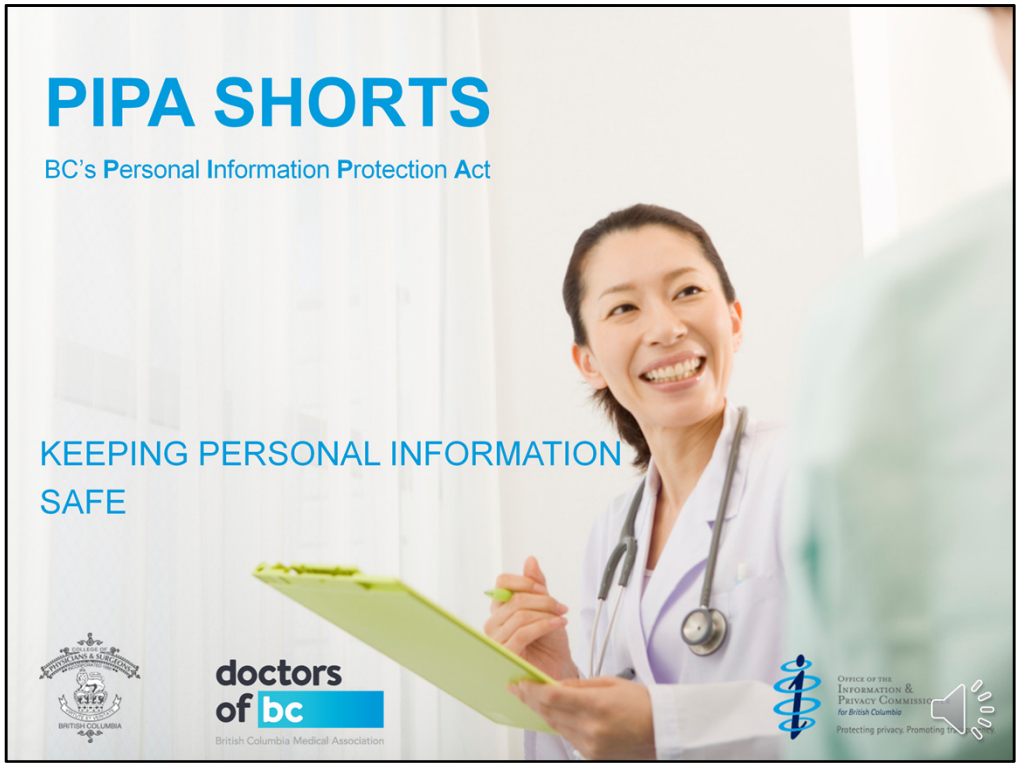
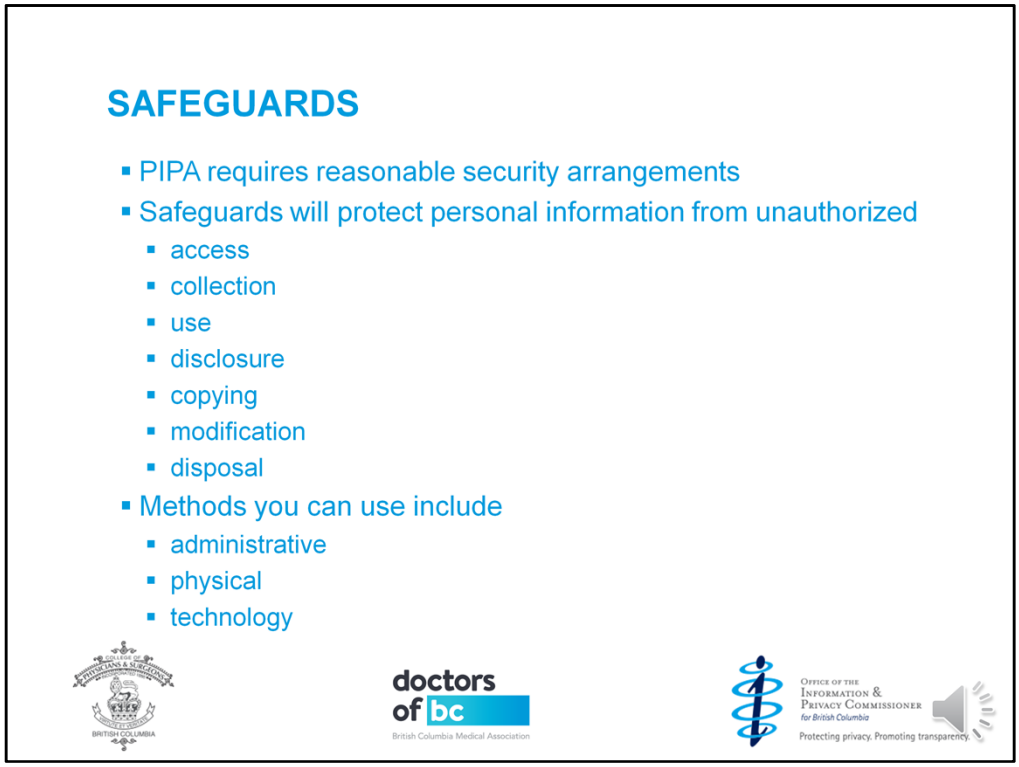


