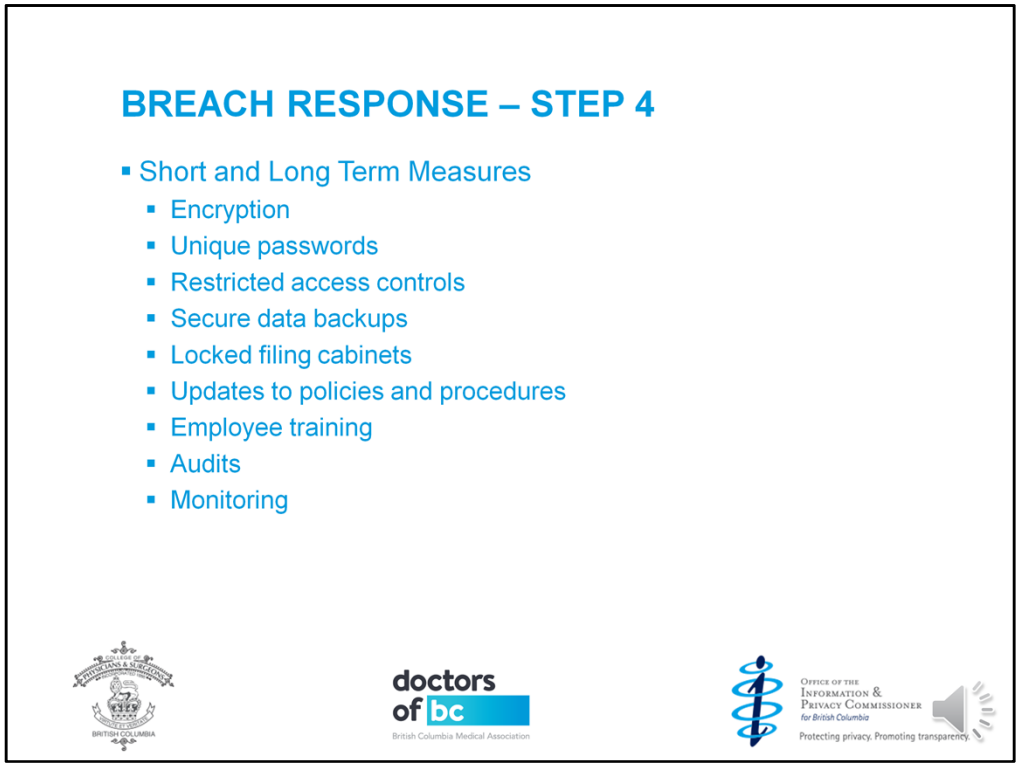
- The first step is to contain the breach by
- Stopping the unauthorized practice
- Taking steps to preserve evidence
- If systems are involved, suspending user accounts
- Revoking access to the network or applications and
- Shutting down systems
- Notifying your Privacy Officer and
- The Police if it resulted from a crime



- The next step is to evaluate the
- cause and potential impact
    - If it was a mistake, is it due to lack of training or poorly written procedures?
    - If it was a theft, could better security measures have prevented it?
    - Was it an isolated incident?
    - Could it happen again?
    - Is there a breach of contract or professional obligations?
- How many individuals were affected?
- How could the personal information be used? and
- What harm could come to affected individuals?
    - Is there a risk to their identity?
    - Financial situation?
    - Personal safety?
    - Reputation?
    - Business or employment opportunities?

