PATIENT PRIVACY IN A WIRED (AND WIRELESS) WORLD: APPROACHES TO CONSENT IN THE CONTEXT OF ELECTRONIC HEALTH RECORDS

NOLA M. RIES*

The author reviews recent changes in legislation in Canada and abroad in the area of patient privacy, consent and electronic health records (EHRs). In her overview of Canadian legislation, she examines the existing patchwork of legal requirements, as well as ethical obligations governing health information and policy initiatives aimed at harmonizing approaches across Canada. Internationally, the United Kingdom and Australia are reviewed on how those jurisdictions are addressing the issue of protecting patient privacy while developing operable EHR schemes. The author concludes that as EHR schemes develop, stringency of privacy and consent protections will likely wane in favour of establishing workable systems and, as a consequence, appropriate security mechanisms should be implemented to safeguard personal information.

L'auteure revoit les récents changements à la législation au Canada et à l'étranger sur la protection de la vie privée d'un patient, le consentement et les dossiers médicaux électroniques. En donnant un aperçu de la législation canadienne, elle examine l'ensemble de mesures disparates relatives aux exigences juridiques ainsi que les obligations éthiques régissant l'information médicale et les initiatives de politique visant l'harmonisation des approches à travers le Canada. Sur la scène internationale, elle examine comment au Royaume-Uni et en Australie certains ressorts abordent la question de la protection de la vie privée d'un patient tout en développant des schémas fonctionnels de dossiers médicaux électroniques. L'auteure conclut qu'au fur et à mesure que l'utilisation de dossiers médicaux électroniques prendra de l'ampleur, les mécanismes de protection et de consentement deviendront moins rigoureux pour faire place à des systèmes exploitables et, par conséquent, des mécanismes de sécurité appropriés devront être mis en place pour préserver l'information personnelle.

TABLE OF CONTENTS

* Nola M. Ries, M.P.A., LL.M., is a research associate with the Health Law Institute, University of Alberta and a lecturer in health law at the University of Victoria, Faculty of Law and School of Health Information Science. This article is based on research funded by the Office of the Privacy Commissioner of Canada and sections of this paper are drawn from a report, *Electronic Health Records and the Personal Information Protection and Electronic Documents Act*, that was the outcome of the project funded by the federal Privacy Commissioner. The author is indebted to Elizabeth Robertson for her extensive research assistance in regard to international experiences with electronic health records. Fiona Moore also very helpfully assisted with research. The author also thanks Professor Francis Lau, School of Health Information Science, University of Victoria, who was a collaborator on the project funded by the federal Privacy Commissioner. The author presented aspects of this research at the 10th Annual Seminar on Medical Law in Toulouse, France in June 2005.

"To err is human, to really screw things up requires a computer."[1]

I. INTRODUCTION

Electronic health records (EHRs) are a topic of much interest in contemporary health care, both in Canada and abroad. An EHR provides a comprehensive, lifelong record of an individual's health history, including diagnoses, treatments, test results and medications.[2] Health care providers and others in settings such as hospitals, private practitioner offices, laboratories and pharmacies access the record electronically and continually add new information to it. Some predict EHRs will enhance the effectiveness and efficiency of health care and play a key role in health system reform.

Yet, despite their potential benefits, EHRs raise many concerns regarding patient privacy and vulnerability to unauthorized access and security breaches. The quotation at the outset of this article expresses popular unease — and, perhaps, resignation — regarding the fallibility of computer systems, a concern that underlies hesitance to embrace EHRs. Many Canadians are concerned about their privacy; a March 2005 survey found that over 60 percent of respondents believe they have less personal privacy than they did a decade ago, almost three-quarters say strong privacy laws are important, and less than half are confident they have adequate information to understand how new technologies might affect their privacy.[3] A recent American survey revealed that 69 percent of respondents expressed concern that EHRs could lead to more sharing of personal information without patient consent and 70 percent feared that sensitive health care details are vulnerable to weak data security.[4] Based on concerns about the sensitivity of health information, much attention has focused on how to safeguard patient privacy and ensure confidentiality and security in an electronic health care environment.

In particular, many countries that are in the process of designing and implementing EHR systems are grappling with the extent to which individual patients should be able to control how (or even if) their information is collected, used and disclosed via EHRs. Debate has

---

1 "Your Morning Smile" *Globe & Mail* (18 February 2005) A2.

2 EHRs are distinct from electronic medical records (EMRs), which are patient records maintained and accessed by practitioners and staff within a specific health care office or facility.

3 EKOS Research Associates, *Canadians, Privacy and Emerging Issues*, report submitted to the Office of the Privacy Commissioner of Canada (10 June 2005), online: Office of the Privacy Commissioner <www.privcom.gc.ca/information/survey/ekos_e.asp#section2>. These results are based on a March 2005 telephone survey of 1,010 Canadians randomly selected across the country. The margin of error is +/-3.1 % points, 19 times out of 20.

4 Program on Information Technology, Health Records and Privacy, Center for Social & Legal Research, *How the Public Sees Health Records and an EMR Program* (16 February 2005), online: Privacy & American Business <www.pandab.org/Healthtopline.pdf>.

arisen in Canada and other jurisdictions about whether explicit patient consent is required before a patient's information is put onto an EHR and whether a patient should be able to limit who has access to their electronic records. Privacy is often described as a consent-based right, so, to respect privacy of personal health information, what consent rights should a patient have in regard to EHRs?

This article examines these fundamental consent questions in the context of EHRs. It begins with a brief overview of EHR development in Canada and summarizes benefits and concerns associated with EHRs. Next, key legal principles regarding privacy of personal information and consent in health care are discussed. Consent rules in several Canadian privacy laws are summarized, with particular focus on rules related to EHRs. Many international jurisdictions are developing large-scale EHR initiatives, so this article examines experiences in Australia and the United Kingdom, focusing specifically on how those jurisdictions are dealing with issues of patient privacy and consent. The article concludes with some recommendations for dealing with consent in the collection, use and disclosure of patient information in EHRs.

II. DEVELOPMENT OF ELECTRONIC HEALTH RECORDS IN CANADA

EHR systems are at various stages of development across Canada and jurisdictions are at different stages in developing components of province-wide EHRs, including client registries and networks for pharmaceutical, laboratory and diagnostic imaging information.[5] Nationally, Canada Health Infoway is a not-for-profit corporation that aims to promote "the development and adoption of electronic health information systems with compatible standards and communications technologies on a pan-Canadian basis, with tangible benefits to Canadians."[6] The Romanow Commission on the Future of Health Care in Canada recommended that "Canada Health Infoway should ... be responsible for developing a pan-Canadian electronic health record framework built upon provincial systems, including ensuring the interoperability of current electronic health information systems and addressing issues such as security standards and harmonizing privacy policies."[7] Indeed, the eventual goal is to establish an EHR system that provides seamless access to personal health information wherever a patient may be in the country.

Various commentators have criticized the slow pace of EHR development in Canada. In its inaugural report in January 2005, the Health Council of Canada recommended "rapid adoption"[8] of EHRs and telehealth technologies "as tools to improve access, quality and

---

5 For a comprehensive summary of such initiatives in jurisdictions across Canada, see Health Canada, *Towards an Evaluation Framework for Electronic Health Records: An Inventory of Electronic Health Records Initiatives Across Canada* (March 2004) by Doreen Neville *et al.*, online: Health Canada <www.hc-sc.gc.ca/ohih-bsi/pubs/kdec/nf_eval_rpt3_e.html#3a>.

6 Canada Health Infoway, "Who We Are, Our Mission" (2005), online: <www.infoway-inforoute.ca/en/WhoWeAre/overview.aspx>.

7 Canada, Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada – Final Report* (Saskatoon: Commission on the Future of Health Care in Canada, 2002) (Chair: Roy J. Romanow, Q.C.) at 76, online: Health Canada <www.hc-sc.gc.ca/english/care/romanow/hcc0086.html> [Romanow Report].

8 Health Council of Canada, *Health Care Renewal in Canada: Accelerating Change* (January 2005) at 41, online: Health Council of Canada <http://healthcouncilcanada.ca/en/index.php?option=com_content&task=view&id=32&Itemid=32>.

comprehensiveness of care."[9] In a commentary published on the Council's website, the Chair, Michael Decter, summarized the benefits of EHRs and lamented the fact that "[o]n the current path and timetable only half the country will have electronic health records by 2009 but the remainder may wait until 2020."[10] A 2004 OECD Economic Survey of Canada cited EHRs as "[a] central element in enhancing the efficiency of health care services" and stated that "further efforts by the federal government or provinces to accelerate the process [of developing EHRs] would be welcome."[11]

Electronic health records may have numerous benefits. Most significantly, EHRs have the potential to: improve health care delivery by allowing timely and accurate access to information by those involved in patient care; reduce medical errors and adverse health events; augment security of patient information; and enhance availability of information to support health system planning and reform as well as research. EHRs that are available to patients can provide them with convenient access to their own health information and facilitate activities such as prescription renewals and appointment booking.

The Romanow Commission advocated EHRs for all Canadians and noted that "[d]iagnoses, treatments and results can be improved when health care providers have access to complete personal health information and can link that information to clinical support tools."[12] Medical errors are an important problem and may be prevented with improved communication. Adverse events are reported as occurring in approximately 7.5 percent of acute care hospital admissions in Canada; that is, each year, around 185,000 admissions are associated with an adverse event.[13] "[T]he judicious application of new technologies and improved communication and coordination among caregivers"[14] are both important means to minimize medical errors.

EHR systems also have the potential to offer greater security of personal health information, as well as provide individuals with easier access to their own information. Research suggests that access to comprehensive EHRs reduces the need for some in-person visits and allows health care providers to respond to patient queries by telephone.[15] This may reduce health care costs by eliminating some unnecessary visits.

---

9 *Ibid.*

10 Michael Decter, *The Electronic Health Record: What it is and why you should want one!* (14 February 2005), online: Health Council of Canada <http://healthcouncilcanada.ca/en/index.php?option=com_content&task=view&id=30&Itemid=137>.

11 OECD, *Economic Survey of Canada 2004*, c. 4: "Institutional Changes to Health Care System" at 5, online: OECD <www.oecd.org/dataoecd/41/63/33851206.pdf>.

