Legislative Framework for Privacy in the BC Health Care System

This section will:

- summarize the private sector privacy legislation in BC that applies to physicians in private practice and private health care organizations: *Personal Information Protection Act [SBC 2003 c 63] (PIPA)*
- explain the requirements related to patient consent
- summarize the public sector privacy legislation in BC that applies to public bodies, such as health care organizations, health authorities, professional regulatory bodies, ministries and other government agencies:
    - *Freedom of Information and Protection of Privacy Act [RSBC 1996 c 165]. (FIPPA)*
    - *E-Health Act*
- Explain the:
    - difference between PIPA and FIPPA
    - role of the Information and Privacy Commissioner for BC
    - difference between Electronic Medical Records (EMRs) and Electronic Health Records (EHRs)
    - provision of collaborative care and use of EHRs

Privacy in the BC Health Care System

Personal health information is one of the most sensitive types of personal information because it encompasses the physical, mental and emotional status of individuals over their lifetime. It is used for a number of purposes, including patient care, financial reimbursement, medical education, research, social services, quality assurance, risk management, public health regulation, litigation and commerce.

Protecting patients' personal health information is a priority for physicians because it is fundamental to maintaining the physician-patient relationship. When seeking medical care, patients disclose their personal health information because they trust their physician to protect their privacy. If patients do not have confidence that their physician has adequate safeguards in place to protect their personal health information, they may refrain from disclosing critical information, refuse to provide consent to use personal health information for research purposes or not seek treatment. Such behavior was illustrated in a Canadian Medical Association (CMA) survey, which found that 11% of the public withheld information from a health care provider due to concerns about whom it would be shared with or what purposes it would be used for.

Patients are also concerned about wrongful release of information to third parties, which may result in harm to themselves. The Supreme Court of Canada has validated this concern and recognized it in the *Canadian Charter of Rights and Freedoms*:

- Section 7 includes the right to be free of the psychological stress resulting from the unauthorized disclosure of one's personal health information.
- Section 8 includes the right to be free from unreasonable search and seizure, including where police authorities request information from a physician about a patient without a warrant, subpoena, court order or other legal authority.

Physicians are governed by the professional requirements as set out in the *Health Professions Act*, the College of Physicians and Surgeons of BC Bylaws, relevant professional standards and guidelines of the College of Physicians and Surgeons of BC, and the CMA Code of Ethics.

For physicians who work within public health care organizations such as hospitals, health authorities, and the BC Ministry of Health, the protection of, and individual's access to, personal information is governed by FIPPA, as well as the applicable requirements of the College of Physicians and Surgeons.

Privacy and security in the health care system today must balance two competing social benefits, namely the need to:

- appropriately access and share information to enhance care quality and safety and provide continuity of care
- implement reasonable safeguards to protect personal health information

Balancing these two needs presents challenges that can be met through a variety of measures ranging from administrative and personnel security safeguards (e.g., employee training, policies, confidentiality agreements) to technical solutions (e.g., role-based access control, auditing, authentication mechanisms, encryption). Implementing these measures will build and maintain public trust and confidence in the privacy and security of personal health information.

Adequately protecting personal health information is a complex undertaking within the context of requirements of privacy legislation, new information technologies (including EMRs and EHRs), new models for information sharing, collaborative teams, and contractual arrangements with service providers. But none of these factors, including the introduction of new information technologies, change the responsibilities of physicians to appropriately protect personal health information; nor do they eliminate the risks to personal health information. Rather, different methods for safeguarding personal health

information that is stored electronically must be considered and implemented. (Note that industry experience has shown that while the threat of hackers is viewed as a major security threat to electronic systems, most instances of privacy and security breaches occur within organizations by staff who have legitimate access but exceed their authorized limits).

BC's *Personal Information Protection Act* (PIPA)

PIPA applies to private organizations, including physician practices, and governs how personal information about patients, employees and volunteers may be collected, used, and disclosed.

PIPA came into force on January 1st, 2004, to govern the BC private sector—both for-profit and not-for-profit. Any organization to which PIPA applies is exempted from the federal legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), which applies only to a "federal work, undertaking, or business" as defined in Section 1 of that Act.

PIPA does not apply to personal information collected and stored by public health care organizations such as hospitals, health authorities and the Ministry of Health. Those entities are governed by FIPPA (see below).

