Ten Steps to Help Physicians Comply with PIPA

This section will:
• Identify the 10 essential steps that physicians in an office-based practice need to take in order to comply with PIPA.

Getting started is simple. Consider the following 10 steps to support compliance with the requirements under PIPA.

Step 1: Put someone in charge

Physicians' offices are responsible for the personal information under their control. Every medical practice must have a designated Privacy Officer accountable for helping patients understand how personal information is being managed and to be responsible for ensuring overall compliance with the Personal Information Protection Act (PIPA).

It is recommended that the Privacy Officer be a physician. This means that if the office is a solo practice, the solo physician is the *de facto* Privacy Officer. In a group practice, one of the physicians must be identified as having responsibility for this function.

The Privacy Officer must understand the following issues:

1. What kind of information is covered under PIPA.
2. What information is appropriate to collect from patients.
3. What circumstances information can be disclosed and to whom.
4. When consent from the patient is required and when it is not.
5. How patients can access their own records.
6. How patients can request corrections to their records.
7. What fees can be charged for access.
8. How to handle a privacy breach.
9. How to respond to privacy complaints.
10. What reasonable safeguards must be implemented commensurate with the level of risks to privacy.

The Privacy Officer is responsible for the practice's privacy policy (see Step 6 below) and for ensuring that procedures are fully implemented and working effectively. Key functions of the Privacy Officer include the following:

1. Developing and implementing policies and procedures to protect personal information.
2. Educating employees about privacy and security.
3. Ensuring that confidentiality agreements are signed.
4. Answering patients' questions about PIPA.
5. Responding to inquiries, complaints, and privacy breaches.
6. Responding to patients' requests for access.
7. Overseeing the office's privacy compliance.

The Privacy Officer and the physician delegating him or her are accountable to the BC College of Physicians and Surgeons and the Office of the Information and Privacy Commissioner for BC (OIPC) .

Step 2: Become familiar with PIPA's privacy principles

The Privacy Officer, physicians, and employees of the practice must familiarize themselves with PIPA's privacy principles. (See the section Ten Principles for Protecting Information in Physician Practices.)

Step 3: Review how the practice handles personal information

The first question to ask is, "What personal information does the practice collect and how does the practice currently manage it?" After that information has been gathered, these steps should be followed:

- Taking an inventory of the personal information the practice currently has.
- Identifying the information needs of the different functions within the practice.
- Identifying the current information practices (including why the practice collects, uses, and discloses personal information).

Step 4: Put information-handling practices to the test

Consider whether the information-handling practices meet PIPA obligations. If well-established ethical and professional principles are currently being applied to the management of patient information, it is unlikely that significant changes are needed. Develop a plan to overcome any deficiencies, starting with

the most problematic areas. These include how to handle the most sensitive personal information collected or of the information most vulnerable to improper use or disclosure.

Step 5: Implement changes

After assessing the information-handling practices, changes may need to be made to practices and systems (technological and otherwise). Regardless of the size of the practice, any person who collects, uses, or discloses personal information should be involved in the implementation of the privacy program and security plans. Complying with the privacy principles may require a change to some computer systems or how the practice physically stores information.

Step 6: Develop a privacy policy

PIPA requires physician practices to prepare and follow a privacy policy, which must also be available for patients and employees. Security measures must also be considered when developing and implementing a privacy policy. Staff who handle personal information in the medical practice should be consulted when developing the privacy policy, and the following considerations should be incorporated into it:

1. How information will be safeguarded by physical, technological, and organizational security measures.
2. How the practice will ensure that personal information is collected accurately, stored securely, and disposed of properly.
3. How patients will be notified of why the information is being collected.
4. How patients may request access or correction to their information.
5. How the privacy of employees' personal information will be maintained.

The CMA Privacy Wizard (www.cma.ca/privacywizard.htm) was designed in collaboration with the BCMA to allow physicians to create an office privacy policy in usually under 20 minutes while earning CME credits. This privacy policy would, when posted in the office or distributed as a pamphlet, explain to patients why personal information is being collected; how it will be used, disclosed, and protected; and what their rights are. It will also provide staff, locum physicians, and physicians-in-training with clear responsibilities and expectations.

Step 7: Ensure compliance of staff and third parties

It is the staff, who will be responsible for complying with the policies on a patient-by-patient, day-to-day basis, and they must be aware of their obligations and expectations. A comprehensive privacy program

should include educating staff about privacy policies and procedures. Remember: staff education is essential to success.

The practice is also responsible for ensuring that third parties (e.g., associates, locums, visiting specialists, physicians-in-training, contractors, volunteers, partners, or agents with whom the practice collects, uses, or discloses personal information) know the privacy policies, and if appropriate, sign a confidentiality agreement. (See the sample Confidentiality Agreement for Employees of a Physician Office and the Confidentiality Agreement for Third Parties.)

Step 8: Develop and revise forms and communications materials

Review and revise forms, brochures, handouts, website content, and any other communication material to comply with PIPA, and inform patients about the office's privacy policy and information practices. A patient's implied consent to collect, use, and disclose personal information for medical treatment and continuity of care can be relied on, but it is recommended that notice of this policy be given to patients at the time the information is collected. (See the sample patient handout Our Privacy Policy that can be generated by using the CMA Privacy Wizard.)

Step 9: Review and revise contracts

The medical practice is responsible for personal information in its custody as well as under its control. This includes personal information that has been transferred for processing to a lab, for example, or information that a third party may have collected on the practice's behalf. To ensure that this personal information is properly protected, contracts should clearly require third parties to comply with PIPA and any policies that have been developed to properly manage personal information. Contracts should specify the purpose for which the third party is allowed to use the personal information and prohibit any other use or disclosure. (See the Confidentiality Agreement for Third Parties.)

Step 10: Develop an effective complaints handling process

PIPA requires that a process for handling privacy complaints be created. It is always more efficient to resolve complaints through the Privacy Officer than to involve an outside regulator (e.g., the College of Physicians and Surgeons of BC, and, failing a successful resolution, the Office of the Information and Privacy Commissioner for BC (OIPC)). Having an effective complaints-handling process is an important part of managing privacy risks within a practice.