12 Romanow Report, *supra* note 7 at 78.

13 G. Ross Baker *et al.*, "The Canadian Adverse Events Study: the incidence of adverse events among hospital patients in Canada" (2004) 170 Canadian Medical Association Journal 1678.

14 *Ibid.* at 1685.

15 See *e.g.* Terhilda Garrido *et al.*, "Effect of electronic health records in ambulatory care: retrospective, serial, cross sectional study" (2005) 330 British Medical Journal 581. The conclusions of this study are expressed as follows (at 581): "Readily available, comprehensive, integrated clinical information reduced use of ambulatory care while maintaining quality and allowed doctors to replace some office visits with telephone contacts. Shifting patterns of use suggest reduced numbers of ambulatory care visits that are inappropriate or marginally productive."

In regard to secondary uses of EHRs, several Canadian investigators have noted that "[r]esearchers and policy makers studying quality of medical care have traditionally used datasets to study the effectiveness of treatments. Recently, however, researchers have turned to electronic medical records, which contain more clinically relevant information."[16] Yet, not everyone agrees that EHRs will deliver on these promises. Some challenge the assertions that EHRs are a lynchpin for more effective and efficient health care.[17] It has been noted that "[t]here is little to no empirical research and analysis of how EHRs will improve health care, and what research exists suggests that comprehensive EHR may not be the best solution."[18] As well, EHRs can only be as effective as their design and implementation; the best EHR idea in the world will not achieve its potential if the people who design, operate and use them are not adequately trained.[19] Further, some observers question the claim that EHRs will improve completeness and accuracy of data.[20]

Some also fear the "function creep" phenomenon, in which uses of EHRs will expand over time to encompass activities not originally foreseen, including matching EHRs with other personal information databases.[21] As well, the creation of comprehensive records may generate increased interest in others to obtain access to those records.[22]

---

16 Donald J. Willison, *et al.* "Patient consent preferences for research uses of information in electronic medical records: interview and survey data" (2003) 326 British Medical Journal 373 at 373.

17 A former Privacy Commissioner of Canada, George Radwanski, summarized some of these concerns in a letter to Roy Romanow during the public consultation of the Commission on the Future of Health Care in Canada (27 June 2002), see online: <www.privcom.gc.ca/media/le_ehr_020627_e.asp>.

18 Nola M. Ries & Geoff Moysa, "Legal Protections of Electronic Health Records: Issues of Consent and Security" (2005) 14:1 Health L. Rev. 18 at 20.

19 For example, a lack of skilled informatics specialists has slowed progress of the U.K.'s health care information technology plan: see Tony Collins, "Head of NHS IT acknowledges severe shortages of skilled staff" (30 March 2005), online: Computerweekly.com <www.computerweekly.com/Article 137533.htm>. An interesting recent article describes the experiences of a U.S. medical practice in implementing an electronic patient record system (Richard J. Baron *et al.*, "Electronic Health Records: Just around the Corner? Or over the Cliff?" (2005) 143 Annals of Internal Medicine 222 at 223). The article explains that "[n]one of the physicians had previously used [an] ... operating system ... and ... needed training.... Some staff members had never used a mouse.... The medical assistants, who had previously made notes by hand, were now asked to use wireless-equipped laptops with mouse pads or track-ball pointers." Training challenges in this context are immense.

20 See Beverly Woodward who contends that:

> The computerized record is envisioned as a newly designed, multipurpose document with a standardized format and nomenclature. This reconstruction of the record raises serious methodologic questions. The frequent claim, for example, that the computer-based patient record will be complete and accurate reflects naiveté about the inherent problems with standardized formats and record keeping. The suitability of a single record for many purposes — business, clinical, research, and public health — is also questionable.

Beverly Woodward, "The Computer-Based Patient Record and Confidentiality" (1995) 333 New England Journal of Medicine 1419.

21 In his 2002 letter to the Romanow Commission, *supra* note 17, former federal Privacy Commissioner Radwanski expressed trepidation about "the growing enthusiasm for electronic health records." He asserted:

> Function creep is almost inevitable. Function creep is a term that refers to the pressure to use personal information that has been collected for a very specific purpose for other purposes. It's not difficult to imagine that police forces will put forward a cogent argument in favour of seeing the information, for example, to ensure that a driver they have stopped doesn't have a history of mental illness. Or the life insurance industry will come up with arguments about why it should have access to databases to collect clients' medical information. And many organizations might demand access to electronically stored genetic information.

22 Woodward, *supra* note 20.

The Kirby Senate Report on health care noted that "[t]he issue of privacy, confidentiality and protection of personal health information in the context of an EHR system is perhaps the most sensitive one raised during the Committee's hearings on this question."[23] In a report on information technology in health care, the British Columbia Medical Association asserted that "[i]mproving access to health information, however, should not come at the cost of sacrificing the privacy rights of the individual patient."[24] Leading U.S. health law scholars have observed that

> [p]rincipal among the legal challenges presented by the computerization of health data information is how to protect individual privacy interests in personally identifiable health information.... Modern computer applications in the health care system threaten individual privacy despite offering significant benefits to patients and practitioners. Computerized databases of personally identifiable information may be accessed, changed, viewed, copied, used, disclosed, or deleted more easily and by more people (authorized and unauthorized) than paper-based records.[25]

III. PRIVACY AND HEALTH INFORMATION

Privacy encompasses an individual's right to control access to and disclosure of their personal information and, through common law and legislation, Canadian law specifies the nature and extent of patients' privacy rights and interests in regard to health information.[26] The Supreme Court of Canada has described informational privacy as "the right of the individual to determine for himself when, how and to what extent he will release personal information about himself."[27] The Supreme Court of Canada has also recognized that individuals maintain an ongoing interest in their health information after it has been collected and is in the hands of health care providers.

In *McInerney v. MacDonald*,[28] the Supreme Court analyzed the nature of a patient's interest in the information contained in her health records. The Court emphasized:

> Of primary significance is the fact that the records consist of information that is highly private and personal to the individual. It is information that goes to the personal integrity and autonomy of the patient. ... such information remains in a fundamental sense one's own, for the individual to communicate or retain as he or she sees fit.[29]

---

23 Canada, Standing Senate Committee on Social Affairs, Science and Technology, *The Health of Canadians – The Federal Role*, vol. 6: Recommendations for Reform (Ottawa: Standing Senate Committee on Social Affairs, Science and Technology, 2002) (Chair: Hon. Michael J.L. Kirby), c. 10 at 177, online: Health Canada <www.hc-sc.gc/ca/hcs-sss/com/kirby/index_c.html> [Kirby Report].

24 British Columbia Medical Association, *Getting IT Right: Patient-Centred Information Technology* (January 2004) at 27, online: <www.bcma.org/public/news_publications/publications/policy_papers/ITPaper/GettingITRight.htm> [*Getting IT Right*].

25 James G. Hodge, Lawrence O. Gostin & Peter D. Jacobson, "Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability" (1999) 282 JAMA 1466 at 1467.

26 For further discussion of the right to privacy in the context of health information, see *e.g.* Mary Marshall & Barbara von Tigerstrom, "Health Information" in Jocelyn Downie, Timothy Caulfield & Colleen Flood, eds., *Canadian Health Law and Policy*, 2d ed. (Markham, Ont.: Butterworths, 2002) at 158-64.

27 *R. v. Duarte*, [1990] 1 S.C.R. 30 at 46.

28 *McInerney v. MacDonald*, [1992] 2 S.C.R. 138.

29 *Ibid.* at 148.

The Court also underscored the fiduciary nature of the physician-patient relationship, noting that "[a] physician begins compiling a medical file when a patient chooses to share intimate details about his or her life in the course of medical consultation. The patient 'entrusts' this personal information to the physician for medical purposes."[30]

Ultimately, the Court summarized its analysis in the following statement:

> [I]nformation about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one's own. The doctor's position is one of trust and confidence. The information conveyed is held in a fashion somewhat akin to a trust. While the doctor is the owner of the actual record, the information is to be used by the physician for the benefit of the patient. The confiding of the information to the physician for medical purposes gives rise to an expectation that the patient's interest in and *control of* the information will continue.[31]

As these passages indicate, privacy is generally viewed as a consent-based right. In the health care context, this position is reflected in the Canadian Medical Association's *Health Information Privacy Code*, which defines privacy as a right that "includes a patient's right to determine with whom he or she will share information and to know of and exercise control over use, disclosure and access concerning any information collected about him or her."[32] In other words, a patient's privacy rights in regard to his health information are respected if he has an opportunity to exercise some control over it by consenting to, or withholding consent for, various uses or disclosures. While these general principles appear largely incontrovertible, they may raise challenges in the context of EHRs.

IV. CONSENT IN HEALTH CARE

The concept of consent is critical in the health care context. The law recognizes patients as autonomous individuals who have a right to decide whether to accept or reject medical interventions and emphasizes patient control over one's bodily integrity. The Supreme Court of Canada has cited the following seminal statement of this principle:

> The right to determine what shall, or shall not, be done with one's own body, and to be free from non-consensual medical treatment, is a right deeply rooted in our common law. This right underlies the doctrine of informed consent.... The fact that serious risks or consequences may result from a refusal of medical treatment does not vitiate the right of medical self-determination.... It is the patient, not the doctor, who ultimately must decide if treatment — any treatment — is to be administered.[33]

To facilitate informed patient decision making, health care providers have an obligation to explain options to the patient and provide information about material risks and benefits of

---

30 *Ibid.* at 148-49.

31 *Ibid.* at 150-51 [emphasis added].

32 Canadian Medical Association, *Health Information Privacy Code* (15 August 1998) Principle 1: The Right of Privacy, online: Canadian Medical Association <www.cma.ca/index.cfm/ci_id/3216/la_id/1.htm> [*Privacy Code*].

