ASSOCIATION MÉDICALE CANADIENNE | CANADIAN MEDICAL ASSOCIATION

CMA POLICY

PRINCIPLES FOR THE PROTECTION OF PATIENT PRIVACY

See also Background to CMA Policy Principles for the Protection of Patient Privacy

RATIONALE

Patients have a right to privacy and physicians have a duty of confidentiality arising from the patient-physician relationship to protect patient privacy. The right to privacy flows from the principle of respect for patient autonomy, based on the individual's right to conduct and control their lives as they choose.[1] When approaching any ethical question around privacy, the principle of respect for patient autonomy must be balanced against other competing principles (e.g. beneficence, non-maleficence).

The protection of privacy and the concomitant duty of confidentiality are essential to foster trust in the patient-physician-relationship, the delivery of good patient care and a positive patient care experience. Privacy protection is an important issue for Canadians,[2] and research suggests that patients may withhold critical health information from their health care providers because of privacy concerns.[3] Patients will be more willing to share complete and accurate information if they have a relationship of trust with their physician and are confident that their information will be protected.[4]

In today's ever-evolving technological environment and due to the shift away from the traditional (paternalistic) physician-patient relationship, patients, physicians and other public and private stakeholders are using and sharing personal health information in new and innovative ways. This raises new challenges for clinical practice and, crucially, how to navigate expanded uses of data via the use of new technologies and the requirements of patient privacy.

Institutions, clinics, and physician-group practices may share responsibility with the physician for the protection of patient information. There is thus a tension between physician and institutional responsibilities to protect patient information, challenged by the rapidly changing use and adoption of new technologies. While this will continue to redefine expectations of privacy and confidentiality, there are several foundational principles that remain unchanged.

SCOPE OF POLICY

The Canadian Medical Association (CMA) Principles for the Protection of Patients' Personal Health Information aim to provide guidance on key ethical considerations pertinent to the protection of patient information in a way that takes into account a physician's (including medical learner) ethical, professional, and legal obligations. The Principles are not designed to serve as a tool for legislative compliance in a particular jurisdiction or to provide a standard of care. Physicians should be aware of privacy legislation in the jurisdiction in which they practice, the standards and expectations specified by their respective regulatory authorities (including Privacy Commissioners), publications and risk management education provided by the CMPA as well as policies and procedures of any given setting (e.g., a regional health authority or a hospital).

SUBSTANTIVE PRINCIPLES THAT GUIDE THE OBLIGATIONS OF THE PHYSICIAN TO PROTECT PATIENT PRIVACY

1. Trust

- Trust is the cornerstone of the patient-physician relationship and plays a central role in providing the highest standard of care.
- Physicians and their patients build relationships of trust that enable open and honest dialogue and foster patients' willingness to share deeply personal information (often) in conditions of vulnerability.
- Physicians can cultivate and maintain patient trust by, unless the consent of the patient has been obtained to do otherwise, collecting health information only to benefit the patient, by sharing information only for that purpose, and by keeping patient information confidential; patient trust has been found to be the most powerful determinant of the level of control patients want over their medical records.[5]
- To maintain trust, physicians must consider the duty to care and the duty not to harm the patient in evaluating privacy requirements.
- The extent to which a patient expects (and may tolerate a loss of) privacy and confidentiality is culturally and individually relative.[6]

2. Confidentiality

- Physicians owe a duty of confidentiality to their patients; there is both an ethical (respect for autonomy) and a legal basis imposed by privacy legislation) for this duty.
- The duty to maintain patient confidentiality, like trust, is fundamental to the therapeutic nature of the patient-physician relationship; it creates conditions that allow patients to openly and confidently share complete health information, resulting in a stronger physician-patient relationship and better delivery of care.[7]
- The duty to maintain patient confidentiality means that physicians do not share the health information with anyone outside of the patient's circle of care, unless authorized to do so by the patient.[1,8] There are varying interpretations of what constitutes the patient's circle of care; this depends on the facts of the situation and the jurisdiction.[9]
- Privacy requirements raise complex issues in learning environments and quality improvement initiatives. It is desirable that any of the patient's physicians who will have ongoing care interactions with the patient can remain included in information-sharing about the patient.

