



Principles for the Protection of Patients' Personal Health Information

The Canadian Medical Association (CMA) Principles for the Protection of Patients' Personal Health Information are intended to provide physicians (including medical students and physicians in training) with a resource to highlight ethical and practical ways to protect patients' personal health information, including situations where legislation grants physicians discretion to collect, use and disclose personal health information without consent. The CMA recognizes that physicians are required to comply with applicable privacy law when dealing with their patients' personal health information. The Principles are not designed to serve as a tool for legislative compliance in a particular jurisdiction or provide a standard of care. Rather, the CMA wishes to provide physicians with guidance and a vision of what physicians might strive for to further their professional and legal obligations in a complex area. The Principles are relevant to physicians practicing in both the public and private sectors.

With the advent of shared electronic records (for example, in provincial/regional Electronic Health Record* (EHR) systems) the physician may not be the custodian of -

i.e., control access to - the patient's records once the health information is collected. Institutions, clinics and physician-group practices may also have responsibility for personal health information and therefore play an important role in ensuring personal health information is protected. The Principles therefore recognize that physicians' responsibilities as data stewards and custodians of health information must be assessed in the light of this framework. Where the term physician is used, it is meant to refer to the custodian of the medical record which in the case of institutions may not be the treating physician.

Foundational Privacy Principles.

Article 31 of the CMA's *Code of Ethics* (Revision 2004) states: Protect the personal health information of your patients.

1. Privacy, confidentiality and trust are cornerstones of the patient-doctor relationship.

Health information is highly sensitive and is confided or collected under circumstances of vulnerability and trust. Trust plays a central

role in the provision of health care and treatment; fulfilment of physicians' fiduciary obligations enables open and honest communications and fosters patients' willingness to share personal health information.

2. Patients have a general right to control the use and further disclosure of their personal health information, and a right of reasonable access to the information contained in their medical record.

The personal health information contained in the medical record belongs to the patient; patients retain an interest in what subsequently happens to it. Patients have a right of reasonable access to any personal health information in a medical record that was used for their care and treatment, regardless of whether the record is electronic or paper. Physicians may provide the patient with access to personal health information in a form that is accessible to the patient (*e.g.* paper or electronic). Patients generally have a right to request a correction of or addition to the information contained in the medical record and physicians may make the correction or addition if it is determined to be appropriate. Health information may be withheld from a patient if there is a significant likelihood of a substantially adverse effect on the physical or mental health of the patient or substantial harm to a third party.

There are circumstances when a physician must consider whether it is the parent or the child who should have control of personal health information. A young person who is deemed to understand fully the implications of a medical decision is generally also deemed to have control over their personal health information.

3. Physicians must handle personal health information in compliance with the applicable federal and provincial privacy laws and professional regulations.

Physicians may be required to comply with more than one privacy law when dealing with their patients' personal health information. Where there is uncertainty, physicians should seek advice from their professional liability protection provider (*e.g.* Canadian Medical Protective Association) and/or their Provincial Regulatory College.

4. Physicians play an important role in educating patients about possible consensual and non-consensual uses and disclosures that may be made with their personal health information.

Prior to the collection of health information, the patient should be informed through means such as websites, letters, posters, flyers or conversations that their personal health information (a) will be shared on a strict need-to-know basis with members of the health care team for the purpose of providing the necessary health care and treatment; (b) will be used to obtain payment for the health services provided; (c) may be used for health system planning and research; (d) may be disclosed to fulfill mandatory reporting obligations (*e.g.* fitness to drive, communicable diseases, *etc.*); (e) may be used or disclosed for other purposes where permitted or required by law (*e.g.* warrants, subpoenas, *etc.*) and (f) where possible, personal health information may be either de-identified or anonymized for any secondary purposes.

Patients should be encouraged as well to raise any concerns they might have about the uses and disclosures of their health information. Where physicians are not the primary

custodians of personal health information (for example in hospitals, multi-disciplinary clinics, or other group practices), such institutions should assist physicians in making these issues clear to patients.

5. Security safeguards must be in place to protect personal health information in order to ensure that only authorized collection, use, disclosure or access occurs.

Consent

6. Under certain circumstances, physicians may rely on a patient's implied informed consent to share personal health information.

Physicians may infer a patient's consent to collect, use, disclose and access personal health information for primary therapeutic purposes (*i.e.* for the purposes of direct patient care and treatment). Thus a physician may infer consent to (a) store personal health information in an electronic or paper medical record; (b) share the necessary personal health information with the appropriate members of the health care team.

7. The patient's *express* consent is generally required to disclose any part or all of the patient's personal health information in response to a third party request (*e.g.* insurance company, patient's lawyer) that is not directly related to the patient's health care or treatment. As discussed further in Principle 9 below, consent is generally not required where disclosure is permitted or required by law.

Patient consent is a fundamental concept in the provision of medical care. Patient consent to share information is crucial for the protection of the right to privacy and for the preservation of trust in the doctor-patient relationship. The principal purpose for the

collection of health information is to benefit the patient, who confides or permits information to be collected for this purpose.

Collection, use and disclosure

8. The use or disclosure of patient information within the "circle of care"*** should be done solely on a need-to-know basis.