33 *Fleming v. Reid* (1991), 4 O.R. (3d) 74 (C.A.), at 85, cited by the Supreme Court of Canada in *Ciarlariello v. Schachter*, [1993] 2 S.C.R. 119, Cory J. at 135.

different courses of action.[34] The care provider must disclose information that a reasonable person in the patient's position would want to know and must also respond to specific questions a patient may ask.[35] A patient also has a right to withdraw consent, subject to safety considerations.[36]

But how far does individual autonomy and control — which is so important in the treatment context — extend to collection, use and disclosure of one's health information, particularly for the purposes of providing care?[37] As health care becomes increasingly specialized, and with greater focus on interdisciplinary and collaborative practice, a wide range of health care providers may be involved in providing care for an individual patient and, to provide appropriate care, the patient's information must be shared among them. Lorne E. Rozovsky and Noela J. Inions observe that

> [o]nce a health system rather than an individual physician treats the individual, the armies of workers who make up the system require the information or parts of it in order to provide the health services. Failure to have the information communicated from one person to another within the system can cause errors, conflicts in treatment and care, and a general lowering of the standard of care.[38]

Development of appropriate EHR systems is often cited as a critical element in facilitating collaboration in health care delivery.[39] Indeed, Elaine Gibson observes that

---

34 For discussion of the standard of information disclosure that must be met to obtain legally valid informed consent, see *Reibl v. Hughes*, [1980] 2 S.C.R. 880. For discussion, see *e.g.* Bernard Dickens, "Informed Consent" in Downie, Caulfield & Flood, eds., *supra* note 26, 129.

35 As Dickens notes, *ibid.* at 135: "Information given to the patient must initially be designed to serve a reasonable person in the position of the patient.... If the individual patient asks a question that demonstrates a special interest, however, the concern underlying the question shows the position of the patient appraised objectively."

36 *Ciarlariello v. Schachter*, *supra* note 33, where the Court stated at 136:

> An individual's right to determine what medical procedures will be accepted must include the right to stop a procedure. ... the patient's right to bodily integrity provides the basis for the withdrawal of a consent to a medical procedure even while it is underway. Thus, if it is found that the consent is effectively withdrawn during the course of the proceeding then it must be terminated. This must be the result except in those circumstances where the medical evidence suggests that to terminate the process would be either life threatening or pose immediate and serious problems to the health of the patient.

37 This article is primarily concerned with collection, use and disclosure of identifiable patient information via EHRs for treatment, rather than secondary uses such as research or audit, which may more readily be conducted with de-identified information. For discussion of legal issues associated with use of personal information in research, see *e.g.* Timothy Caulfield & Nola M. Ries, *Consent, Privacy and Confidentiality in Longitudinal, Population Health Research: The Canadian Legal Context* (2004) Special Supp. to Health L.J. For a discussion of whether individuals retain a privacy interest in anonymized health information, see *e.g.* Gibson, *infra*, note 40.

38 Lorne E. Rozovsky & Noela J. Inions, *Canadian Health Information: A Practical Legal and Risk Management Guide*, 3d ed. (Markham, Ont.: Butterworths, 2002) at 84.

39 For recent commentary and analysis on issues associated with EHRs in the context of collaborative health care, see *e.g.* Raisa Deber & Andrea Baumann, "Enhancing Interdisciplinary Collaboration in Primary Health Care," *Barriers and Facilitators to Enhancing Interdisciplinary Collaboration in Primary Health Care*, (2005) online: Primary Health Care <www.eicp-acis.ca/en/resources/pdfs/Barriers-and-Facilitators-to-Enhancing-Interdisciplinary-Collaboration-in-Primary-Health-Care.pdf>. See especially 23-25.

> [t]he electronic era has had a formidable impact on health information.... as greater and greater numbers of health care providers may be involved in providing services to a patient, the system has espoused the concept of "seamless care". This in turn requires access by many individuals to personal health information, facilitated by the utilization of electronic health records in various settings in Canada.[40]

By and large, this sharing of information occurs without explicit patient consent and, rather, is done on the basis of implied agreement on the part of the patient. A typical example of implied consent in the health care treatment context is when a patient holds out her arm so a health care provider can draw a blood sample. Once the blood is extracted and sent to a laboratory with instructions for analysis, personal information about the patient will flow back and forth between the lab and the care provider. Just as the initial blood draw occurred on the base of implied consent, so too, does the exchange of patient information.

The term "circle of care" is often used to describe those who are directly involved in providing health care and treatment for a patient. Industry Canada, Ottawa's department responsible for overseeing federal privacy legislation,[41] describes the "circle of care" as including:

> [T]he individuals and activities related to the care and treatment of a patient. Thus, it covers the health care providers who deliver care and services for the primary therapeutic benefit of the patient and it covers related activities such as laboratory work and professional or case consultation with other health care providers.[42]

The federal Privacy Commissioner has also indicated "the need for information to flow from health care provider A to health care provider B in order to ensure the best level of patient care" and that this includes the principle of implied consent for information to flow freely within the "circle of care."[43]

However, not all agree on how wide the circle of care should be construed. For example, a Saskatchewan woman objected to the disclosure of her Pap test results to the Saskatchewan Cancer Agency as part of a cervical cancer prevention program.[44] The Cancer Agency responded that disclosure of Pap test results is within an appropriate circle of care. In a lengthy investigation report into how personal health information is handled for the Prevention Program for Cervical Cancer, the Saskatchewan Privacy Commissioner considered issues of consent and acknowledged that requiring express consent to collect, use

---

40 Elaine Gibson, "Is There a Privacy Interest in Anonymized Personal Health Information?" (2003) Special Edition of Health L.J., *Precedent & Innovation: Health Law in the 21st Century* 97 at 98.

41 Through its Information and Privacy Rights Administration Office, Industry Canada administers the *Privacy Act*, R.S.C. 1985, c. P-21, the *Access to Information Act*, R.S.C. 1985, c. A-1 and oversees the private sector legislation, the *Personal Information Protection and Electronic Documents Act*, R.S. 2000, c. 5 [*PIPEDA*].

42 Industry Canada, *PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector*, online: <http://strategis.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gov00235e.html> [*PARTs Initative*].

43 Address by Jennifer Stoddart, Privacy Commissioner of Canada, "Privacy Laws & Health Information: Making it Work," presented at Privacy Laws & Health Information Conference, 27 October 2004, Regina, Saskatchewan. Text of address available online at: <www.privcom.gc.ca/speech/2004/sp-d_041027_e.asp> [Stoddart address].

44 Lana Haight, "Privacy issue angers Saskatchewan woman" *Saskatoon StarPhoenix* (7 July 2004) A8.

and share patient information for a cancer prevention program may undermine its purpose.[45] He concluded the Cancer Agency may rely on "deemed consent" provisions in Saskatchewan's *Health Information Protection Act*,[46] but emphasized the Agency should be more transparent about its uses of information and give women an opportunity to opt out of the cancer prevention program. He also emphasized that privacy legislation "should be viewed as a floor and not as a ceiling."[47]

Deemed consent occurs in situations where individuals are assumed to consent to collection, use or disclosure of their personal information unless they explicitly decline consent. In this circumstance, an organization may give an individual notice of a particular use of their information that will occur unless the person expressly chooses to opt out of that use. This attenuated form of consent is generally regarded as appropriate only in situations involving non-sensitive information. Further, the organization ought to clearly indicate the purposes for which the information will be used so the individual can make an informed choice regarding opting in or out.

The degree to which consent that is less than explicit informed consent can be relied on for collection, use and disclosure of personal health information via EHRs is contentious. One commentator has observed that:

> EHRs, which facilitate sharing of information by a wide network of people, potentially conflict with privacy principles unless patients *control* how the record is shared and appropriate security measures are in place. A coherent legal framework to appropriately protect the privacy and confidentiality of personal health records is therefore an essential first step for successful EHRs.[48]

The next section examines relevant Canadian legislation that imposes rules regarding consent and health information, particularly in the context of EHRs.

V. CANADIAN LEGISLATION, CONSENT AND ELECTRONIC HEALTH RECORDS

Recent years have witnessed proliferation in the number of Canadian statutes that regulate the collection, use and disclosure of personal information, including health information. Around the early- to mid-1990s, many provinces and territories across Canada began enacting laws — typically called *Freedom of Information and Protection of Privacy Acts* — to regulate the collection, use and disclosure of personal information in the public sector. Quebec enacted public sector privacy and information access legislation a decade earlier in 1982.[49] At the federal level, the *Privacy Act* and the *Access to Information Act* came into force in 1983 to cover federal government departments and agencies. In the late 1990s, laws

---

45 Office of the Information and Privacy Commissioner, *Investigation Report H – 2005-002, Prevention Program for Cervical Cancer* (27 April 2005), online: <www.oipc.sk.ca/reviews.htm> [*H-2005-002*].

46 S.S. 1999, c. H-0.021 [*HIPA*].

47 *H-2005-002*, *supra* note 45 at 6.

48 Amanda Cornwall, "Connecting Health: A review of electronic health record projects in Australia, Europe and Canada," (2003), online: Public Interest Advocacy Centre <www.piac.asn.au/publications/pubs/churchill_20030121.html> at 16 [emphasis added].

49 See *An Act respecting access to documents held by public bodies and the protection of personal information*, R.S.Q., c. A-2.1.

aimed specifically at health information began to emerge. Manitoba, Alberta, Saskatchewan and Ontario enacted such legislation over the seven-year period from 1997 to 2004.

In 2001, Ottawa enacted the *Personal Information Protection and Electronic Documents Act*[50] (*PIPEDA*) to regulate information handling in the private sector[51] and, as of 1 January 2004, *PIPEDA* came fully into force in the health sector. *PIPEDA* was enacted to establish national rules for personal information protection in the private sector and establishes, as law, the Canadian Standards Association's *Model Code for the Protection of Personal Information*.[52] *PIPEDA* was phased into effect over three years and initially applied to the federally regulated private sector (for example, airlines, banks and broadcasting) and to all organizations that disclose personal information for consideration across provincial or national borders. In its next phase, *PIPEDA* extended to cover personal health information for the organizations and activities noted above. *PIPEDA* now applies to every organization that collects, uses or discloses personal information, including personal health information, in the course of a commercial activity within a province, but will not apply where substantially similar provincial legislation is in force.

Quebec, Alberta and British Columbia all have private sector privacy legislation that the federal Governor-in-Council has recognized as substantially similar to *PIPEDA*.[53] The Province of Ontario has requested that its *Personal Health Information Protection Act*[54] be declared substantially similar to *PIPEDA* and expects an exemption order will be forthcoming.[55]

The range of privacy laws across Canada has been described as a patchwork[56] and organizations have expressed concern about the challenges of complying with overlapping — or even worse, conflicting — legislative rules. Touching on some of these issues, the Kirby Report noted that:

> Currently, there is significant variation in privacy laws and data access policies across the country that poses a challenge for EHR systems that are dependent on inter-sectoral and inter-jurisdictional flows of personal

---

50 *Supra* note 41.