PIPA applies to personal information. In this context, "personal information" means both information that can identify an individual (e.g., name, home address, home phone number, ID numbers) and information about an identifiable individual (e.g., physical description, educational qualifications, blood type). Personal information includes employee personal information, but not business contact information or work product information.

The core principle of PIPA relevant to physicians is that personal information should not be collected, used, or disclosed without the voluntary and informed "consent" of the individual. This principle is subject to limited exceptions. For example, consent is not required where the collection, use, and disclosure is:

- clearly in the interests of the individual and consent cannot be obtained in a timely way; or
- necessary for medical treatment of the individual and the individual is either unable to give consent or does not have the legal capacity to give consent

There are two types of consent: express and implied. Patients provide "express consent" when they agree, verbally or in writing to the collection, use or disclosure of their personal information for a particular purpose. Express consent is necessary for research purposes, education purposes, or other purposes that are not related to the patient's care. "Implied consent" on the other hand is deemed to be given

where the purpose of collection, use, or disclosure would be considered to be obvious to a reasonable person, and where the individual voluntarily provides the information. The collection, use and disclosure of personal information for direct health care purposes in BC is usually authorized by implied consent. Implied consent can also be provided by giving a patient the opportunity to "opt-out" (e.g. when informing the patient about a referral, you provide them with a reasonable time to decline).

Under PIPA, physicians have custody of the personal health information they have collected and physical control of the documents/electronic data. They are accountable for any privacy breach that occurs to personal health information in their custody and control, including any breach committed by an employee under their authority.

BC's *Freedom of Information and Protection of Privacy Act* (FIPPA)

In BC, public health care bodies such as hospitals, health authorities, and the Ministry of Health are subject to the privacy protective measures contained in FIPPA. FIPPA guarantees the right of individuals to gain access to and request correction of personal information collected about them by public bodies. It also prohibits the unauthorized collection, use, or disclosure of personal information by public bodies and requires that reasonable safeguards be put in place to protect personal information. FIPPA does not apply to personal information collected and stored in a physician's private practice, private laboratories or other private health providers as PIPA governs these organizations (see above).

FIPPA prohibits the disclosure of personal information outside of Canada as well as any access to such records from outside Canada by health authorities and other public bodies without express consent (except in limited circumstances). It also provides whistle-blower protections for individuals who report contraventions of FIPPA in good faith, including unauthorized disclosure and access as well as foreign demands for disclosure or access.

FIPPA permits public bodies to provide "foreign access" under certain circumstances, such as performing system and equipment maintenance or data recovery from out-of-country, or with consent, and subject to other conditions. The out-of-country access must be necessary and the information can only be accessed and stored outside of Canada for the minimum amount of time needed to complete the task.

Comparing PIPA and FIPPA

Physicians in private practice who are also providing services to a public health care body will generally be governed by PIPA with respect to the personal information collected, used and disclosed by the

private practice, and by FIPPA with respect to the personal information they collect, use and disclose in their capacity as physicians for the public health care body.

There are some notable differences between PIPA and FIPPA:

- PIPA does not restrict the storage of, or access to personal information from outside Canada. As long as privacy is sufficiently protected, data can be stored or accessed from outside Canada.
- PIPA requires consent for the collection, use, and disclosure of personal information. It is up to the organization to determine whether the form of consent is express (written or verbal opt-in) or implied (opt-out or deemed).
- FIPPA does not permit the collection, use and disclosure of personal information on the basis of consent to the same extent as PIPA; instead it operates on the principle of appropriate authority and "notification" for collection of information.

BC's E-Health Act

The BC *E-Health (Personal Health Information Access and Protection of Privacy)* Act was enacted to provide legislative authority and a privacy framework to protect personal health information contained in designated health information banks (HIBs) of the Ministry of Health or health authorities. The Provincial Laboratory Information Solution, the Client Registry/Enterprise Master Patient Index and the Provider Registry are examples of HIBs. The E-Health Act includes the following provisions:

- allows individuals to issue disclosure directives to block access to (or "mask") some or all of their personal health information stored in HIBs
- prohibits disclosure of personal health information from a HIB for market research purposes
- establishes a Data Stewardship Committee (DSC) made up of representatives of health authorities, health professions including Doctors of BC and the College of Physicians and Surgeons and the public to evaluate data access requests for research purposes
- permits patient contact information to be disclosed for the purposes of recruiting individuals to participate in health research, but only with the prior approval of the Information and Privacy Commissioner
- adds new whistle-blower protection to protect individuals who report privacy breaches to the chief data steward or the Information and Privacy Commissioner and to encourage good faith reporting to enhance privacy protections
- establishes penalties for privacy and security breaches in the HIB (the penalty for a privacy breach in HIBs is a "fine of up to $200,000")

There is a patchwork of other health laws that apply to specific types of personal health information. The following Acts may apply depending on the context: Continuing Care Act (s. 5)

- *Continuing Care Act* (s. 5)
- *Health Act* (ss. 9 and 10)
- *Hospital Insurance Act* (s. 7)
- *Pharmaceutical Services Act* and the Information Management Regulation
- *Public Health Act*
- Health Act Communicable Disease Regulation

Role of the Information and Privacy Commissioner for BC

Monitoring compliance with BC privacy legislation (FIPPA and PIPA) is the responsibility of the Information and Privacy Commissioner, who is an independent officer of the BC Legislature.

If patients or employees have concerns related to privacy and security of their personal information, they can contact the Office of the Information and Privacy Commissioner (OIPC) for British Columbia at info@oipc.bc.ca. Also, if patients or employees are dissatisfied with how their privacy complaint was addressed by the practice or the College of Physicians and Surgeons, they can file their complaint with the OIPC.

More information on privacy and access to information rights in British Columbia, the role of the Information and Privacy Commissioner and privacy legislation in BC can be found at www.oipc.bc.ca.

EMRs vs EHRs: What is the Difference?

An EMR generally refers to an electronic version of the traditional paper-based medical record used within a private practice setting. The collection, use and disclosure of personal health information in an EMR is governed by PIPA. The EMR is a comprehensive record of health information compiled in the context of a direct patient-provider relationship and is under the custody and control of the physician providing primary care.

The terms EMR and EHR are often used interchangeably, although an understanding of the distinctions between the two has improved as a result of a number of eHealth related initiatives in progress within BC and across Canada.

Canada Health Infoway defines an EHR as “a secure and private lifetime record of an individual’s health and care history, available electronically to authorized health care providers”. The EHR is generally a compilation of core data from multiple and diverse sources submitted by different providers and health care organizations, and potentially from different jurisdictions. An EMR can be a potential source of core data that may be automatically shared or uploaded to an EHR. The objective of an EHR is to provide authorized health care providers with timely access to relevant portions of a patient’s electronic record when they need it to provide care, regardless of where a patient presents. An EHR may also have a patient portal whereby patients can access their own records on-line.

EMRs and EHRs both offer considerable opportunities for improving patient care, safety, and health outcomes, including ways to improve efficiencies and cost-savings in the provision of care. While numerous benefits are evident in EMRs and EHRs, they present similar challenges in terms of meeting the expectations of patients and protecting personal health information

A province-wide EHR has not yet been fully implemented, but there are a number of provincial repositories for personal health information already in place. These include PharmaNet, the Provincial Lab Information System, the Panorama public health information system as well as the Client and Provider Registries. Various EHRs have been implemented in health authorities. The governance of those EHRs rests with the health authorities governed under FIPPA.

Collaborative Care and EHRs

In BC there are new and evolving models for where and how physicians work, such as primary care networks, integrated health networks, specialty-related medical groups working in association and medical clinics within health authorities. With such new forms of practice and with institutional or provincial EHRs, the sharing of personal health information is now broadened beyond what is customarily understood by a patient to be included in their circle of care. In patient-centric institutional or provincial EHRs, personal health information from a broad range of sources and providers can be shared with and accessed by others. Adding further complexity is the potential for secondary uses of personal health information by persons or organizations beyond the circle of care.

With varying amounts of information-sharing, models for patient consent will vary depending on the situation, and it is not possible to establish guidelines that fit all scenarios. The interplay between PIPA and FIPPA is complex, and it is important that information-sharing meets the requirements of both pieces of legislation. Tools such as obtaining consent, role--based access, opt out, masking, and audits can be

used to protect patient privacy while sharing information appropriately and efficiently to support the delivery of care.