Privacy and Security in the BC Health Care System Today

This section will:
• Summarize the privacy legislation in BC that applies to physicians in private practice (PIPA) and the requirements related to patient consent. • Summarize the privacy legislation in BC that applies to health care organizations and government (FIPPA and e-Health Act). • Explain the difference between PIPA and FIPPA. • Explain the role of the BC Information and Privacy Commissioner. • Identify key elements of physician compliance with data stewardship requirements. • Introduce key notions on data stewardship (paper and electronic) for physicians relating to both information in their practice and information shared outside their practice. • Explain the difference between Electronic Medical Records (EMRs) and Electronic Health Records (EHRs).

Privacy and Security in the BC Health Care System Today

Health information is one of the most sensitive forms of personal information. Health information 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 commercial concerns.

Both privacy and security of personal health information are major concerns for physicians because both are fundamental to the confidentiality and trust of the physician-patient relationship. If patients do not have the confidence that their privacy will be maintained, or that reasonable security safeguards will be in place to protect their information, they may do things to protect their privacy on their own (such as 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 1999 Canadian Medical Association (CMA) survey, which found that 11% of the public held back 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 the patients. The Supreme Court of Canada has recognized that Section 7 of the Canadian Charter of Rights and Freedoms includes the right to be free of the psychological stress resulting from the unauthorized disclosure of one's personal health information.

Physicians are governed by the professional requirements in the CMA Code of Ethics (see cma.ca) and the regulatory standards in the College of Physicians and Surgeons of BC Data Stewardship Principles (see www.cpsbc.ca). In addition, for private practice physicians, including their employees and staff, obligations concerning the privacy of information are enforced by the Personal Information Protection Act (PIPA) (see below). This BC Physician Privacy Toolkit focuses on physicians' responsibilities under PIPA.

For physicians who operate within public health care organizations, such as hospitals, Health Authorities, and the health ministries, the applicable privacy protection measures are contained in the Freedom of Information and Protection of Privacy Act (FIPPA or FOIPPA; see below).

Privacy and security in the health care system today must balance two competing social benefits: the need to appropriately access and share information to enhance care quality and safety and provide continuity of care, and the need to implement reasonable safeguards to maintain the privacy of personal health information. Balancing these two needs presents a challenge, one 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., roles-based access control, auditing, authentication mechanisms, encryption). Implementing these factors will build and maintain public trust in the privacy and security of personal health information.

Adequately protecting personal health information is a complex process within the context of a patchwork of privacy legislation, new information technologies (including Electronic Medical Records (EMRs) and Electronic Health Records (EHRs)), new models for information sharing, collaborative teams, partnerships, and mergers. But none of these factors, including the introduction of new information technologies, change the responsibilities of physicians to appropriately protect patient information; nor do they eliminate the risks to patient information. Rather, different methods for safeguarding personal 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.)

BC's Personal Information Protection Act (PIPA)

The Personal Information Protection Act (PIPA) applies to private physicians' offices and governs how personal health information of 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 health ministries. Those entities are instead governed by the Freedom of Information and Protection of Privacy Act (FIPPA, see below). As well, PIPA **does not** apply to information to which FIPPA applies or information in the custody or control of a federal undertaking, to which the federal private sector privacy legislation (PIPEDA—Personal Information Protection and Electronic Documents Act) applies.

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). As well, personal information includes employee personal information, but **not** business contact information, work product information, or anonymous/aggregate information.

The core principle of PIPA that is relevant to physicians is that personal information should not be collected, used, or disclosed without the prior knowledge and consent of the patient, which may be implicit. This principle is subject to limited exceptions. For example:

- Where the collection, use, and/or disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way.

- Where the collection, use, and/or disclosure is 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.

Under PIPA, the consent for collection, use, and disclosure of personal information for direct health care purposes in BC operates primarily on an "implied consent" model. This means that those individuals who form part of a patient's "circle of care" (e.g., specialists, referring physicians, lab technologists) can access, use, disclose, and retain patient information for the purposes of ongoing care and treatment.