- Welcome to a webinar about understanding BC's Personal Information Protection Act or PIPA for short.
- If you're a physician or MOA working in a private practice, this webinar is for you.



- PIPA requires an organization to protect personal information in its custody or under its control by making reasonable security arrangements to safeguard it

- Safeguards will help protect personal information from unauthorized
    - access
    - collection
    - use
    - disclosure
    - copying
    - modification or
    - disposal

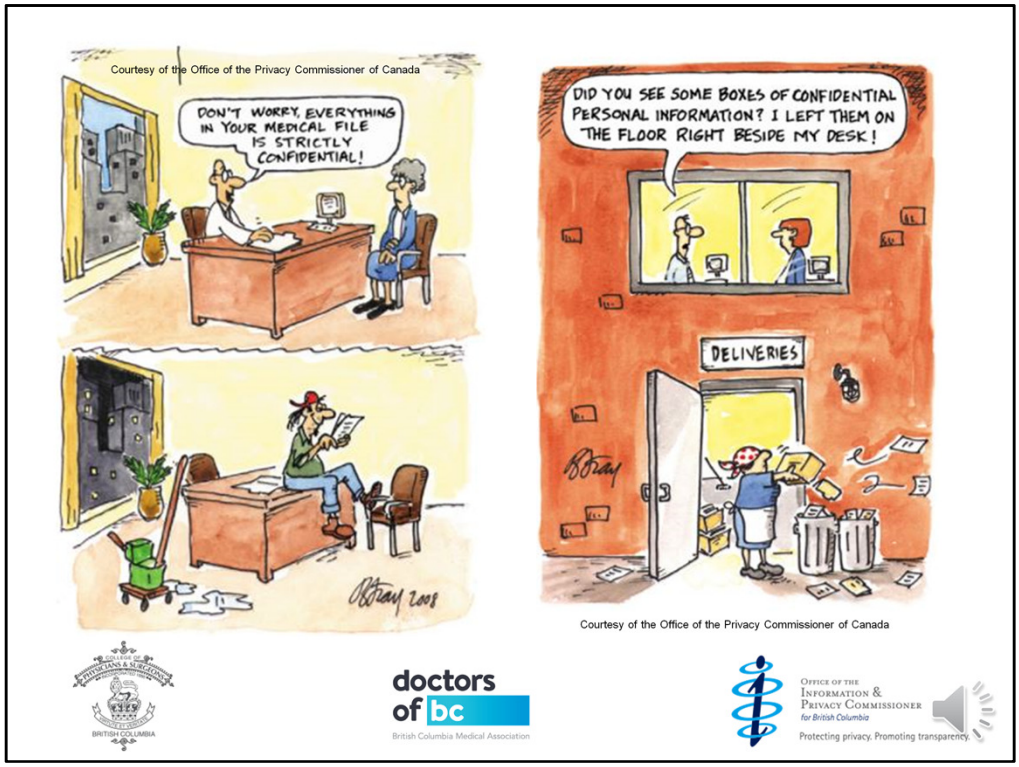
- Methods you can use include
    - administrative
    - physical and
    - technology safeguards

