Step 1 – Be Accountable

Accountability in relation to privacy is the acceptance of responsibility to protect personal information. In order to demonstrate accountability and compliance with the *Personal Information Protection Act* (PIPA), organizations should have a comprehensive privacy management program.

The person responsible for structuring and managing a privacy management program is the organization's privacy officer. In a physician's practice, it is recommended that the physician act as the privacy officer. In a solo practice, the physician is the de facto privacy officer, while in a clinic or group practice, one physician should be designated as the privacy officer. The privacy officer is answerable to the College of Physicians and Surgeons and the Office of the Information and Privacy Commissioner.

The privacy officer must do the following to establish and maintain a privacy management program for the practice:

- Compile a personal information inventory that documents the types of personal information that the practice collects and how and where it is stored.
- Develop internal privacy policies and procedures in relation to the obligations of the practice under PIPA and monitor compliance with them.
- Ensure all service contracts and information-sharing agreements include adequate privacy protective provisions.
- Put systems in place for responding to access requests, requests for correction, and complaints from patients.
- Institute mandatory privacy training and education for physicians and staff.
- Use risk assessment tools to identify and mitigate privacy impacts of new initiatives or services that involve the collection, use or disclosure of personal health information.

This Toolkit includes guidelines that are a useful starting point in demonstrating accountability by formulating privacy policies and procedures in areas that present particular challenges from a privacy perspective. These topics include the following:

- Patient consent for collection and requirements to notify patients
- Administrative and physical security controls to protect medical records
- Technological security controls and role-based access for EMRs
- Using email or fax
- Photography, videotaping and other imaging
- Responding to a privacy breach

- Using and disclosing personal health information for secondary purposes such as research
- Protecting medical records outside the practice
- Protecting medical records when leaving the practice
- Retention and secure destruction of medical records
- Informing patients about the privacy management program and their information rights

Privacy officers may also wish to develop policies and procedures on other topics depending on the practice and the nature and volume of the personal information in its custody or control.

All components of a privacy management program should be reviewed and assessed by the privacy officer on a regular basis and revised as necessary. For example, the practice may need additional security controls or improvements to privacy training and education for employees.

For further information regarding a privacy management program and the responsibilities of a privacy officer, a guidance document entitled Getting Accountability Right with a Privacy Management Program is available on the website of the Office of the Information and Privacy Commissioner.