51 *PIPEDA* applies to "commercial activities," which are defined in s. 2(1) as including "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

52 *Model Code for the Protection of Personal Information: A National Standard of Canada*, CAN/CSA-Q830-46 (Etobicoke, Ont.: Canadian Standards Association, 1996). For further information on this *Code*, see the Canadian Standards Association online: <www.csa.ca/standards/privacy/Default.asp?language=english> [CSA *Model Code*]. This *Code* encompasses the following principles: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

53 Section 26(2)(b) of *PIPEDA* authorizes the Governor-in-Council to declare a provincial law to be substantially similar to *PIPEDA* and exempt activities and organizations subject to provincial law from the federal statute.

54 S.O. 2004, c. 3 [*PHIPA*].

55 See Ann Cavoukian, *Commissioner's PHIPA Highlights* (March 2005), online: Information and Privacy Commissioner of Ontario <www.ipc.on.ca/ docs/phipa02-e.pdf>, where the Commissioner notes that she "anticipate[s] seeing a final exemption order recognizing the substantial similarity of Ontario's *PHIPA* to the federal *PIPEDA*, so that health information custodians covered by *PHIPA* will not also be subject to *PIPEDA*."

56 See *e.g. Getting IT Right*, *supra* note 24 at 20.

> health information. Differences in rules on how the scope of purpose is defined, the form of consent required, the conditions for substitute decision-making, the criteria for non-consensual access to personal health information, periods for retention of data and requirements for destruction, to name but a few, must be seriously addressed in order to enable the development of EHR systems.[57]

To address this concern, efforts are currently underway to develop harmonized principles at the national level that will guide handling of personal health information, a topic addressed in further detail below. The following section identifies legislative rules related to consent, particularly as they relate to health information and EHRs. A full analysis of how different laws in the legislative patchwork will interact with one another is, however, outside the scope of this article.[58]

A. FEDERAL LEGISLATION

As noted above, the federal *PIPEDA* came fully into force in the health sector on 1 January 2004, leading to considerable discussion about the impact of this legislation on organizations and individuals such as health care providers in private practice, pharmacies and laboratories.[59] There has been much debate as to whether *PIPEDA* applies to health care providers who are funded through the public health insurance system, but, short of a judicial decision reaching the opposite conclusion, this controversy has been resolved in favour of the position that those activities are still of a commercial character and subject to *PIPEDA*. One text observes: "The fact that the [health care] services are publicly funded seems an unlikely basis for treating them as non-commercial when similar services provided for a fee outside provincial health plans, perhaps by the same health professionals, would likely be commercial."[60] Industry Canada confirms that "[t]he funding source (public health insurance, private payer, 3rd party payer, etc.) is not relevant in determining the existence of a commercial activity."[61]

The situation in regard to public hospitals has been described as follows:

> Public hospitals are unlikely to be subject to the Act since they operate on a not-for-profit basis and are not generally understood to be commercial.... If public hospitals are not generally affected by the Act, a number of inconsistencies are likely to arise. For example, the activities of a hospital pharmacy or laboratory would

---

57 Kirby Report, *supra* note 23, s. 10.4, "Protection of Personal Health Information."

58 For fuller discussion, see University of Alberta, Health Law Institute and University of Victoria, School of Health Information Science, *Electronic Health Records and the Personal Information Protection and Electronic Documents Act* (April 2005), online: Faculty of Law, University of Alberta <www.law.ualberta.ca/centres/hli/pdfs/ElectronicHealth.pdf>.

59 Some health care groups actively opposed *PIPEDA*'s application in the health sector. For example, the College of Physicians & Surgeons of Ontario (CPSO) and the Ontario Medical Association were jointly "lobbying the government to exempt physicians specifically, and health care generally, from the Act" due to concerns "that the application of PIPEDA in the medical system will introduce significant impediments to the delivery of health care services, while providing virtually no substantive improvements to patient confidentiality over existing laws." See CPSO, "Concerns about privacy legislation: College lobbies government to exempt physicians" (September/October 2003) *Members' Dialogue*.

60 Colin H.H. McNairn & Alexander K. Scott, *A Guide to the Personal Information Protection and Electronic Documents Act*, 2004 ed. (Markham, Ont.: LexisNexis Butterworths, 2003) at 18-19.

61 *PARTs Initiative*, *supra* note 42.

not be subject to the Act, while the very same activities carried out by a private pharmacy or laboratory would, very likely, be subject to the Act.[62]

Industry Canada has advised that "[h]ospitals are beyond the constitutional scope of the Act as their core activities are not commercial in nature."[63] The federal Privacy Commissioner has affirmed that *PIPEDA* will not cover core hospital activities related to patient care.[64] Non-core activities, such as a pharmacy carrying on a commercial enterprise out of leased hospital space would, however, be subject to *PIPEDA*. To date, *PIPEDA*'s application in the health sector has not been subject to litigation so there is currently no judicial ruling on this issue.[65] It is likely a court would consider Industry Canada's guidance material in interpreting *PIPEDA*'s intended scope, but that material is, of course, not legally binding.

Despite the current lack of judicial rulings on specific cases, there is good reason to operate on the assumption that, in provinces without substantially similar legislation, *PIPEDA* applies to a wide range of health care providers and organizations that engage in commercial activities. As EHR networks expand, many of these entities will collect, use and disclose personal health information through that mechanism and will need to be aware of *PIPEDA*'s rules.

PIPEDA sets out a general principle that "[t]he knowledge and consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate."[66] Section 7(1) sets out limited situations in which it is permissible to collect personal information without consent.[67] In regard to facilitating "knowledgeable" consent, *PIPEDA* requires organizations to "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."[68] Concomitantly, organizations must identify and document the purposes for which it will collect personal information.[69] If an organization wishes to use personal information for a new purpose that is not otherwise permitted by law, that organization must obtain individual consent for that new use.[70]

Consent under *PIPEDA* may be express or implied, oral or written. The statute states that express consent should generally be sought for the collection, use and disclosure of sensitive information, and medical records are "almost always considered to be sensitive."[71] Express consent has been described as "the strongest form of consent, and is in keeping with the spirit

---

62 McNairn & Scott, *supra* note 60.

63 *PARTs Initiative*, *supra* note 42.

64 Stoddart address, *supra* note 43.

65 The Government of Quebec has launched a challenge to *PIPEDA*'s constitutionality, alleging that the federal statute trenches unlawfully on areas of provincial legislative authority.

66 *PIPEDA*, *supra* note 41 at Sch. 1, Principle 3: Consent.

67 These narrow exceptions to consent include situations when timely consent cannot be obtained and collection of information is "clearly in the interests of the individual" (*ibid.*, s. 7(1)(a)) and when consensual collection would compromise an investigation into a breach of the law (s. 7(1)(b)).

68 *Ibid.*, Sch. 1, cl. 4.3.2.

69 *Ibid.*, Sch. 1, cl. 4.2.1.

70 *Ibid.*, Sch. 1, cl. 4.2.4.

71 *Ibid.*, Sch. 1, cl. 4.3.4.

of PIPEDA."[72] Some concern has been expressed that *PIPEDA* will be unworkable in health care as it emphasizes express consent.[73] However, as discussed above, both Industry Canada and the federal Privacy Commissioner have indicated that implied consent is acceptable under *PIPEDA* within the circle of care.

PIPEDA also confers a right to withdraw consent at any time, subject to the legal obligations of a third party.[74] For example, an individual cannot withhold consent for *any* recording of his interaction with a health care provider as that provider has an obligation to maintain complete and accurate records. An organization must inform an individual of consequences of her choice to withdraw consent to collection, use and/or disclosure of personal information.[75]

B. PROVINCIAL LEGISLATION

PIPEDA does not contain specific provisions regarding EHRs, which is not surprising considering that the statute is not focused solely on the health sector. As a consequence, *PIPEDA*'s consent rules and other provisions must be construed in the EHR context in jurisdictions and in regard to activities where the law applies.

Provinces with health sector legislation have developed specific rules regarding EHRs. In some cases, those rules have been amended as providers and patients have gained experience with EHR systems. The following section summarizes provisions in provincial health information statutes in Manitoba, Saskatchewan, Ontario and Alberta that are relevant to EHRs.[76]

Manitoba's *Personal Health Information Act*[77] was enacted in 1997 and applies to "trustees" of health information, including both public and private sector entities, such as hospitals, other care facilities and health professionals. *PHIA*'s preamble points out that "clear and certain rules for the collection, use and disclosure of personal health information are an essential support for electronic health information systems that can improve both the quality of patient care and the management of health care resources."[78] While this statute sets out a general rule requiring individual consent for the collection, use and disclosure of health information, it authorizes trustees to disclose personal health information without individual consent

> to a computerized health information network and database, established by the government or another trustee that is a public body specified in the regulations, in which personal health information is recorded for the

---

72 Office of the Privacy Commissioner of Canada, *Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act*, online: <www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp>.

73 See *e.g.* British Columbia Medical Association, *Policy Backgrounder – Privacy Legislation in BC's Health Care System* (September 2003), online: <www.bcma.org/public/news_publications/publications/policy_backgrounders/PrivacyLegislation.asp>.

74 *PIPEDA*, *supra* note 41, Sch. 1, cl. 4.3.8.

75 *Ibid.*

76 This analysis builds on Ries & Moysa, *supra* note 18.

77 C.C.S.M. c. P33.5 [*PHIA*].

78 *Ibid.*, preamble.

> purpose of facilitating (i) the delivery, evaluation or monitoring of a program that relates to the provision of health care or payment for health care, or (ii) research and planning that relates to the provision of health care or payment for health care.[79]

PHIA further authorizes a trustee to disclose health information without consent to another person for the purposes of providing care to the subject individual, unless that individual has directed the trustee not to disclose the information,[80] a provision referred to as a "lock box." Commentators note that "health care providers have opposed the inclusion of a 'lock box' on the basis that it would lead to multiple streams of records, compromise patient care, and increase the risk of health provider liability"[81] and note that "[a] related concern is whether patients should have the right to block the transfer of their information by electronic means."[82] While Manitoba's lock box provision empowers a patient to prevent disclosure of information to particular persons, it is arguable that this right does not extend to prohibiting disclosure to a health information network.