WHAT DO WE MEAN BY ADMINISTRATIVE SAFEGUARDS?
They include

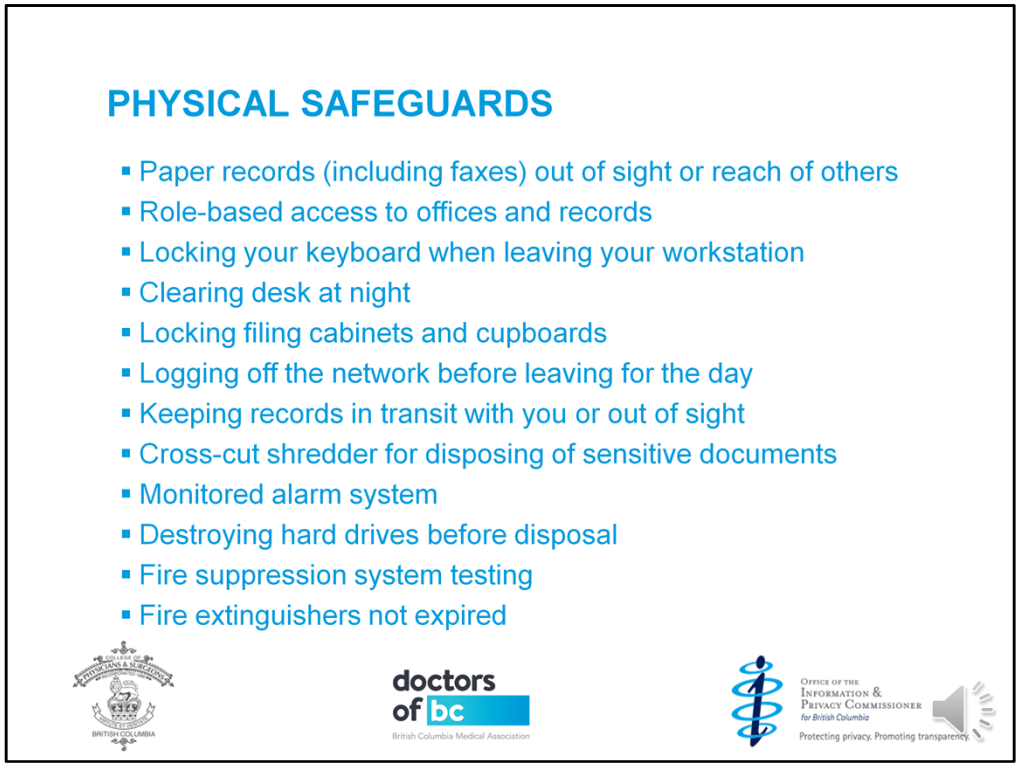
- Documented policies and procedures that include consequences for non-compliance for
    - Privacy
    - Information and system security
    - Security incident response
    - Breach management
- Forms for
    - Fax cover sheets and the confirmation process
    - Email and fax disclaimers
    - Confidentiality and Information Sharing Agreements
    - Contracts
- Employee training
    - when hired and
    - periodically afterwards

These are just a few examples that will help everyone know what to do and how

Check out the Forms Tab in the Privacy Toolkit for confidentiality and information sharing agreement templates