However, implied consent must be informed, and physicians should provide adequate information to patients on how they manage the privacy of patient information (see the section, Ten Steps to Help Physicians Comply with PIPA, and the handout Privacy of Your Personal Health Information). Implied consent is signified by a reasonable individual accepting the collection, use, and disclosure of information for an obvious purpose where it is understood that the individual will indicate if he or she does not accept (the "opt-out" model). For implied consent to be meaningful, the individual has to know that he or she has the right to expressly withhold or withdraw consent at any time without fear of retribution.

Expressed consent from a patient is required when identifiable personal information is intended to be collected, used, or disclosed outside of the circle of care, or for secondary purposes such as research (see the section Secondary Use of Personal Information for Research). Expressed consent is signified by the individual willingly agreeing to the collection, use, and disclosure of personal information for a defined purpose (the "opt-in" model). The consent can be given verbally or in writing.

Under PIPA, physicians have custody of the personal health information that they have collected and physical ownership of the documents/electronic data. They are accountable for any privacy breach that occurs to patient information in their custody and control, including any breach committed by an employee under their authority. The individual patient has the right to control, with limited exceptions under Section 18 of the Act, the collection, use, and disclosure of that data.

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

In BC, public health care organizations such as hospitals, Health Authorities, and the health ministries are subject to the privacy protection measures contained in the Freedom of Information and Protection of Privacy Act (FIPPA, also referred to as FOIPPA). FIPPA guarantees the right of the public to gain access

to and request correction of personal information collected about them by public bodies and prevents the unauthorized collection, use, or disclosure of personal information by public bodies. It also requires that reasonable safeguards be in place to protect personal information. FIPPA **does not** apply to personal information collected and stored by private physician offices, private laboratories, or other private health providers. The BC Personal Information Protection Act (PIPA, see above) governs these entities.

An amendment to FIPPA, Bill 73, was brought into effect in 2004 and prohibits the disclosure of personal identifiable information outside of Canada as well as any access to such records from outside Canada without explicit consent (except in limited circumstances). Under whistle-blower protection, individuals are expected to report unauthorized disclosure and access as well as foreign demand for disclosure or access.

Bill 30, which was introduced in 2006, amends some aspects of Bill 73. It permits "foreign access" under certain circumstances, such as out-of-country system and equipment maintenance and data recovery, but only under strict 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 to complete the task. It must also be under tightly controlled and secure circumstances.

Comparing PIPA and FIPPA

There are some notable differences between PIPA and FIPPA:

- PIPA does not include the FIPPA provisions regarding storage and access to personal information from outside Canada. As long as privacy is contractually protected, it does not matter where the data is or where it is accessed from.
- PIPA excludes business contact information from the definition of personal information.
- 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 expressed (written or verbal) or deemed (implied).
- FIPPA does not contain consent requirements; instead it operates on the principle of “notification” for collection of information.

BC’s e-Health Act

The BC e-Health Act (Personal Health Information Access and Protection of Privacy Act) received Royal Assent on May 29, 2008. It was introduced to provide legislative authority and a privacy framework to protect personal health information collected in designated Health Information Banks (HIBs) by public bodies such as the Ministry of Health Services or BC Health Authorities. HIBs are the underlying data repositories that will support information access and sharing in the provincial Electronic Health Record (EHR). The e-Health Act does not override FIPPA, but supplements its provisions with the following new regulations:

- Allows individuals to issue disclosure directives to block access to (or "mask") some or all of their personal information stored in HIBs.
- Prohibits disclosure of information from an HIB for market research.
- Establishes a Data Stewardship Committee (DSC) made up of members from the health authorities, health professions including the BCMA and College of Physicians and Surgeons, and the public to evaluate requests for secondary access of information in the EHR.
- Permits patient contact information to be disclosed for the purposes of asking individuals to participate in health research, but only with the specific approval of the BC Information and Privacy Commissioner.
- Adds new whistle-blower protection to protect individuals who report privacy breaches to the chief data steward or the privacy commissioner and to encourage good faith reporting to enhance privacy protection.
- Establishes penalties for privacy and security breaches in the EHR. The penalty for privacy breaches in HIBs is a fine of up to $200,000.