Saskatchewan's *Health Information Protection Act*[83] came into force in September 2003 and, like Manitoba's legislation, applies to "trustees" of health information, including health care practitioners, health facilities, and government institutions. As with other health sector statutes, *HIPA* generally requires express or implied consent for the collection, use and disclosure of personal health information. Under the statute, implied consent is acceptable to permit the trustees to arrange and provide care requested or required by a patient. In the case of express consent, the consent must be informed and relate to the purposes for which the information is obtained.[84]

Province-wide EHR initiatives in Saskatchewan are being developed under the auspices of the Health Information Solutions Centre (HISC),[85] which is the arm of the provincial health ministry charged with health information technology. Prior to establishing HISC in 2003, the provincial government had created the Saskatchewan Health Information Network (SHIN) in 1997 as a Crown corporation. In 2003, SHIN was integrated as an agency into HISC.

HIPA allows the SHIN (or a prescribed person) to create "comprehensive health records," which compile personal health information from two or more trustees (defined as health care providers, institutions, government agencies and others that hold personal health information[86]) to create a full health history for a particular individual that may be accessed by other trustees.[87] When *HIPA* was first implemented, it gave individuals the right to direct that a trustee not store their specified information on the SHIN network.[88] This provision was removed in 2003 and an individual no longer has this explicit right. However, individuals

---

79 *Ibid.*, s. 22(2)(h).
80 *Ibid.*, s. 22(2)(a).
81 Marshall & von Tigerstrom, *supra* note 26 at 177.
82 *Ibid.*
83 *Supra* note 46.
84 *Ibid.*, s. 6.
85 For further information, see <www.health.gov.sk.ca/ph_hisc_abouthisc.html>.
86 *HIPA*, *supra* note 46, s. 2(j).
87 *Ibid.*, s. 18.1(1).
88 *Ibid.*, s. 8(1).

retain the right to restrict who has access to their comprehensive health record by giving written instruction to SHIN, with which SHIN is obliged to comply.[89]

In addition, *HIPA* states that access to the comprehensive health record may only be granted if the trustees whose records were used to compile the comprehensive record give authorization and either the individual about whom the record relates consents in writing, consent is deemed to exist[90] or is not required.[91] As a result, *HIPA*'s consent requirements allow both individuals and trustees to exert some control over disclosure of information through the provincial EHR system.

Ontario's *Personal Health Information Protection Act*[92] came into force on 1 November 2004, and applies to health information custodians such as health care providers and facilities. The legislation largely leaves specific rules regarding EHRs to be developed in regulations. For example, s. 10(3) of the *Act* provides that "[a] health information custodian that uses electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any." The *Act* also authorizes the making of regulations

> specifying requirements, or a process for setting requirements ... with which a health information custodian is required to comply when using electronic means to collect, use, modify, disclose, retain or dispose of personal health information, including standards for transactions, data elements for transactions, code sets for data elements and procedures for the transmission and authentication of electronic signatures.[93]

Regulations enacted under *PHIPA* are particularly concerned with circumscribing the activities of those who provide services to allow custodians to collect, use and disclose personal health information electronically.[94] The service provider must give custodians

> a plain language description of the services that the provider provides to the custodians, that is appropriate for sharing with the individuals to whom the personal health information relates, including a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information.[95]

The provider must also make available a public description of its services and security safeguards.

---

89 See *ibid.*, s. 8, as am. by S.S. 2003, c. 25.

90 *Ibid.*, s. 27(2) sets out several purposes for which individuals are deemed to consent to disclosure of information including "the purpose of arranging, addressing, assessing the need for, providing, continuing, or supporting the provisions of the service requested or required by the subject individual."

91 *Ibid.*, s. 27(4) describes circumstances in which individual consent is not required for the disclosure of personal health information.

92 *Supra* note 54.

93 *Ibid.*, s. 73(1)(h).

94 O. Reg. 329/04, s. 6(2) refers to a "health information network provider," defined as "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another."

95 *Ibid.*, s. 6(3)(2).

Like Manitoba's legislation, *PHIPA* creates a lock box provision that permits an individual to decline consent for disclosure of personal health information to other custodians for purposes of care and treatment.[96] Where an individual imposes a lock box, their care provider must inform the recipient of information about the lock box if the provider feels that not all information relevant to providing adequate care to the patient has been disclosed.[97]

Alberta's *Health Information Act*,[98] which came into force in April 2001, applies to custodians of health information, including government departments, health authorities, health care practitioners paid under the provincial health insurance scheme, and pharmacies, as well as affiliates of custodians, who are employees, contractors or volunteers under the control of custodians.

Since its enactment, *HIA* has undergone some revisions to its provisions relevant to EHRs. When the statute was first implemented, it required consent from individuals before their health information could be disclosed electronically. Specifically, s. 59 of the statute required valid consent to include:

> (a) an authorization for the custodian to disclose the health information specified in the consent,
> (b) the purpose for which the health information may be disclosed,
> (c) the identity of the person to whom the health information may be disclosed,
> (d) an acknowledgment that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent,
> (e) the date the consent is effective and the date, if any, on which the consent expires, and
> (f) a statement that the consent may be revoked at any time by the individual providing it.[99]

The Alberta government removed this provision in 2003 based on feedback that compliance posed significant operational challenges. For example, one report describes a

---

[96] *PHIPA*, *supra* note 54, s. 38(1)(a), which provides:

> A health information custodian may disclose personal health information about an individual,
> (a) to a person [described in earlier provisions] if the disclosure is reasonably necessary for the provision of health care and it is not reasonably possible to obtain the individual's consent in a timely manner, *but not if the individual has expressly instructed the custodian not to make the disclosure* [emphasis added].

[97] *PHIPA*, *ibid.*, s. 20(3) states:

> If a health information custodian discloses, with the consent of an individual, personal health information about the individual to a health information custodian ... for the purpose of the provision of health care to the individual and if the disclosing custodian does not have the consent of the individual to disclose all the personal health information about the individual that it considers reasonably necessary for that purpose, the disclosing custodian shall notify the custodian to whom it disclosed the information of that fact.

See also s. 38(2), which provides:

> If a health information custodian discloses personal health information about an individual under clause (1)(a) and if an instruction of the individual made under that clause prevents the custodian from disclosing all the personal health information that the custodian considers reasonably necessary to disclose for the provision of health care or assisting in the provision of health care to the individual, the custodian shall notify the person to whom it makes the disclosure of that fact.

[98] R.S.A. 2000, c. H-5 [*HIA*].

[99] *Ibid.*, s. 34(2). Saskatchewan's *HIPA*, *supra* note 46, s. 6, also stipulates certain requirements for valid consent, as does the Ontario *PHIPA*, *supra* note 54, s. 18.

pilot project for Alberta's Pharmaceuticals Information Network where "doctors were taking more than 30 minutes to explain the system, driven by concerns about professional liability."[100] The Alberta Information and Privacy Commissioner acknowledged that the costs of complying with this legislative requirement (namely, the extra time spent by health care providers to obtain patient consent) outweighed its value.[101] He also noted that "[i]n facilitating a province wide electronic health record (EHR), practical experience made it apparent that getting consent from Albertans was going to be difficult and costly."[102] The Alberta Commissioner also stated he does not believe "it is possible to inform people in a meaningful way, of all the specific disclosures by electronic means, which might ever be made of their health information."[103] Consequently, consent can never be truly informed according to legal standards that require full disclosure of details.

In 2004, the Alberta government appointed a special committee to review *HIA* and some of that committee's recommendations are relevant to EHRs.[104] The Committee recommended that another legislative committee ought to be struck to examine in detail "the need for more clear and transparent rules for the electronic health record."[105] Further, the Committee suggested that *HIA* should be amended "to allow for the collection, use and disclosure of a unique identifier for health service providers for authorization and authentication purposes in the electronic health record."[106] The Committee also recommended further review of consent requirements under *HIA*, particularly considering the development of a pan-Canadian health information and privacy framework.[107]

To date, both Alberta and Saskatchewan have amended their health information privacy laws to remove consent provisions that, in practice, seemed to be unworkable in the EHR context. As EHR systems develop across the country, other jurisdictions will have to determine whether existing legislation – including relevant public, private and health sector laws – provides an appropriate framework for protecting privacy while not impeding delivery of care.

C. PRIVACY GUIDELINES AND ETHICAL OBLIGATIONS

In addition to legislative rules, health care providers and organizations must also consider privacy guidelines and ethical obligations that are relevant to patient privacy and consent regarding health information. As noted earlier, efforts are underway to harmonize rules to guide uses of health information in Canada. In June 2005, the Advisory Committee on Information and Emerging Technologies, which reports to the Conference on

---

100 Cornwall, *supra* note 48 at 19.

101 See News Release, Office of the Information and Privacy Commissioner, "Commissioner's response to repeal of section 59 and introduction of section 60(2) of the *Health Information Act*" (26 February 2003), online: Office of the Information and Privacy Commissioner <www.oipc.ab.ca/ims/client/upload/Repeal_of_s.59.pdf>.

102 *Ibid.*

103 *Ibid.*

104 See Select Special Health Information Act Review Committee, *Final Report* (October 2004), online: Legislative Assembly of Alberta <www.assembly.ab.ca/HIAReview/hiawebreport.pdf>.

105 *Ibid.* at i, Recommendations #1 and #18.

106 *Ibid.* at ii, Recommendation #19.

107 *Ibid.* at iv, Recommendation #37.

Federal/Provincial/Territorial (F/P/T) Ministers of Health, released a pan-Canadian health information privacy and confidentiality framework. This advisory committee is comprised of F/P/T representatives, the Canadian Institute of Health Information, Statistics Canada, Canada Health Infoway and the National Aboriginal Health Organization.[108] The Framework aims "to suggest a harmonized set of core provisions for the collection, use and disclosure of personal health information in both the publicly and privately funded sectors" and it maintains that "[c]onsistent, or at least more consistent, privacy regimes among jurisdictions would facilitate health care renewal, including the development of electronic health record systems."[109]

The Framework focuses on privacy as "a consent-based right"[110] and stipulates that individual consent should be required for all collection, uses and disclosures of personal health information unless otherwise authorized by law. However, the Framework acknowledges that much sharing of patient information for the purposes of care and treatment is done without obtaining explicit informed consent and it supports a model of "implied knowledgeable consent" for collecting, using and disclosing patient information within a circle of care.