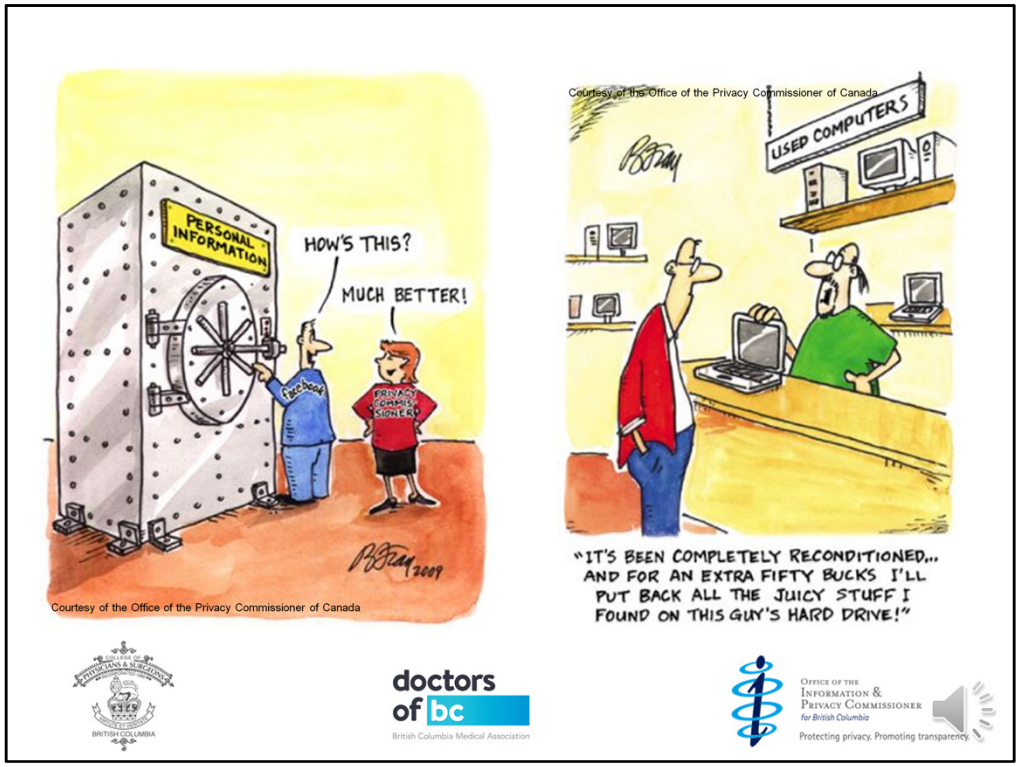


- Locking up medical records at night will prevent unauthorized reading of those records.
- Clearly labelling records will prevent accidental disposal.