This principle limits the sharing of personal health information with members of the health care team to only that information which is necessary for each team member, in accordance with their specific training, skills, responsibilities and terms of employment or other engagement, to provide the patient with direct health care and treatment.

9. Physicians may use or disclose personal health information without consent when it is required by law.

Patient consent is not required to permit physicians to fulfill mandatory reporting requirements such as the duty to report child abuse, fitness to drive, communicable diseases, *etc.* Patient consent is not required to disclose personal health information to regulatory authorities (Colleges) and billing audit agencies when the information is required by the College/agency to fulfill their respective mandates. Patient consent is not required to permit physicians to disclose personal health information in accordance with a warrant, subpoena, court order, or summons. Physicians must limit the personal health information that is disclosed to only that information which is necessary to fulfill the requirement. Physicians will want to consider if it is appropriate in the circumstances to advise the patient when a disclosure has been made.

10. Physicians may exercise discretion when the use or disclosure of personal health information without consent is permitted, but not required by law.

When privacy legislation permits the disclosure of personal health information without consent, physicians will want to exercise their discretion to ensure the disclosure is consistent with the duty of confidentiality or otherwise reasonable in the circumstances. For example, in some jurisdictions, medical officers of health may use personal health information for purposes related to the administration of a public health program or services prescribed in regulations. Given the number of factors involved in determining when it is appropriate to exercise discretion to use or disclose personal health information where permitted by law, physicians may wish to consider contacting their professional liability protection provider (e.g. CMPA) and/or Provincial Regulatory College for advice in these instances.

Physicians will also want to consider whether it is reasonable and/or preferable to obtain patient consent. There may be circumstances where it is not reasonable to seek patient consent, such as where the disclosure is required to avoid an imminent risk of harm to the patient or another person or where the disclosure is required to obtain risk management or legal advice. Physicians should limit the personal health information that is disclosed to that information which is necessary for the purpose. Physicians will want to consider if it is appropriate in the circumstances to advise the patient when a disclosure has been made.

11. Physicians should be aware of applicable requirements before collecting, using, or disclosing personal health information for research purposes.

Even if not required to do so by privacy legislation, physicians should obtain the approval of a properly constituted and informed research ethics board (REB) or review committee prior to collecting, using or disclosing patients' personal health information for research purposes without consent. ***

Retention

12. Personal health information should be retained at least for the period required by the provincial or territorial regulatory authority (College) or by any applicable legislation. It may be necessary to maintain personal health information beyond the applicable period where there is a pending or anticipated legal proceeding related to the care provided to the patient.

Physicians should retain, transfer and dispose of records in a safe and secure manner, in accordance with the requirements specified by their regulatory authorities and any applicable legislation.

Electronic Records*

13. Patients should be informed that the treating physician cannot control access and guarantee confidentiality for an electronic health record (EHR) system.

Every institution with a role to play in the EHR environment (e.g. health authorities, hospitals, clinics and governments) must play a part in educating patients and the public about the use of the EHR to store and share personal health information.

When transfer of patient health information to an interoperable (i.e. provincial or regional) EHR system is legislatively required, patients should be informed of this requirement.

Implementation of an interoperable EHR requires a strict privacy framework, including an access audit “trail” to safeguard against unauthorized access. Patients should be able to access this audit trail.

Patients and the public can be informed through means such as websites, letters, posters, flyers, conversations or public awareness campaigns that their personal health information will be included in an EHR. Options for protecting that information such as opt-out, disclosure directives, masking, or lock-boxes should be available and disclosed to patients.

Where possible, personal health information contained in an EHR should be de-identified before it is used for secondary purposes, such as health-system planning. Physicians may also wish to consult the Provincial Regulatory College in their jurisdiction as to whether patient consent might be required to upload a core segment of the EMR to an EHR.

14. Physicians may wish to consider entering into a Data Sharing Agreement to govern their participation in any shared electronic record (i.e. EMR/EHR)

The CMA and the CMPA have published Data sharing principles for Electronic Medical Record/Electronic Health Record agreements to provide guidance with respect to the main principles that should be addressed when a physician is entering into an agreement for an EMR, where multiple health care providers will have access to personal health information submitted by the physician.

The Data Sharing Agreement should address issues including but not limited to: confidentiality and privacy; security; accuracy

and data quality; record maintenance; quality assurance; and functionality.

***“Electronic health record”** is the health record of an individual that is accessible online from many separate, interoperable automated systems within an electronic network. It is maintained by a hospital, regional health authority or provincial/territorial government and typically includes a wider cross section of information from a number of sources.

“Electronic medical record” is essentially an electronic version of the paper record that doctors have long maintained for their patients. It may be a simple office-based system or a more sophisticated and interconnected system that links health professionals through a shared network.

** **“Circle of Care”** refers to those members of the health care team directly involved in the clinical care and management of the patient.

*** For further information on consent requirements and research, please refer to the CMA document “Research Guidelines: A web-based decision-guide for physicians”, available online at:
http://www.cma.ca/multimedia/CMA/Content/Images/Inside_cma/Ethics/Final_Toolkit_Research.pdf