

PRINCIPLES FOR THE PROTECTION OF PATIENT PRIVACY

See also [CMA Policy on Principles for the Protection of Patient Privacy](#)

Context

The advent of Electronic Medical Records, the rapid spread of mobile health apps, and the increasing use of social media within the health care community, have each created new challenges to maintaining a duty of confidentiality within the physician-patient relationship. These technologies present both opportunities and challenges with respect to medical professionalism.¹ The permeation of these types of interactions into everyday life now places physicians in new situations that some find difficult to navigate.² These challenges will only increase in the coming years, as the use of online technologies in health care is continuously growing.³ Canada is only in the early stages of managing the emerging issues of technology-induced errors that compromise privacy in the health care setting.⁴ Therefore, this paper will briefly discuss the importance of protecting privacy, followed by an overview of the main challenges to maintaining privacy as the physician-patient relationship evolves at the backdrop of emerging technologies.

Privacy and Confidentiality

The overlapping, but not identical, principles of the protection of privacy and the duty of confidentiality are essential to the physician-patient relationship. These principles not only foster trust, but also the delivery of effective and lasting care. Rooted in the Hippocratic Oath, the modern-day right to privacy flows from the principle of autonomy, which attributes to individuals the right to conduct and control their lives as they choose.⁵ Privacy protection is an important issue to Canadians,⁶ with research suggesting that patients may even withhold critical health information because of privacy concerns.⁷ Health care professionals are bound by legal and ethical standards to maintain privacy and confidentiality of patient information.⁸ Physicians must therefore be aware of the implications of privacy legislation specific to their jurisdiction.⁷ The duty to protect patient privacy is important to uphold, as health information can potentially be identifiable and sensitive; the confidentiality of this information must therefore be protected to ensure that patient privacy is not breached.⁹ While the traditional, and largely obsolete, models of the physician-patient relationship involve a unidirectional flow

of information, the ease at which patients can now access medical information through the Internet, and the use of social media within the health care community, have reinterpreted how information is communicated from physician to patient, and vice versa.¹⁰ We must therefore re-define expectations of privacy and confidentiality, first by distinguishing one from the other.

The terms “privacy” and “confidentiality” are often used interchangeably by both researchers and clinicians. Several bioethics discussions on the distinction between these terms places confidentiality under the umbrella of privacy.¹¹ While confidentiality involves the information itself, which is disclosed or not, privacy is about the impact of that disclosure on the person.⁹ Privacy seems to be more intimately linked to the individual, focusing on the circumstances under which the information is used.¹²⁻¹³ Confidentiality, on the other hand, is a duty that health professionals have towards their patients to not share the information exchanged during their encounter, unless authorized by the patient.^{5,12} In practice, the duty of confidentiality governs the physician’s role as data stewards, responsible for controlling the extent to which information about the person is protected, used or disclosed.¹⁴ As one paper describes, “privacy is invaded, confidentiality is breached.”¹³

From a patient perspective, it is important to respect and protect privacy because it allows individuals time and space to share their concerns without feeling judged or misunderstood,¹¹ resulting in a stronger physician-patient relationship and better delivery of care. However, from a research perspective, a fine balance must be struck between using accurate information while still upholding the privacy rights of individuals.¹¹ As such, the argument for absolute confidentiality puts a near impossible burden on research clinicians.¹¹ Moreover, from a public safety perspective, a physician may be morally and legally required to break confidentiality in order to protect both the patient and others who may be involved. The challenge is to balance the traditional goal of confidentiality – to protect patient privacy and interest – with that of third parties and public health.⁵ Therefore, a central rule to balancing confidentiality with a patients’ right to privacy 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.⁸ It is equally important to recognize that the extent to which a patient may tolerate a loss of privacy is culturally and individually relative.¹⁵ Health care providers have a legal and ethical obligation to keep patient health information private, sharing it only with the authorization of the patient.¹⁵ Informed consent, therefore, appears to be a fundamental requirement to upholding confidentiality and patient privacy rights.

Issues

While emerging privacy issues touch many areas of practice, this section will emphasize three of the most prominent issues in recent literature: access and use of information, electronic medical and health records and, online communication and social media.

1. *Technological change and institutional data stewardship*

In today's ever-evolving technological environment, including the emergence of shared electronic health records, online communication, social media, mobile applications, and big data, physicians, patients and other public and private stakeholders are using and sharing personal health information in new and innovative ways. The traditional (paternalistic) model of the physician-patient relationship involved a bidirectional flow of information. However, the ease at which patients can now access medical information from alternative sources via the Internet, and the use of social media within the health care community, has redefined how information is communicated from physician to patient, and vice versa.¹⁰ This raises new challenges for clinical practice, specifically how to navigate expanded access of data via the use of new technologies and the requirements of patient privacy by effectively managing security concerns.