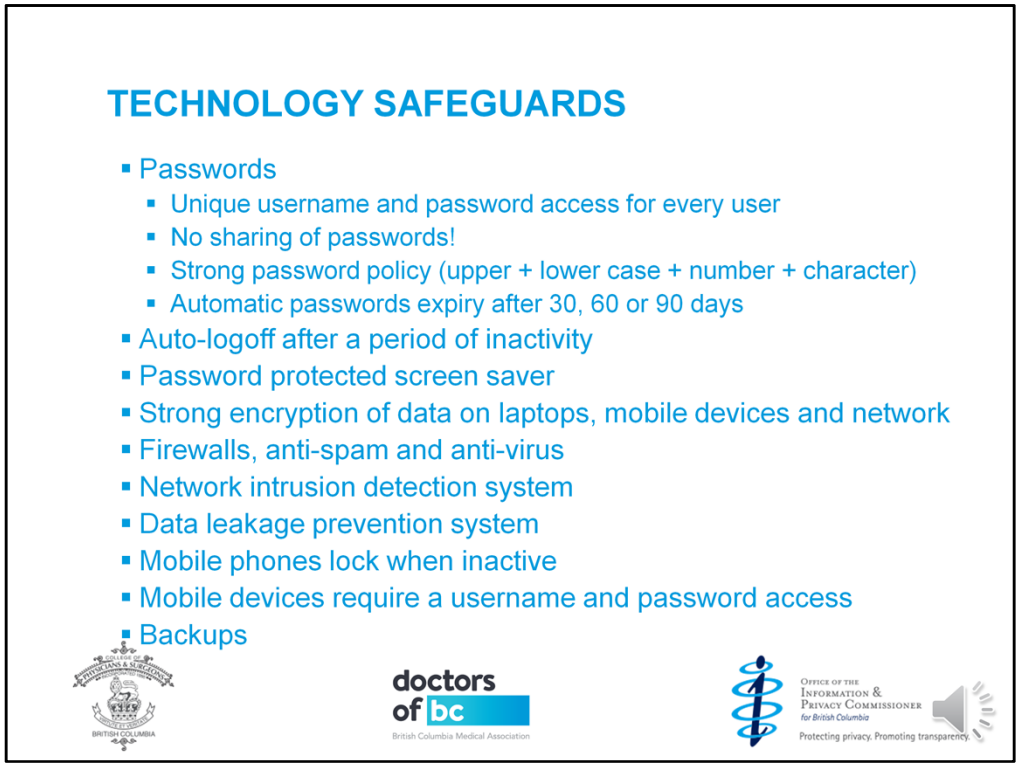


Physical safeguards over sensitive information include having

- Paper records out of sight or reach of others
- Role-based access to offices and records
- Locking your keyboard when leaving your workstation
- Clearing files with sensitive information off your desk at the end of the day
- Locking sensitive documents up at night
- Logging off the network before leaving the office
- Keeping records in transit with you or out of site in a locked trunk
- Using a cross-cut shredder to dispose of sensitive documents
- Having a monitored alarm system
- Destroying computer hard drives that contain personal information before you discard them
- Having fire suppression systems tested periodically and
- Making sure fire extinguishers haven't expired

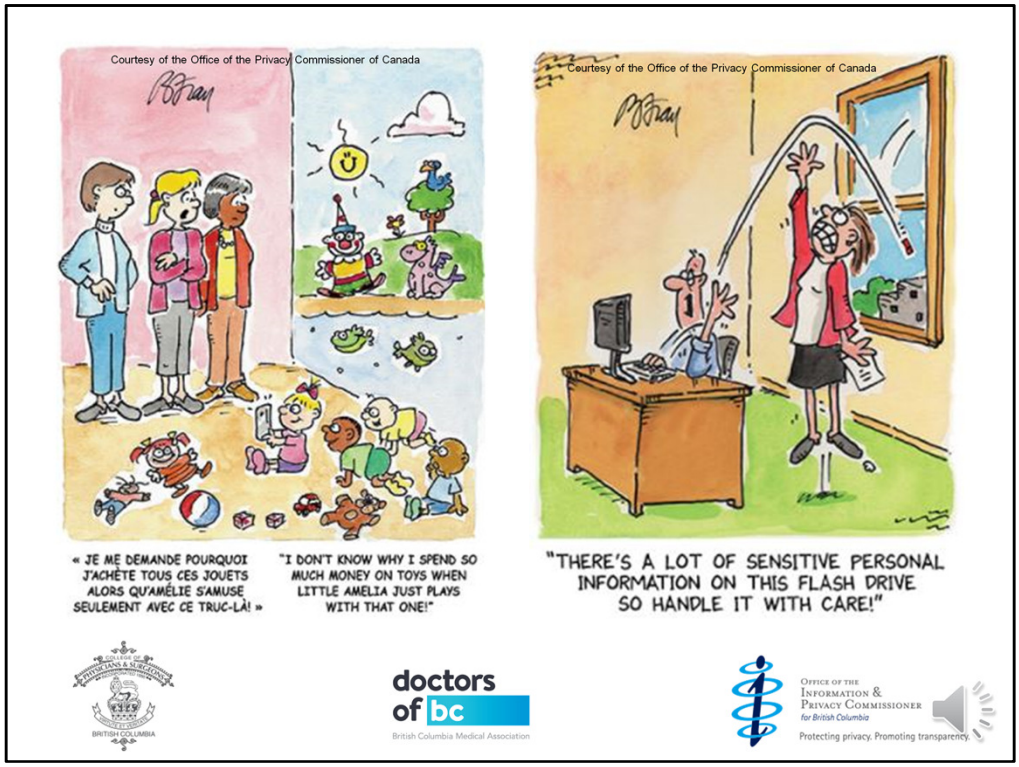


- The measures you take need to be reasonable in relation to the risks
- and take the sensitivity of the information into account



