

## PRIVACY INFORMATION SHEET

### PITO Commitment to Protecting Privacy

PITO is committed to supporting physicians in adopting adequate and reasonable privacy and security safeguards to protect personal health information. Initiatives and strategies include:

- A PITO Master Standing Agreement (MSA) contract between the Province and the PITO-approved EMR service providers with stringent privacy and security requirements for the EMR functionality and ASP hosting services
- A PITO Privacy Working Group which identifies concerns and issues, and provides feedback and input from the BC Medical Association (BCMA), College of Physicians and practising physicians
- Several privacy implementation activities have been incorporated into the overall PITO support and implementation activities to support physician offices with their privacy enhancements
- Information sharing and collaboration with the College of Physicians and Surgeons of BC and the Office of the Information Privacy Commissioner of BC

### Privacy Legislation Overview

While there is no specific health information privacy legislation in BC, there is personal information privacy legislation that governs public and private bodies:

- The BC Freedom of Information and Protection of Privacy Act (FOIPPA) governs public bodies such as health authorities and government
- The Personal Information Protection Act (PIPA) governs private sector organizations such as medical practices and private labs.

### PITO Privacy and Security Requirements

- At all times, patient personal information is under the custody and control of the physicians including while stored at the ASP data centre.
- The Province does not have custody or control, nor any access to data stored in an ASP EMR unless the physician grants explicit consent pursuant to legislation or patient requests.
- Service providers cannot permit access to EMR data stored in the data centres by any party without the explicit knowledge and consent of the physician.
- Service providers are contractually obligated to protect the privacy of personal information and only have access to systems as authorized by physicians, and for the purposes of support and maintenance.

- Service providers may store and access patient personal information only under specific purposes and only within Canada. Support must also be from within Canada and performed by employees of Canadian entities.

## Application Service Provider (ASP) Model

- The Application Service Provider (ASP) hosts the EMRs in a professionally managed data centre on one or more servers within a secure and redundant environment.
- Reliable and appropriate access to the EMR occurs over the Private Physician Network (PPN)
- Access to the data centres are controlled contractually, as well as through physical, procedural and technical security measures.

## EMR Privacy and Security Safeguards

The introduction of EMRs does not change a physician's responsibilities for appropriately and ethically accessing patient information for the purpose of providing direct patient care. Protecting personal health information requires a combination of the following:

- Designation of a **Privacy Officer** for each practice
- **Physical security**
  - locked file cabinets, locked down workstations, printers in non-public areas, alarms
- **Technical security**
  - unique user IDs, passwords, encryption, firewalls, audit trails, role-based access controls
- **Administrative controls**
  - staff training, office policies and procedures, confidentiality agreements, contractual agreements with third parties, account management, patient privacy notices

## Important Privacy References

- PITO Privacy Guide – [www.pito.bc.ca](http://www.pito.bc.ca)
- College of Physicians and Surgeons of BC Data Stewardship Framework – [www.cpsbc.ca](http://www.cpsbc.ca)
- The BCMA 10 Steps to PIPA Compliance – [www.bcma.org](http://www.bcma.org)
- Office of the Information and Privacy Commissioner of BC – [www.oipcbc.org](http://www.oipcbc.org)