In many situations, the physician may not be the sole or primary 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 patient information and therefore play an important role in ensuring it is protected. There is thus a grey area between physician and institutional responsibilities to protect patient information, challenged by the rapidly changing use and adoption of new technologies, such as electronic health and medical records. While this will continue to redefine expectations of privacy and confidentiality, there are several foundational principles that remain unchanged.

2. *Electronic medical and health records*

Medical records are compiled primarily to assist physicians and other health care providers in treating patients.¹⁶ Yet, they are particularly vulnerable to privacy breaches when this information is exposed to secondary uses, including epidemiological studies, research, education and quality assurance. As contemporary information management and stewardship have had to evolve in response to emerging technology, the parameters of the "medical record" have grown increasingly ambiguous.¹⁷ With the proliferation of a wide variety of new health information technology (including electronic health and medical records), concerns about quality and safety have been raised.⁴ There is evidence that if such technology is not designed, implemented and maintained effectively, it may result in unintended consequences, including technology-induced errors and breaches of patient privacy.⁴ Reports involving Canada Health Infoway have even pointed to health information technology as a tool that may sometimes reduce rather than enhance patient safety, most often due to human factors.⁴ As a result, recommendations have been made to develop a reporting system that would allow health professionals to anonymously report human errors resulting from the use of

health information technology – a challenge in itself, as the distinction between human and technological error is often blurred.⁴ In Canada, a number of efforts have been undertaken by several organizations, including Health Canada and Canada’s Health Informatics Organization.⁴ Yet, services aimed at improving health information technology safety, from a national level, remain poor.⁴ As a result, organizations like Canada Health Infoway have promoted the need for collaborative efforts to improve health information technology safety standards in Canada,⁴ so to ensure that the current and future uses of “medical record” data are accurate and respectful of patient privacy.

3. Access and use of personal health information for research

The courts have long established that health information belongs to the patient.¹⁸ As a result, privacy ownership refers to the belief that patients own their private information as well as the right to control access to this information.¹⁹ As in other jurisdictions, the overarching challenge in Canada is to strike a balance between enabling access to health and health-related data for research while still respecting Canadians’ right to privacy and control over the confidentiality of their information.²⁰ The integrity of healthcare information is fundamental, given that it is the basis on which treatment decisions are made both in research and in clinic.⁹ There are three principles upon which information security is based:⁹ 1) only authorized people have access to confidential information; 2) information must be accurate and consistent, may only be modified by authorized people in ways that are appropriate; 3) information must be accessible by authorized users when needed. Canadian research ethics have demonstrated that beneficial work can be done while maintaining confidentiality to sensitive personal health information.²⁰ Yet, the challenge remains to create a uniform system for accessing data and performing data-based research due to 1) the lack of consistency and clarity in Canada’s ethical and legal framework and, 2) varied interpretations of key terms and issues across the country.²¹ For example, the term “non-identifiable data” remains ambiguous across provinces and is subject to interpretation by data custodians, who may consider their legal duty to protect privacy as precluding access to data.²¹ This lack of legal clarity has contributed to varied cautious and conservative interpretations of data access legislation.²¹ National uniform guidelines on the appropriate access, disclosure and use of personal health data would allow data stewards to advance their research while respecting their patients’ right to privacy.

4. Online communication with patients and social media

Social media and online communication is pervasive in Canadian society; from Facebook to Twitter, social media has changed the way people interact and disseminate information.²¹ There is currently widespread discussion among health care professionals and academics regarding the role that social media and online communication should play in the physician-patient relationship.²¹ A growing number of physicians have embraced the opportunities of interconnectivity that social media affords, implementing their own privacy procedures to reflect this new type of data collection, use and storage.⁷ While evidence has been lacking on whether the use of social media does improve patient outcomes,²² there is no denying that patients are seeking health care information from online platforms, including social media.²¹ This type of communication poses a unique set of opportunities and challenges for

physicians: while the use of social media could increase physician reach and patient engagement, it can also blur boundaries between one's personal and professional life.²¹ Although patient-physician online communication is currently limited, physicians still feel that they are encountering an ethical dilemma, especially when they find themselves in boundary crossing situations, like a friend request from a patient.² Physicians are particularly concerned that, through online communication, they may be exposed to medico-legal and disciplinary issues, especially with respect to patient privacy.² Given different studies have suggested that unprofessional uses of social media are not uncommon,²³ physicians who choose to communicate with patients online or through social media must remember that they are still governed by the same ethical and professional standards that remain paramount.²¹

As technology continues to evolve, so too will the traditional parameters of the patient-physician relationship. The physician's ethical and professional obligation to protect patient privacy, however, must remain paramount at the backdrop of technology use. Simply banning social media and online communication would neither eliminate risk, nor benefit patient care outcomes.²⁴ Instead, institutions should establish stringent policies that outline how to prevent or minimize the effects of privacy breaches associated with social media and online communication.²⁵ This should also include a tracking mechanism to help balance the obligation to privacy with evolving technology.²⁴

December 2017

See also [CMA Policy on Principles for the Protection of Patient Privacy](#)

REFERENCES

¹ Farnan JM, Snyder Sulmasy L, Worster BK, Chaudhry HJ, Rhyne JA, Arora VM. Online medical professionalism: patient and public relationships: policy statement from the American College of Physicians and the Federation of State Medical Boards. *Ann Intern Med* 2013;158(8):620-627.