According to the Framework, implied knowledgeable consent

> [e]xists where it is reasonable in the circumstances and as a result of the individual's behaviour to believe that the individual knows:
>
> a. the purposes of the collection, use, or disclosure and how their personal health information will be used or disclosed; and
> b. that the individual may provide or withhold consent.[111]

The Framework states that individuals should have a right to withhold consent for collection, use and disclosure of personal health information and a custodian of personal health information must comply with a patient's instruction, for example, that the information not be shared with another care provider. The care provider must explain to the patient any consequences of refusing consent and, where the provider believes that the restricted information is important for the patient's care, must inform other providers involved in the patient's care that she has refused to allow disclosure of her information. Presumably, if the custodian warns another care provider, that second provider may ask the patient directly for information the provider cannot obtain through disclosure of the patient's file from the first custodian. Finally, in emergency situations, the Framework permits a custodian to ignore a patient's requested restriction on use or disclosure of his information, but the custodian must inform the patient of any uses or disclosures that override the patient's previously expressed wishes.

---

108 Quebec did not participate in the development of the Framework and Saskatchewan withdrew late in the process.

109 Health and the Information Highway Division, Health Canada, Pan-Canadian Health Information Privacy and Confidentiality Framework (January 2005) at "Introduction," online: Health Canada <www.hc-sc.gc.ca/ohih-bsi/pubs/privacy_framework_e.html#intro>.

110 *Ibid.*

111 *Ibid.* at "Core Concepts."

In addition to the core concepts, the Framework also includes so-called ancillary provisions for consideration. Interestingly, these ancillary provisions dilute the ostensibly robust requirement that patients should have a right to restrict uses or disclosure of their information. The ancillary provision related to patient control over their information states:

> Where compliance with an individual's notice to withhold or withdraw consent places an unreasonable burden on a custodian/trustee, that custodian/trustee will not be expected to fully comply with the request but must take reasonable steps to inform the individual of why they are unable to comply. This requirement to take reasonable steps, *in particular, within the EHR environment* and within larger institutions, such as hospitals recognizes the technical costs to build in "masking" and the potential administrative burden on custodians/trustees.[112]

The reference to administrative burdens is telling as it reflects the primary challenge that arises in giving patients "too much" authority to control their information. The ancillary provisions further state that "[i]ndividuals should not have the ability to instruct the provider to only use non-electronic means (paper, fax, *etc.*) for the purpose of providing health care/health services to the individual."[113]

Other organizations have promulgated guidelines that emphasize the importance of consent. In its *Guidelines for the Protection of Health Information*, COACH, Canada's Health Informatics Association, states:

> Consent forms the basis for the contract between the subject of the information, in this case the client, and the person or organization that collects, uses, discloses, retains, and eventually destroys the information.... All collections, uses and disclosures of information should have the consent of the person who is the subject of the information..., or be specifically prescribed by law or ethical practice. Consent can be implied or explicit.... Implied consent, where well implemented, is supported by openness, transparency and by defined, justified and clearly communicated data uses.[114]

In a statement that recalls the difficulties associated with obtaining consent for Alberta's Pharmaceuticals Information Program, the COACH *Guidelines* advise information custodians to balance "efficiency" with consent: "Care providers and health organizations need to provide sufficient information about the purposes for collecting the information and to whom it will be disclosed, while at the same time not burdening the client with excessive detail."[115] Presumably efficiency concerns arise not just from overloading patients with information, but also consuming too much time for busy health care providers.

Amid complying with laws and applying best practice guidelines, health care providers are bound to observe ethical principles related to privacy and consent. For physicians, the Canadian Medical Association *Health Information Privacy Code* establishes specific principles regarding privacy, confidentiality and security of health information.[116] This *Code*

---

112 *Ibid.* at Appendix A — Ancillary Provisions 5.2 [emphasis added]

113 *Ibid.* at Appendix A — Ancillary Provisions 5.3.

114 Canada's Health Informatics Association, *Guidelines for the Protection of Health Information* (Toronto: COACH, 2004) at 58 [COACH *Guidelines*].

115 *Ibid.* at 59.

116 *Privacy Code*, *supra* note 32.

is focused on maintaining trust necessary to foster a therapeutic relationship between provider and patient. The *Code* is premised on the belief that health information is special, both because it may be very sensitive and also because it is typically revealed to a care provider with an expectation of confidentiality. The *Code* establishes a general principle that patient consent is required for the collection, use and disclosure of identifiable health information: "The patient's ability to decide with whom he or she will share information is crucial for the protection of the right of privacy and for the preservation of trust in the therapeutic context."[117]

The *Code* states that implied consent is appropriate for collecting, using and sharing information "for the primary therapeutic purpose," unless the provider has evidence to believe that a patient would not give consent if asked.[118] Even in situations where a provider would generally rely on implied consent, a patient maintains a right to refuse consent for collection, use and disclosure of his information.[119] This provision raises the question of whether a patient could request a provider not to disclose her information via an EHR, even if the provider would typically do so on the basis of implied consent. Presumably the answer is yes.

Interestingly, the *Health Information Privacy Code* is described as "an ideal to strive for" and opens with the following caution:

> [The Code's] provisions are more exacting than those currently in place in the Canadian health care system. Although a patchwork of laws across Canada permit or require health information collection, use, disclosure and access without patient consent, or even knowledge, this Code would require that all of these laws and any proposed laws be reviewed for consistency with its provisions. Moreover, existing practices and initiatives concerning health information collection, use, disclosure and access, including health information systems or networks, may be contrary to patient expectations and the physician's duty of confidentiality. These practices and initiatives must also be reviewed for consistency with this Code. Many laws, practices and initiatives may not withstand the kind of scrutiny deemed necessary and reasonable for the protection of privacy and the trust and integrity of the therapeutic relationship.[120]

As such, differences in provincial legislation are to be tempered by Medical Association members complying with their *Code*.

VI. INTERNATIONAL INITIATIVES[121]

As with Canada, numerous jurisdictions around the world are investing significant resources into EHR development. This section provides an overview of EHR initiatives in Australia and the United Kingdom, focusing especially on how these jurisdictions have grappled with issues related to consent. Lessons from other jurisdictions may help inform

---

117 *Ibid.*, Principle 5 "Consent."

118 *Ibid.*, Principle 5.3.

119 *Ibid.*, Principle 5.8.

120 *Ibid.* at preamble.

121 The author acknowledges with much gratitude the significant research assistance Elizabeth Robertson provided in regard to international experiences with EHRs.

Canadian policy decisions about how best to implement EHRs in a manner that balances patient privacy with other interests at stake.

A. AUSTRALIA

In 1999, the National Electronic Health Records Taskforce was established in Australia to bring "a coordinated approach to electronic health record systems and to avoid the potential for duplication and incompatible systems."[122] In 2000, the Taskforce issued a consultation paper to seek feedback from health care providers, patients and others on key issues related to the development and operation of a national EHR system.

This early report predicted — perhaps somewhat optimistically — that "consumers will have far greater control over their personal health information than is currently the case with paper-based systems — making them, in effect, empowered gatekeepers of their own health information."[123] The report also states that, to respect legal principles regarding consent, patients ought to have a right to "opt out" of electronic exchanges of their health records.[124] Participation in the national EHR system is not mandatory for patients or health care providers, though the purportedly voluntary nature of the system for practitioners may end up illusory as it has been suggested that they may have a legal duty of care to participate in the system.[125]

By late 2000, Australian health ministers had agreed to commit funding for development of components necessary to create a national EHR infrastructure, known as Health*Connect*.[126] In October 2002, implementation trials began in Tasmania and the Northern Territory, with North Queensland following in November 2003. In March 2004, the national government announced that Health*Connect* would be implemented across the country.

Under the Health*Connect* system, an event summary is created and stored for future access whenever a patient receives health care. The event summary includes information such as test results, diagnosis, care plan, medication and referrals to other care providers. The event summary format allows information to be recorded in a standardized form. A description on the Health*Connect* website asserts that event summaries "contain only the information that is relevant to the future health and care of the consumer, rather than the comprehensive notes that a doctor may keep as a record of a consultation. With the consumer's consent, these event summaries may be retrieved and exchanged at any time via a secure network by an

---

122 National Electronic Health Records Taskforce, *Issues Paper: A National Approach to Electronic Health Records for Australia* (March 2000) at 7, online: Health*Connect* <www.healthconnect.gov.au/pdf/ehr_apxc.pdf>.

123 *Ibid.* at 22.

124 *Ibid.*

125 Danuta Mendelson, "Health*Connect* and the duty of care: A dilemma for medical practitioners" (2004) 12 J.L. & Med. 69.

126 For further information, see Health*Connect*, online: <www.healthconnect.gov.au>. For a timeline of key events in the development of Health*Connect*, see <www.healthconnect.gov.au/about/About. htm>. For some reason unknown to the author, there appears to be an unwritten convention requiring that all EHR initiatives have to be designated by a word with a combination of regular font, italics and capital letters; as in Australia's "Health*Connect*," British Columbia's "*health*netBC," and "netCARE," the regional EHR for Alberta's Capital Health Region.

authorised health care provider."[127] Patients will be able to request that an event summary not be entered onto the system with respect to a particular health consultation. Patients will also be able to request that incorrect information be changed or that a comment be added to an event summary. The patient will also have the ability to request that an event summary be withdrawn from view, but the masked information will remain in the system for audit and litigation purposes.[128]

Final privacy and consent models for Health*Connect* have not yet been finalized. The most current Health*Connect* Business Architecture plan (version 1.9) outlines a broad consent model and privacy framework[129] but many details remain to be worked out.[130] Some commentators are concerned that Australian states are proceeding with Health*Connect* implementation in the absence of a final consent model or privacy code.[131]

The Business Architecture Plan provides the following discussion of patient consent:

> Consumer participation in Health*Connect* will be voluntary ....
>
> The consumer must have given informed consent before their EHR and other personal information can be collected, accessed, used or disclosed by Health*Connect*. ...
>
> A key aspect of the consent process is the creation and maintenance of a list of provider organisations authorized to access the consumer's Health*Connect* record. Organisations not identified on the consumer's access list will not be able to access the consumer's EHR, unless using the emergency override facility. At any time, the consumer will be able to nominate or change the provider organisations that may access their EHR.[132]

To ensure ongoing informed consent, patients would be provided with an opportunity to "opt-in" to Health*Connect* at each clinical interaction and specify whether a particular event can be recorded in the EHR and indicate who may access their online record. The Business Architecture document also speculates that further privacy-enhancing features may be implemented: "In the future, there may also be the opportunity to control access through features such as restriction by provider type and the 'secure' envelope which allows more restricted access for sensitive information, although these are subject to the findings of further research."[133]

---

127 Health*Connect*, "Event Summary," online: Health Connect <www.healthconnect.gov.au/building/Event.htm>.

128 Australian Government Department of Health & Ageing, Health*Connect* Business Architecture version 1.9, at 52, 55, 73.