Role of the BC Information and Privacy Commissioner

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

If patients have concerns related to privacy and security of their information, they can contact the Office of the Information and Privacy Commissioner (OIPC) of British Columbia at www.oipc.bc.ca. Also, if patients are unsatisfied with how their privacy complaint was addressed by the physician's practice and by the BC College of Physicians and Surgeons, they can escalate their complaint to the OIPC.

More information on the role of the Information and Privacy Commissioner for BC and privacy legislation in BC can be found at www.oipc.bc.ca.

Data Stewardship and Physician Compliance

As the traditional practice environment evolves, physicians should regularly evaluate and update their practice's data stewardship framework and related policies on accountability, information management, and privacy. This includes, but is not limited to, the following:

- Reviewing and revising policies, processes, and procedures related to the collection, use, and disclosure of personal health information within the practice and with associated health care professionals.
- Reassessing regularly if information collected is truly required and what the minimum requirement is to satisfy the intended uses.
- Managing all aspects of patient information including orders, results, reports, and managing referrals and consultations.
- Appropriately using information accessed from external electronic health records or systems and determining what should be recorded in the physician medical record.
- Ensuring that contractual agreements with appropriate privacy provisions are in place with service providers engaged to implement and support the EMR or EHR.
- Ensuring that any submission of personal information to a third party is done:
    - With respect to requirements of patient consent and privacy legislation and under an information-sharing agreement (ISA) whenever appropriate.
    - With an understanding of the intended uses of the data prior to submission of such data and what controls are in place to control access (e.g., roles- and needs-based access model).
    - After examination of whether it is truly required and what the minimum requirement is to satisfy the intended uses.
    - With a secure protocol for data transfer including encryption whenever possible.
    - With assurance that the other party has acceptable privacy and security policies and practices in place.

Individuals own their personal health information, and physicians act as data stewards, which means that physicians are responsible and accountable for the personal information they collect, use, and disclose.

This responsibility is enforced through specific obligations under the BC Personal Information Protection Act (PIPA).

The College of Physicians and Surgeons of BC with representation from the BC Medical Association created a Data Stewardship Framework in May 2007 to describe how physicians can meet the requirement to protect the integrity of a patient's medical information in both the paper and electronic contexts. The BC Physician Data Stewardship Framework can be accessed from the College website (www.cpsbc.ca).

Data Stewardship within a Physician Practice: Paper Records and Electronic Medical Record (EMRs)

The traditional provider-centric model of data stewardship is one where a physician practising in a clinic environment maintains a medical record of care provided to an individual patient. That medical record can be in paper or electronic form, but the principles of physicians' data stewardship remain the same.

The Electronic Medical Record (EMR) generally refers to an electronic version of the traditional paper-based patient record used within a medical practice setting. The EMR is a comprehensive record of health information compiled during a direct patient-provider relationship and is under the stewardship of the physician providing primary care.

The physician manages the relationship with the patient as well as with others involved in the patient's circle of care. Within the practice setting, the physician is responsible for complying with applicable legislation governing personal information in addition to the professional and ethical duties in maintaining the confidentiality of patient information. This includes obtaining appropriate consent; managing the practice for collection, use, and disclosure of patient information; allowing patients access to their own personal information; correcting personal information; and securely retaining personal information. For information on how to implement these requirements, see the section Ten Steps to Help Physicians Comply with PIPA.

Data Stewardship and Information Sharing outside of a Physician Practice: Collaborative Care and Electronic Health Records (EHRs)

Many current trends are transforming the traditional model of trust between physicians and other health professions in the sharing of information for continuity and quality of care. These include collaborative care teams, integrated health networks, and the shift to Electronic Health Records (EHRs).

Canada Health Infoway defines an Electronic Health Record 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. The EMR can be a 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. The EHR can also allow patients access to their own records on-line.

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 practices geographically located within Health Authority regions. With such new forms of practice and with institutional or provincial EHRs, the sharing of personal 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, 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 electronic health information by persons or organizations beyond the circle of care.