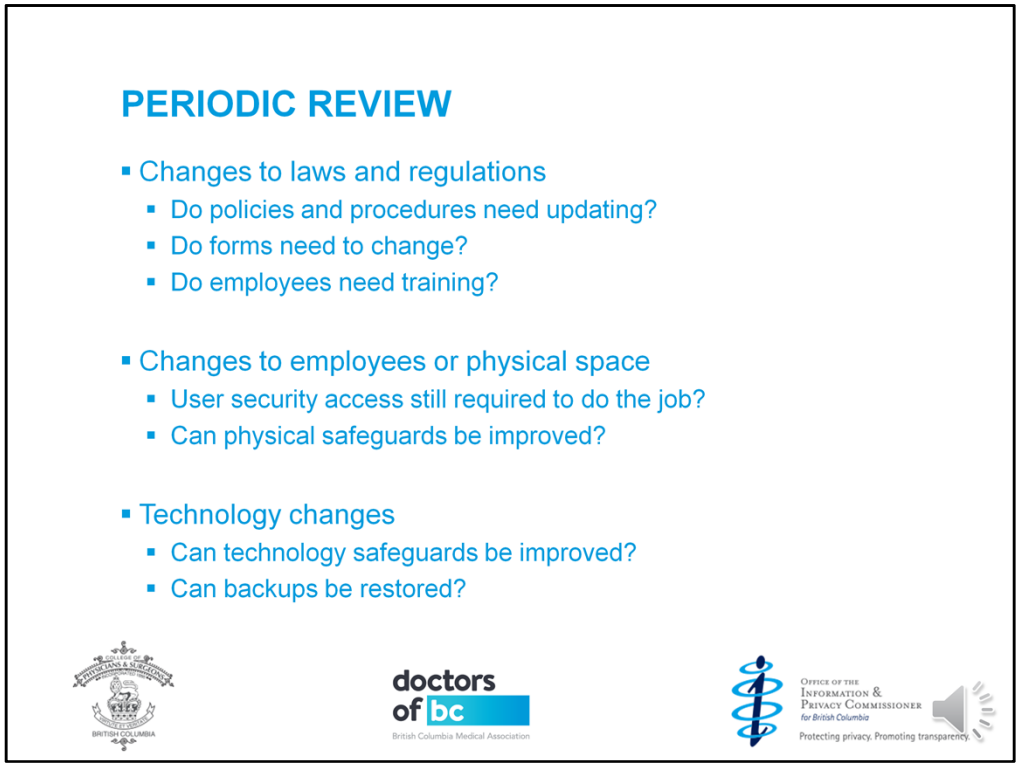
Technology safeguards include

- Passwords that are
    - unique for every user
    - never shared
    - subject to a strong password policy
    - and automatically expire after 30, 60 or 90 days
- Automated logoff after a period of inactivity
- A password-protected screen saver
- Strong encryption on laptops, mobile devices including USBs and the network
- Firewalls, anti-spam and anti-virus
- A network intrusion detection system and
- Data leakage prevention system
- Mobile phones that lock when inactive and
- Username and password access to mobile devices
- and finally, system backups



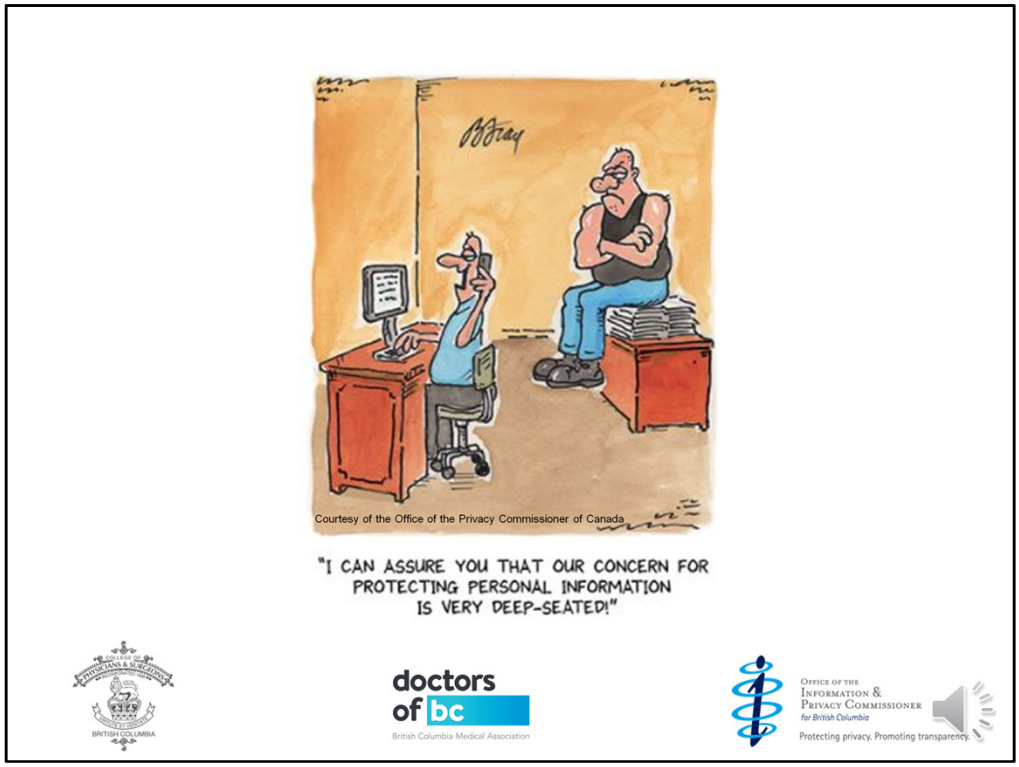
- Letting your kids play with your phone can be dangerous if you have any sensitive information on it.