² Brown J, Ryan C. How doctors view and use social media: a national survey. *J Med Internet Res* 2014;16:e267. Available: <https://doi.org/10.2196/jmir.3589> (accessed 2017 Nov 17).

³ Lambert KM, Barry P, Stokes G. Risk management and legal issues with the use of social media in the healthcare setting. *J Healthc Risk Manag* 2012;31(4):41-47.

⁴ Kushniruk AW, Bates DW, Bainbridge M, Househ MS, Borycki EM. National efforts to improve health information system safety in Canada, the United States of America and England. *Int J Med Inform* 2013;82(5):e149-160.

⁵ Martin JF. Privacy and confidentiality. In: ten Have H, Gordijn B (Eds). *Handbook of global bioethics*. New York: Springer, Dordrecht; 2014. p.120-1.

⁶ 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).

⁷ 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).

⁸ 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.

⁹ Williams PA. Information security governance: a risk assessment approach to health information systems protection. *Stud Health Technol Inform* 2013;193:186-206.

¹⁰ Borza LR, Gavrilovici C, Stockman R. Ethical models of physician-patient relationship revisited with regard to patient autonomy, values and patient education. *Rev Med Chir Soc Med Nat Iasi* 2015;119(2):496-501.

-
- ¹¹ Crook MA. The risks of absolute medical confidentiality. *Sci Eng Ethics* 2013;19(1):107-122.
- ¹² Cohen I, Hoffman A, Sage W (Eds). *The Oxford handbook of U.S. health law*. New York: Oxford University Press; 2015.
- ¹³ Francis L. Privacy and confidentiality: the importance of context. *The Monist*; 91(1);2008:52-67.
- ¹⁴ Francis JG, Francis LP. Privacy, confidentiality, and justice. *J Soc Philos* 2014;45:408-31.
- ¹⁵ 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).
- ¹⁶ Canadian Medical Association (CMA). *Medical record confidentiality, access and disclosure*. Ottawa: CMA; 2000. Available: https://www.cma.ca/Assets/assets-library/document/en/advocacy/policy-research/CMA_Policy_The_medical_record_confidentiality_access_and_disclosure_Update_2000_PD00-06-e.pdf (accessed 2017 Oct 30).
- ¹⁷ Fenton SH, Manion F, Hsieh K, Harris M. Informed Consent: Does anyone really understand what is contained in the medical record? *Appl Clin Inform* 2015;6(3):466-477.
- ¹⁸ Canada. Supreme Court. *McInerney v MacDonald*. Dom Law Rep. 1992 Jun 11;93:415-31.
- ¹⁹ Petronio S, Dicorcia MJ, Duggan A. Navigating ethics of physician-patient confidentiality: a communication privacy management analysis. *Perm J* 2012;16(4):41-45.
- ²⁰ Council of Canadian Academies (CCA). *Assessing health and health-related data in Canada*. Ottawa: The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation, Council of Canadian Academies; 2015. Available: <http://www.scienceadvice.ca/uploads/eng/assessments%20and%20publications%20and%20news%20releases/Health-data/HealthDataFullReportEn.pdf> (accessed 2017 Nov 17).
- ²¹ Canadian Medical Association (CMA). *Social media and Canadian physician: Issues and rules of engagement*. Ottawa: CMA; 2011. Available: https://www.cma.ca/Assets/assets-library/document/en/advocacy/CMA_Policy_Social_Media_Canadian_Physicians_Rules_Engagement_PD12-03-e.pdf (accessed 2017 Oct 30).
- ²² Eysenbach G. Medicine 2.0: Social networking, collaboration, participation, apomediation, and openness *J Med Internet Res* 2008;10(3):e22.
- ²³ Mayer MA, Leis A, Mayer A, Rodriguez-Gonzalez A. How medical doctors and students should use social media: A review of the main guidelines for proposing practical recommendations. *Stud Health Technol Info* 2012;180:853-857.
- ²⁴ Moses RE, McNeese LG, Feld LD, Feld AD. Social media in the health-care setting: Benefits but also a minefield of compliance and other legal issues. *Am J Gastroenterol* 2014;109(8):1128-1132.
- ²⁵ Yang YT, Silverman RD. Mobile health applications: The patchwork of legal and liability issues suggests strategies to improve oversight. *Health Aff (Millwood)* 2014;33(2):222-227.