- Shared electronic health records present challenges to confidentiality. For example, patients may wish to limit some aspects of their record to only some providers within their circle of care.[10]
- In practice, respecting privacy and the duty of confidentiality govern the physician's role as data steward, responsible for controlling the extent to which information about the person is protected, used or disclosed.[11] A central rule to balancing a patient's right to privacy and the duty of confidentiality is the "minimum necessary" use and disclosure of personal health information, whereby a data steward should use or disclose only the minimum amount of information necessary to fulfil the intended purpose. In some circumstances, de-identifying or aggregating personal health information before use or disclosure can minimize the amount of information disclosed.[12]
- The duty to maintain patient confidentiality is not absolute and is subject to exceptions in limited circumstances,[13] i.e., when required or permitted by law to disclose information (see below in *Data Stewardship: Collection, use and disclosure of personal health information*).

3. Consent

- Patient consent is an important mechanism for respecting patient autonomy; obtaining voluntary and informed consent to share patient information is fundamental to the protection of privacy and the duty of confidentiality.
- Physicians are generally required to obtain informed consent from the patient before they can disclose the patient's personal health information. Consent is only informed if there is disclosure of matters that a reasonable person in the same circumstances would want to know, including 1) to whom the patient information will be disclosed, 2) whether it could be disclosed to other third parties, and 3) the purpose for which it could be used or disclosed.
- While informed consent is required as a general rule, physicians may infer that they have the patient's *implied* consent to collect, use, disclose and access personal health information 1) for the purpose of providing or assisting in providing care (i.e., share only the necessary information with those involved within the patient's circle of care); and 2) to store personal health information in a medical record (i.e., paper, electronic, or hospital-based). Physicians will want to consider if it is appropriate in the circumstances to advise the patient when a disclosure has been made.
- When the patient is a minor, the physician must consider whether it is the parent or the child who determines the use and disclosure of the minor's personal health information. A young person who is deemed to understand fully the implications of a decision regarding proposed collection, use or disclosure of personal health information is generally deemed to have control over their personal health information with respect to the decision.
- Where the patient is not capable to provide the required consent (e.g. is deemed to be incompetent), physicians must seek consent from the patient's substitute decision-maker.

4. Physician as data steward

- As data stewards, physicians have the responsibility to understand their role in protecting patient privacy and appropriate access to patient information.

- The information contained in the medical record belongs to the patient who has a general right of access to their personal health information, and the right to control the use and further disclosure and to the continued confidentiality of that information.
- A data steward (e.g., physician, institution or clinic) holds the physical medical record in trust for the care and benefit of the patient.[14]
- Physicians should provide their patients access to their medical record, if requested.[15] (See below in *Data Stewardship: Access to personal information*).
- Physicians ought to have appropriate access to personal health information and have the ability to provide their patients with access to their medical record. Appropriate access should be interpreted to include access for patient follow up (as part of the duty to care) and review for the purpose of improving patient care.
- Physicians should consider consulting available resources to assist them in fulfilling their duties as data stewards.

PROCEDURAL PRINCIPLES THAT GUIDE THE APPLICATION OF PHYSICIAN OBLIGATIONS

Physicians must manage personal health information in compliance with relevant legislation that establishes rules governing the access, collection, use, disclosure, and retention of personal health information, provincial privacy laws, and professional expectations and regulations specified by their respective regulatory authorities.

1. Data Stewardship: Access to personal information

- Patients have a right of reasonable access to the personal health information in their medical record (i.e., paper, electronic, or hospital-based) under the control or in the custody of a physician, institution, or clinic.
- In exceptional situations, physicians can refuse to release the information in the patient's medical record.

2. Data Stewardship: Collection, use and disclosure of personal health information

- There are circumstances where there are *required* (e.g., monitoring of claims for payment, subpoenas) and *permitted* disclosures of personal health information without patient consent (e.g., where the maintenance of confidentiality would result in a significant risk of substantial harm to the patient or to others).
- Security safeguards must be in place to protect personal health information in order to ensure that only authorized collection, use, disclosure or access occurs.
- 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, including secondary uses of data for, e.g., epidemiological studies, research, education, and quality assurance, that may or may not be used with explicit consent.

3. Data Stewardship: Retention of personal health information

- Personal health information should be retained for the period required by any applicable legislation and as specified by their respective regulatory authorities. 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.