129 *Ibid.* Overview, online: <www7.health.gov.au/healthconnect/pdf/BAv1-9P2Overview.pdf>.

130 Livia Iacovino, "Networking Electronic Health Records: Issues Arising from the Health*Connect* Initiative" (2004) 12 J.L. & Med. 5 at 7. For an excellent discussion of consent issues associated with the Health*Connect* program, see Health*Connect* Program Office, *Consent and Electronic Health Records: A discussion Paper* (July 2002), online: <www.healthconnect.gov.au/pdf/cons_dp.pdf>.

131 Livia Iacovino, "Trustworthy shared electronic health records: Recordkeeping requirements and Health*Connect*" (2004) 12 J.L. & Med. 40 at 59.

132 *Supra* note 128 at 3, 4.

133 *Ibid.*

Despite these assurances, experience from implementation trials in Tasmania reveals that care providers do not always obtain individual informed consent before recording patient information into the Health*Connect* system. In Tasmania, verbal consent was to be obtained every time a care provider entered an event summary. However, focus groups with participants in the trial implementation process revealed this had not occurred.[134] Patients could not recall having been asked to provide consent and physicians indicated they had not entered the event summary until after the patient left the office and therefore, there was no consent discussion.[135] Physicians also "regarded consent as the consumer's responsibility, expecting consumers to advise the general practitioner if they did not wish an event summary to be submitted to Health*Connect*."[136] It has also been acknowledged that requiring consent at each interaction before a care provider can create a Health*Connect* event summary may be administratively burdensome.[137]

Based on the Tasmanian experience, there has been some discussion in Australia about modifying consent requirements to a "blanket" consent model where patients make a one-time decision to participate in Health*Connect*, rather than specifying preferences at each health care interaction. However, a recent, comprehensive legal analysis commissioned for the Health*Connect* program has cautioned against such a policy: "An 'all or nothing' approach,' that is asking individuals to give blanket consent for any and all future uses of information would not constitute informed consent."[138] The report also observes that "obtaining consent on every occasion before an event summary can be loaded onto the Health*Connect* may not be practicable in different healthcare settings. Notwithstanding this providers are and should be encouraged to check with the consumer during, or at the end of, each episode before sending information about an episode to Health*Connect*."[139]

The ability for patients to opt in and out has raised concern regarding the usefulness and completeness of Health*Connect* records, not only for primary care, but also for secondary uses.[140] The Business Architecture document recommends that consent to participation in Health*Connect* will include consent to secondary use. Patients would be advised that most secondary uses will require anonymous data but that identified data may be used in limited circumstances.[141]

Like Canada, Australia currently has privacy legislation at both the federal and state levels. The *Federal Privacy Act 1988* outlines the National Privacy Principles.[142] In addition,

---

134 Bernadette McSherry, "Ethical Issues in Health*Connect*'s shared electronic record system" (2004) 12 J.L. & Med. 60 at 66; *Vol. 3 Background documents, Part Three, Tasmania Health Connect Trial Interim evaluation report* (February 2003) at 73, online: Health Connect <www.healthconnect.gov.au/pdf/v3-3.pdf> [Tasmania Trial].

135 Tasmania Trial, *ibid.*

136 *Ibid.*

137 Health*Connect*, *Legal Issues Report: Summary of Key Findings and Recommendations* (January 2005), online: Health Connect <www.healthconnect.gov.au/pdf/lirsummary_web2.pdf> at 40.

138 *Ibid.* at 41.

139 *Ibid.* at 40.

140 Moira Paterson, "Health*Connect* and privacy: A policy conundrum" (2004) 12 J.L. & Med. 80 at 84.

141 Health*Connect* Business Architecture version 1.9, *supra* note 128 at 53.

142 The National Privacy Principles in Australia are: collection, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, transborder data flows and sensitive information. For further information, see Office of the Federal Privacy Commissioner of Australia,

three jurisdictions – Victoria, New South Wales and the Australian Capital Territory – have specific health privacy legislation and Western Australia is currently developing privacy legislation. Queensland, Tasmania and South Australia have protocols that establish privacy rules for health information.[143] With this overlapping legislation, there is concern that the current legislative framework will result in inconsistent privacy rules for Health*Connect*.

A National Health Privacy Code has been proposed to address the problem of overlapping federal and state legislation.[144] Akin to the Canadian effort to develop a health information and privacy framework that can be applied across the country, a key goal of Australia's proposed Code is "to achieve national consistency in the handling of health information across the private and public sectors."[145] The Code sets out a general principle that organizations must only collect information necessary to carry out its functions, and with express or implied consent of the subject individual.[146] An organization may use and disclose personal information without consent for the purposes for which it was collected. As presently drafted, the Code has no specific provisions related to EHRs and there has been debate about whether Health*Connect* participants will be required to adhere to it.[147]

B. THE UNITED KINGDOM

The United Kingdom National Health Service (NHS) is in the process of implementing the National Programme for Information Technology, an ambitious project that aims to "connect over 30,000 GPs in England to almost 300 hospitals and give patients access to their personal health and care information, transforming the way the NHS works."[148] This Programme, with a price tag of US$11 billion,[149] consists of various elements, including: the Care Records Service, the national EHR initiative; electronic prescription transmission;[150] the Secondary Uses Service, which will "pseudonomize" patient data to make it available for research and other purposes not related to direct patient care;[151] and GP2GP, an initiative to support transfer of patient electronic records from one general practice to another when a patient registers with a new practice.[152]

National Privacy Principles, online: <www.privacy.gov.au/publications/npps01.html>.

143 Colin Thomson, "The Regulation of Health Information Privacy in Australia" (January 2004), online: National Health and Medical Research Council <www.nhmrc.gov.au/publications/synopses/nh53syn.htm>.

144 The National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, "Proposed National Health Privacy Code" (August 2003), online: Department of Health & Ageing <www7.health.gov.au/pubs/nhpcode.htm>.

145 *Ibid.*, Part 1 — Preliminary, 2(a).

146 *Ibid.*, Appendix 1, National Health Privacy Principles, cl. 1.1.

147 *Vol. 2 Research Reports: Research Report 5: What will be necessary to manage privacy?* Health*Connect* Interim Research Report (April 2003) at 9, online: <www.healthconnect.gov.au/pdf/v2-5.pdf>.

148 National Health Service, *National Programme for IT in the NHS* (July 2005), online: <www.connectingforhealth.nhs.uk/>.

149 Michael Humber, "National Programme for information technology: Is sorely needed and must succeed – but is off to a shaky start" (2004) 328 British Medical Journal 1145.

150 For further information, see online: NHS <www.connectingforhealth.nhs.uk/programmes/etp/>.

151 For further information, see online: NHS <www.connectingforhealth.nhs.uk/delivery/programmes/sus/>.

152 For further information, see online: NHS <www.connectingforhealth.nhs.uk/programmes/gp2gp/>.

This project is part of a ten-year process of National Health Service reform that began in July 2000.[153] The move to implement a national EHR system was also inspired, in part, by a 2002 report that found that without a national EHR system, the health service would find it increasingly difficult to deliver high quality care. A number of separate EHR systems had already been created at local levels, but these systems were unable to share information with each other. The complex nature of health care and the need for immediate access to current information prompted the move to a national system.[154]

The Care Records Service will eventually include personal patient details, such as name, date of birth, health care number and a complete health care history. The history will include treatment summaries, medication history, allergies and consent forms.[155] The Care Records Service is being implemented at both national and local levels. A national service provider will be responsible for services that are common to all users, including GPs, hospitals and other health care facilities. A national database, referred to as the "spine" of the system, will contain basic patient information such as name, birth date, allergies, adverse drug reactions and NHS number.

At the local level, England has been divided into five clusters and each area will have its own service provider to deliver local services. The local EHR will contain more detailed information than the national database, including medication records, test results, and disease history. The national database system will be able to link to local EHRs.[156]

The Care Records Service is currently in its first phase, which will allow general practitioners to book appointments at hospitals electronically and will create an electronic record of basic patient information. The second phase, expected to be complete by summer of 2006, will allow access to more detailed records, allow electronic requests for pathology tests and diagnostic imaging, and access to emergency records. From 2006 to 2008, it is planned that electronic prescribing will be implemented, along with further decision-making supports for health care providers. The full implementation of the project is expected by 2010 and will include integration of health and social care records in the U.K.[157]

The implementation of the Care Records Service was preceded by the Electronic Record Development and Implementation Programme (ERDIP) that began in 2000. This program, which concluded in 2003, tested various aspects of the use of EHRs in 17 communities and evaluation results are being used to inform the implementation of the Care Records Service.[158] As part of the ERDIP trials, privacy and consent issues were studied and a number

---

153 National Programme for Information Technology, *NHS Care Records Service*, online: NHS <www.connectingforhealth.nhs.uk/delivery/programmes/nhscrs>.

154 Humber, *supra* note 149.

155 The NHS Confederation Briefing, "The NHS Care Records Service" (20 August 2004) at 7, online: <www.nhsconfed.org/publications> at 2.

156 *Ibid.* at 3.

157 *Ibid.* at 7.