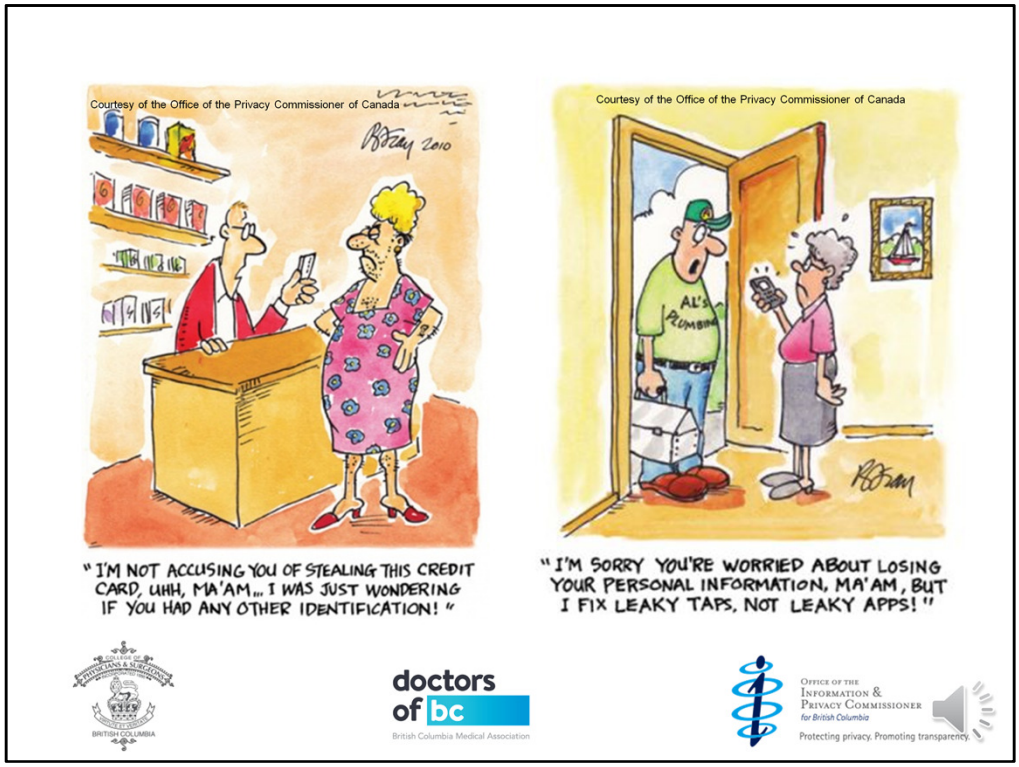


- The next step is to notify parties that need to know such as the
  - Affected individuals and as necessary
  - The Office of the Information and Privacy Commissioner
  - Police
  - Regulators
  - Insurers and
  - Third parties
- The notice should contain
  - The date the breach occurred
  - A description of what happened
  - Personal information involved
  - Potential risks
  - Steps taken and to be taken
  - What to do in terms of monitoring credit
  - How to contact the Privacy Commissioner's office and the Privacy Officer



- The last step is to implement short term and long term measures to improve how personal information is protected in the practice and help prevent future breaches. Changes could include:
    - Encrypting laptops and mobile devices
    - Making sure every user has unique credentials for system access
    - Implementing restricted access controls
    - Making data backups more secure
    - Purchasing lockable filing cabinets
    - Updating policies and procedures
    - Providing employees with more training
    - Conducting audits and
    - Implementing monitoring procedures

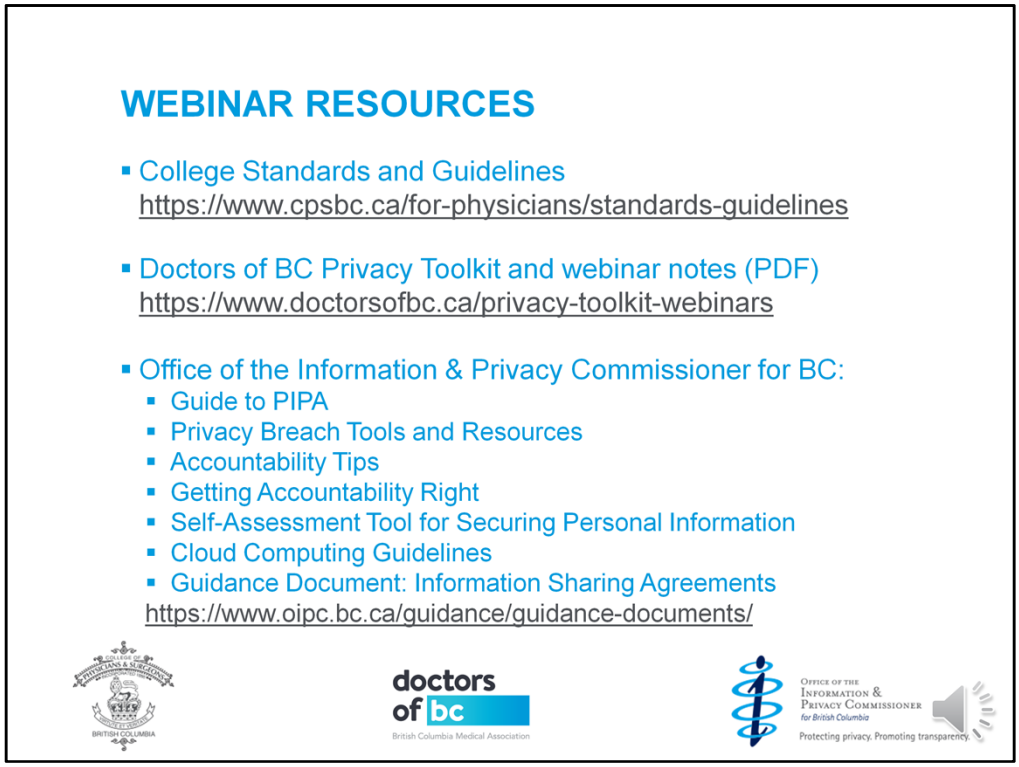
Taking these measures will help restore your reputation and help prevent future breaches.



- We're all too familiar with the PharmaNet Breach of 2017 where hackers impersonated physicians to obtain access to their patient records.

  It's a terrible violation of your privacy to know someone is impersonating you.
  And it's incredibly hard to recover your identity once it's been stolen.
  Doctors of BC Members are covered by identity theft insurance but that doesn't make it any easier.

- Making sure you get the right people on board to help you respond to a breach is important too.



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