- And encrypting a USB flash drive will prevent information from accidentally getting into the wrong hands.

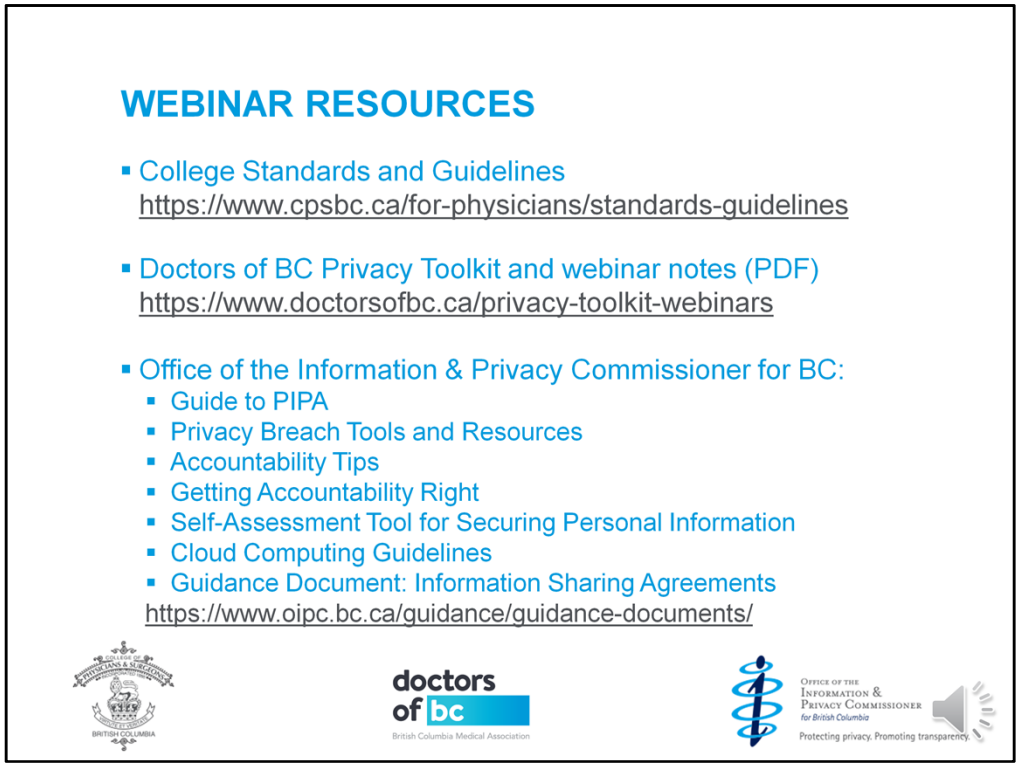


It's a good idea to review your safeguards periodically

- If there have been changes to laws or regulations affecting your practice,
    - policies and procedures
    - or forms may need to be updated
    - and employees may need training
- If there have been changes to employees, their roles or physical space,
    - user security access may need to be updated
    - There's always room for improvement so other small changes could improve physical safeguards.
- Technology is always changing so
    - There may be better technology safeguards you can use
    - and you should always test your business continuity plan each year to be sure you can still restore from backups



You want to be able to say with confidence that you protect personal information in your practice



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