



- 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.

WHERE DO YOU START?

- Policy and procedures
 - Retention policy (based on PIPA, College and other requirements *)
 - Destruction policy and procedures
- Identify
 - Where records are (files, computers, laptops or mobile devices)
 - Media records are on (paper, CDs, hard drives, USBs)
 - Third parties data has been shared with
- Destroy (only after the permitted period of time *)
 - All copies
 - Securely
 - Logs
 - Certificates of destruction



Before destroying personal information,

- check your
 - retention policy as it should be in compliance with PIPA, College standards and other legislative requirements and
 - destruction policies and procedures
- Identify
 - where the data is (in files or on computers, laptops or mobile devices)
 - what media it's on (paper, CDs, hard drives, USBs) and
 - any third parties the personal information has been shared with
- Destroy (only after the permitted period of time)
 - all copies
 - securely
 - logging what was done and
 - obtaining certificates of destruction

HOW TO DESTROY

- Paper records
 - Incineration
 - Cross-cut shredding

- Electronic records
 - Degaussing
 - Grinding platters
 - Incineration
 - Shredding
 - Sanitizing overwrites-multiple overwrites using specialized software
 - Selective wipes-multiple wipes using specialized software

- Portable Media: CDs, disks, DVD, hard drives, tapes and USB drives
- Computers & Servers: desktops, PCs, laptops and file servers
- Backups



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia



Protecting privacy. Promoting transparency.

The way to destroy records depends on the record type

- The best way to destroy paper records is to
 - burn them or
 - use a cross-cut shredder (if it's not cross-cut, records can be reconstructed)
- There are several ways to destroy electronic records
 - Degaussing virtually eliminates the magnetic field to destroy data on magnetic media
 - Grinding hard drive platters
 - Incinerating
 - Shredding
 - Sanitizing Overwrites (this requires multiple overwrites using specialized software)
 - Selective Wipes are similar and would be done when you need to preserve some of the data on the media
- Portable Media includes CDs, disks, DVDs, hard drives, tapes and USB devices
- Computers and Servers include desktops, PCs, laptops and file servers
- and don't forget the media holding your backup data



Deletion of files just doesn't cut it

- Computers need to be wiped several times before they can be sold or re-used
- Paper and CDs and be destroyed with a cross-cut shredder to prevent reconstruction

OUTSOURCING

- The National Association for Information Destruction Canada
<http://www.naidonline.org/ncan/en/index.html>
- Accredited vendor
- Contract
 - Responsibilities
 - Safe collection of records
 - Safe destruction
 - Methods of security records pending destruction
 - Limited timeframe
 - Certificate of Destruction



You might decide to outsource destruction

- The National Association for Information Destruction provides excellent guidance
- Find a vendor that is accredited by them and
- have a contract with the vendor to outline
 - Responsibilities
 - Safe collection of records
 - Safe destruction of records
 - Methods of securing records pending destruction
 - Timeframe for destroying records and
 - Completion of a certificate of destruction

Check out the Forms Tab in the Privacy Toolkit for a customizable Certificate of Destruction you can use



- CDs look beautiful when used in craft projects but data on them should be destroyed first.
- And we all need to be responsible about how we destroy sensitive information.

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



PIPA SHORTS

BC's Personal Information Protection Act

QUESTIONS?
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