With varying levels 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 physician offices governed under PIPA and public organizations governed under FIPPA is complex, and provincial collaboration is underway to define appropriate information-sharing that also meets the requirements of both pieces of legislation. Combinations of several tools (such as obtaining consent, roles- and need-based access, opt out, masking, disclosure directives, and auditing) are being used or implemented to best meet the needs of protecting patients' confidentiality and rights while sharing information appropriately and efficiently.

Establishing robust roles-based access is possible particularly in the information technology environment. The objective of a roles-based access model is to identify all possible roles that require access to patient

health information, to which a standard set of patient information (e.g., lab results, medication information, registration information) and permissions (e.g., reading, writing, printing) can be assigned. Defining this model also allows for ease of account management when setting up new users and modifying accounts. Roles-based access models must be designed to support both business and clinical workflow and, therefore, the software must have the flexibility to support the unique needs of each provider. It must also allow for exceptions to the standard roles and permissions as long as they are authorized and necessary for the performance of job duties. (See the section Electronic Medical Records and Roles-Based Access.)

Roles-based access has great potential to strengthen the trust of patients by ensuring appropriate access to the patient record. However, roles-based access needs also to integrate a "need to know" principle, based on a legitimate relationship with the patient. Unfortunately, "need to know" often becomes "want to know", so it is necessary to always consider the degree to which access to the personal information is truly needed to perform a given role's duties.

Physicians as primary custodians must maintain the responsibility for stewardship of patient information that they collect, use, and disclose. While technology is changing and influencing the future of health care, data stewardship remains a professional responsibility and not a technology issue.[1] If asked to transfer information to a public health organization or to government, physicians must consider all those issues identified above in the section Data Stewardship and Physician Compliance.

EMRs vs. EHRs: What is the Difference?

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.

Both systems offer considerable opportunities for improving patient care, safety, and health outcomes, and both can assist health care planners in finding ways to improve on efficiencies and cost-savings. While numerous benefits are evident in EMRs and EHRs, both present similar challenges in terms of meeting the expectations of patients and protecting personal information privacy. Understandably, with the consolidation of patient information available electronically and the potential for access to that

[1] Data Stewardship Framework, Committee on Privacy and Data Stewardship, BC College of Physicians and Surgeons, July 31, 2007.

information by unauthorized persons, there are specific privacy considerations related to the following topics (each cross-referenced to various sections within this Toolkit):

- Data stewardship and accountability (see the section Privacy and Security in the BC Health Care System Today).
- Consent for collection, use, and disclosure of personal information (see the section Consent and Disclosure Directives in BC).
- Secondary use for research (see the section Secondary Use of Personal Information for Research).
- Privacy and security of EMRs (see the section Privacy and Security Considerations for EMR Implementation).
- Appropriate access (see the section Electronic Medical Records and Roles-Based Access).
- Accuracy of personal information (see the section Guidelines for Ensuring Accuracy of Patient Records).
- Safeguarding personal information (see the section Protecting Patient Information in and outside of the Office).

The provincial EHR has not yet been implemented. It is anticipated that implementation will be incremental and staged over several years. However, within the various health authorities, EHRs have been implemented to varying levels. The governance of those EHRs rests with the Health Authorities regulated under FIPPA.

Currently, the policies on confidentiality of data contained within EMRs in private physicians' offices (regulated under PIPA), and particularly those policies impacting disclosure (i.e., the core data set and its components, disclosure directives, roles-based access, audit, breach policies, secondary use), have not been determined, and the implementation of the provincial EHR is conditional on those determinations, at least to the extent that implementation is to include private physicians' offices. Until that time, data from private physicians' EMRs can only be sent to consultants who share in a particular patient's care, to the extent that the data is relevant and under the implicit consent of the patient (by his or her agreement to the referral). In all other circumstances, explicit patient consent is required to disclose personal health information from the EMR.

These same constraints apply to any consortium of EMRs (e.g., community of practice initiatives), with the caveat that alternative processes (to those enabling the provincial EHR) may ultimately be engaged to

enable limited data exchange and, potentially, data sharing. One way to determine whether or not there are privacy issues related to a new information exchange, whether paper or electronic or both, is to evaluate the proposed exchange using a Privacy Impact Assessment (PIA). The PIA can then help determine whether any changes are required, including possibly the need to design and implement an information sharing agreement (ISA).