Tips for Developing Privacy and Security Policies

Policies are high level documents that guide operational procedures. They describe how the clinic protects personal information of staff, patients, and third party associates.

- Keep major topics in separate documents to make them easier to update. A policy can be quite short as long as it clearly sets expectations and is complete.
- Avoid repeating similar information in two different documents so only one needs to be updated when changes occur.
- Reference in the policy relevant supporting documents such as procedures or forms to enhance understanding.
- Consider using numbering system for efficient document management.
- Keep a master list of all privacy and security related policies and procedures. Ensure they are covered during staff orientation and refresher training.
- Indicate the version and/or last revision date on the document itself and on the master list to facilitate updates and annual reviews.
- Ensure all policies and procedures are easily accessible. Have paper copies available in case of a system outage.

Privacy Policy Describes	• The clinic's accountability for records access, correction, and complaints. • Principles for personal information collection, use, and disclosure including the purposes for collection and patient consent. • Administrative, physical, and technological safeguards. • Information retention and disposal. • Incident breach management. The *Doctors of BC Privacy Toolkit* provides **a template sample** to be adapted for use by clinics.	Related Forms: • Certificate of Destruction • Patient Consent • Confidentiality Agreements • Information Sharing Agreements *Privacy Breaches: Tools and Resources* published by the OIPC
Security Policy Describes	• User account management and role-based access protocols including granting and revoking access. • Password complexity and non-sharing requirements. • Administrative, physical and technological data, equipment and network protection protocols • Incident response plan. • Acceptable use of network, phone, internet, wireless, email and fax including prohibition of downloads.	Related Forms: • Software Update/Patch Log • System Performance Monitoring Log • User Access Update Form

DOCTORS TECHNOLOGY OFFICE

☎ 604-638-5841 ✉ DTOinfo@doctorsofbc.ca

www.doctorsofbc.ca/doctors-technology-office

DTO Doctors Technology Office
A GPSC initiative

BUILDING A SECURITY CULTURE IN PRIVATE PRACTICE

GPSC
General Practice Services Committee

DTO Doctors Technology Office
A GPSC initiative

CREATING A SECURITY CULTURE STARTS HERE

As each physician is a custodian of personal health information, a clinic must have only one most responsible physician for electronic medical records and other privacy and security decisions.

This physician takes a role of **Privacy Officer**. Complying with privacy legislation can be time consuming and the Privacy Officer may delegate responsibilities to an appointed Security Lead, another clinician, a staff member, or contractually

Employee Training

Employee training is an important foundation needed to build a culture of security at the clinic.

- Use policies and documented procedures as a starting point for on-boarding training.
- Combine the ongoing staff education with periodic (yearly) reviews of procedures and assessment of safeguards to promote a security culture.
- Use the evaluation of current practices as opportunity for refresher sessions.
- Welcome critique and use errors to improve quality and foster ongoing education.

Risk Assessment

Schedule ongoing (e.g. yearly) assessments of the clinic's safeguards. Use the *Clinic Self-Assessment Form* handout and/or the *Privacy Breach Checklist* to create checklists that will work for your clinic. Keep filled out checklists for your records.

Privacy/Security Breaches

To investigate and address privacy breaches, utilize the *Privacy Breaches: Tools and Resources* published by Office of The Information and Privacy Commissioner. It offers guidance, investigation checklists, and the Breach Management Policy template.

Documentation

- Ensure the clinic maintains a Privacy and Security Binder – see the *Essential Privacy and Security Documentation for a Private Practice* handout for details.
- Visit the DTO website and select Physician Office IT Security section from the side menu for information and generic samples of documents that can be quickly adopted for your clinic.
- Develop a *Privacy Policy* and a *Security Policy* at the minimum (see reverse page of this brochure for more information).