- Likewise, physicians should transfer and dispose of personal health information in compliance with any applicable legislation and professional expectations outlined by their respective regulatory authorities.
- Physicians are encouraged to seek technical assistance and advice on the secure transfer, disposal, and/or selling of electronic records.[15]

4. Data Stewardship: Use of technology

- Physicians should obtain patient consent to use electronic means and/or devices for patient care (e.g., sending digital photographs) and for communicating patient information (e.g., the use of email). To obtain informed consent, physicians should explain to patients that there are necessary benefits and risks in using technologies in clinical contexts. The CMPA has provided a written consent form to that effect that can be included in the patient's medical record.
- As a general practice, physicians are encouraged to make use of technological innovations and must evaluate whether the technology is appropriate for patient care and has reasonable safeguards to protect patient privacy.

Approved by the CMA Board of Directors December 2017
See also Background to CMA Policy Principles for the Protection of Patient Privacy

REFERENCES

[1] Martin JF. Privacy and confidentiality. In: ten Have H, Gordijn B (Eds). *Handbook of global bioethics*. New York: Springer, Dordrecht; 2014. p.119–37.
[2] Office of the Privacy Commissioner of Canada. *Canadians and privacy final report*. Gatineau: Office of the Privacy Commissioner of Canada; 2009. Available: https://www.priv.gc.ca/information/por-rop/2009/ekos_2009_01_e.asp (accessed 2017 Nov 17).
[3] Canadian Medical Protective Association (CMPA). *Privacy and a wired world – Protecting patient health information*. Ottawa: CMPA; 2011 Dec. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2011/privacy-and-a-wired-world-protecting-patient-health-information (accessed 2017 Nov 17).
[4] Royal College of Physicians and Surgeons of Canada (RCPSC). *Duty of confidentiality*. Ottawa: RCPSC; 2017. Available: http://www.royalcollege.ca/rcsite/bioethics/cases/section-3/duty-confidentiality-e (accessed 2017 Dec 15).
[5] Damschroder LJ, Pritts JL, Neblo MA, Kalarickal RJ, Creswell JW, Hayward RA. Patients, privacy and trust: patients' willingness to allow researchers to access their medical records. *Soc Sci Med* 2007;64:223–35.
[6] Campbell JI, Eyal N, Musiimenta A, Haberer JE. Ethical questions in medical electronic adherence monitoring. *J Gen Intern Med* 2016;31:338–42. Available: https://link.springer.com/content/pdf/10.1007%2Fs11606-015-3502-4.pdf (accessed 2017 Nov 17).
[7] Crook MA. The risks of absolute medical confidentiality. *Sci Eng Ethics* 2013;19:107–22.
[8] Cohen I, Hoffman A, Sage W (Eds). *The Oxford Handbook of U.S. Health Law*. New York: Oxford University Press; 2015.
[9] Canadian Medical Protective Association (CMPA). *The voice of professionalism within the system of care*. Ottawa: CMPA; 2012 Oct. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2012/the-voice-of-professionalism-within-the-system-of-care (accessed 2017 Nov 17).
[10] Canadian Medical Protective Association (CMPA). *Did you know? Patients can restrict access to their health information*. Ottawa: CMPA; 2017 Nov. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2017/did-you-know-patients-can-restrict-access-to-their-health-information (accessed 2017 Nov 17).
[11] Francis JG, Francis LP. Privacy, confidentiality, and justice. *J Soc Philos* 2014;45:408–31.
[12] Burkle CM, Cascino GD. Medicine and the media: balancing the public's right to know with the privacy of the patient. *Mayo Clin Proc* 2011;86:1192–6.
[13] Canadian Medical Protective Association (CMPA). *When to disclose confidential information*. Ottawa: CMPA; 2015 Mar. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2015/when-to-disclose-confidential-information (accessed 2017 Nov 17).
[14] Canadian Medical Protective Association (CMPA). *Releasing a patient's personal health information: What are the obligations of the physician?* Ottawa: CMPA; 2012 Oct. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2012/releasing-a-patient-s-personal-health-information-what-are-the-obligations-of-the-physician (accessed 2017 Nov 17).
[15] Canadian Medical Protective Association (CMPA). *Protecting patient health information in electronic records*. Ottawa: CMPA; 2013 Oct. Available: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2013/protecting-patient-health-information-in-electronic-records (accessed 2017 Nov 17).