158 NHS Information Authority, "Background to ERDIP" (April 2003), online: <http://webarchive.org/web/20030407025607/www.nhsia.nhs.uk/erdip/pages/backgroundtoerdip.asp>.

of reports issued.[159] With respect to public concerns about privacy and EHRs, a consumer association survey found that patients were primarily concerned that third parties outside the NHS might access their health records.[160] In the Hampshire and Staffordshire ERDIP trials, leaflets were distributed to inform the population of the EHR project, but this resulted in only about one-third of households being aware of the project.[161] In Hampshire, a website was established to allow people to opt-out or express concerns, but usage of the website was very low. In Staffordshire, a survey revealed that nearly 80 percent of respondents were comfortable with personal information being stored in an EHR.

Analysis of legal issues related to the Care Records Service has also focussed primarily on matters of consent and security. Indeed, there is a great deal of concern that patient records will not be kept confidential and that it will be impossible to obtain informed consent from patients before transfer of patient records to the national database. Physicians in England, represented by the British Medical Association, have been a vocal source of concern. A poll conducted in February 2005 found support for the Care Records Service was dropping among GPs and consultants in England.[162] Only 21 percent of GPs and 51 percent of consultants were in favour of the project. Only 2 percent of GPs thought electronic records would be more secure than the current system. The British Medical Association has advised doctors to avoid participation in the electronic booking system due to concerns about confidentiality.[163] In a 2004 speech, the Chairman of the British Medical Association's information technology committee stated that physicians had not been sufficiently consulted about plans to implement a national EHR system.[164]

The U.K. project has also been plagued with confusion over whether participation in the Care Records Service will be voluntary. Media stories have suggested that patients will require approval from their general practitioner to opt out of the system.[165] In addition to issues of voluntary participation, it has been unclear how much control patients will have over the material placed in the EHR. It has been stated that control over what goes into the

---

159 See *e.g.* Department of Health, Information Policy Unit, *Legal and Policy Constraints on Electronic Records: Requirements Report*, version 1.1 (March 2002) and Department of Health, Information Policy Unit, *Legal and Policy Constraints on Electronic Records: Options Report*, version 1.2 (March 2002); NHS Information Authority, *ERDIP Update March 2003*; NHS Information Authority, *ERDIP:Lessons Learned Final Report* (April 2003); *ERDIP: EHR Issues and Lessons Learned Report* (October 2002), online: <http://webarchive.org/web/20030416030731/www.nhsia.nhs.uk.erdip/pages/default.asp>.

160 Parliamentary Office of Science and Technology, "New NHS IT" (2004) 214 *Postnote* at 4, online: <www.parliament.uk/documents/upload/POSTpn214.pdf>.

161 Trina Adams *et al.*, "Lessons from the central Hampshire electronic health record pilot project: issues of data protection and consent" (2004) 328 British Medical Journal 871 at 873.

162 Lucy Sherriff, "GPs have no faith in £6bn NHS IT programme" *The Register* (8 February 2005), online: <www.theregister.co.uk/2005/02/08/npfit_gp_lose_confidence>; John Carvel, "Doctors fear £6bn IT project will be a fiasco" *The Guardian* (8 February 2005), online: <www.guardian.co.uk/uk_news/story0,,1407870,00.html>.

163 Lucy Sherriff, "BMA tells doctors: avoid NPfIT's flagship project" *The Register* (23 November 2004), online: <www.theregister.co.uk/2004/11/23/bma-bpfit/>; John Carvel, "Secrecy worries hit NHS scheme" *The Guardian* (23 November 2004), online: <www.guardian.co.uk/uk_news/story/0,,1357483,00.html>.

164 Speech from the Chairman of the IT Committee, Dr. John Powell (1 July 2004), online: British Medical Association <www.bma.org.uk/ap.nsf/Content/ARM04chIT?OpenDocument&Highlight=2,john,powell>.

165 John Lettice, "NHS chief cans patient control over health record access" *The Register* (30 March 2005), online: <www.theregister.co.uk/2005/03/30/nhscrs_optout_canned/>.

record will be the responsibility of the general practitioner, although patients will be able to discuss what is included with the GP.[166] In addition, there has been some discussion about creating "secret envelopes" for confidential data that a patient may wish to withhold from general access in the Care Record.[167]

In an effort to remedy this confusion, the National Health Service issued a "Care Record Guarantee" in May 2005 that sets out patient rights and health provider obligations in regard to privacy and confidentiality of health care records. This guarantee explains and assures that "[a] modern computer system is being introduced in the NHS over the next few years. It will hold electronic health records about you securely, making them available to the right people where and when they are needed for your health care, while maintaining your confidentiality."[168] The document establishes that patient information will be held electronically and shared with others involved in the patient's care, but will not be disclosed to third parties except with the patient's consent, or where necessary to comply with legal obligations. While the guarantee does not permit patients to withhold consent for compiling and storing their information electronically, patients may "choose not to have information in your electronic records shared."[169] The document further advises that, "[i]n helping you decide, we will discuss with you how this may affect our ability to provide you with care or treatment, and any alternatives available to you."[170] According to at least one commentator, the implication of this is that "UK doctors will be expected to spend time in every consultation discussing with patients what information about them is shared across NHS computers."[171]

However, at a British Medical Association Conference held the day after the Care Record Guarantee was released, the Deputy Chair of the Care Records Development Board advised that the document was still under revision and the Board recommends that patients not be given a choice to opt out of the national EHR scheme.[172] However, the Board supports a patient's right to exercise some control over disclosure of information contained in the EHR.[173]

The overall scope of the NHS information technology program is vast and early confusion and controversy about the nation-wide EHR initiative is perhaps not surprising. However, on an optimistic note, a recent British Medical Journal editorial has likened the twenty-first century creation of a national health information technology program to construction of

---

166 *Ibid.*

167 Susanne Mccabe "Very serious concerns are played down in this Editoral"; John R. Williamson, "No consent for EPR"; Peter Fletcher, "NHS IT system — problems ahead!" Correspondence published online in (January 2005) 330 British Medical Journal <http://bmj.bmjjournals.com/cgi/eletters/330/7484/164-a>.

168 NHS, *The Care Records Guarantee: Our Guarantee for NHS Care Records in England* at 3, online: National Health Service <www.connectingforhealth.nhs.uk/all_images_and_docs/crbb/crs_guarantee_2.pdf>.

169 *Ibid.*, Point #6 at 5.

170 *Ibid.*

171 Michael Cross, "UK patients can refuse to let their data be shared across networks" (2005) 330 British Medical Journal 1226.

172 "Comments wanted on Care Record Guarantee" (26 May 2005), online: E-Health Insider <www.e-health-insider.com/news/item.cfm?ID=1226>.

173 *Ibid.*

London's sewer system, "one of the wonders of 19th century civil engineering."[174] If the government manages to implement the extensive IT program for the NHS, "it will be like the sewers: we'll wonder how we ever did without them."[175]

VII. MOVING FORWARD: MANAGING CONSENT IN THE CONTEXT OF ELECTRONIC HEALTH RECORDS

Canada's federal Privacy Commissioner has described informed consent as "the backbone of our net of privacy principles and practice – the glue that holds the fair information principles together."[176] Yet, as Canadian and international experiences attest, the application of legal rules and ethical imperatives regarding informed consent to collection, use and disclosure of one's personal health information is challenging in the context of EHRs. This challenge arises from the fact that it may be largely impossible to obtain truly informed consent from a patient regarding uses and disclosures of her or his information via an EHR, particularly as all future uses of information on the EHR cannot be foreseen when the individual's personal information is initially put into the system.[177]

However, legal rules, ethical duties and best practice guidelines generally require knowledgeable consent to authorize collection of personal health information, and express consent is the most appropriate form of consent when sensitive information, such as health information, is involved. To comply with this requirement, it is preferable to obtain a patient's express, informed consent for at least the initial collection of personal health information that will be added to an EHR.

To give informed consent, an individual must have sufficient information about what it is they are being asked to give consent. In the EHR context, this would include details about the scope of the EHR system, including who has access to information in the EHR, for what purposes, and what security measures are in place to protect the information. Risks and benefits of consenting or refusing consent would need to be discussed. Individuals may also want an option to exclude specific health care details from an EHR network or permit access to only specified health care providers. These requests may arise in regard to information that is considered especially sensitive, such as diagnoses and treatment for psychiatric conditions, information about reproductive health (such as abortion or sexually transmitted diseases), and information (including genetic test results) that reveals a predisposition to particular diseases. As one Alberta physician has stated:

---

174 Jane Smith, "The NHS's sewers?" (August 2005) 331 British Medical Journal at 2, online: <http://bmj.bmjjournals.com/cgi/reprint/331/7512/0-f>.

175 *Ibid.*

176 Stoddart address, *supra* note 43.

177 For further discussion of the consent challenge in the EHR context, see Office of the Privacy Commissioner of Alberta, *Consent Issues with respect to the Electronic Patient Record*, by Frank Work, Q.C. (October 2002) [on file with author].

> In this electronic age, the notation of a problem such as ethanol abuse, depression or unexpected pregnancy must be carefully guarded. In my opinion, this element of the medical record should never be automatically introduced into the societal "electronic health record."[178]

Although the consent process is a critical one, it is not anticipated, based on scarcity of time and lack of technical knowledge, that health care providers will have a lengthy conversation with a patient at each visit to explain details regarding the EHR system. To meet the requirement for knowledgeable consent, some entities are developing educational materials such as pamphlets and posters that explain the nature of the EHR system. Yet, it is important to keep in mind that consent typically is interpreted as having both an objective and a subjective component. That is, to obtain informed consent, a health care provider must provide information that a reasonable person in the patient's position would want to know. Some patients, particularly those who are "privacy fundamentalists," may want additional detail about how information will be shared and protected and may want to withhold consent for including their information on an EHR. Other patients who are technologically savvy may also want detailed information about the system's security measures. In each case, providers ought to have more detailed information available for those patients who seek it.

Once a patient gives initial informed consent regarding inclusion of their information in an EHR, it is arguable that subsequent uses and disclosures of that information for the purpose of treating that specific patient can proceed on the basis of implied consent. To require express consent for every use and disclosure of a patient's information via EHRs within a circle of care would likely grind health care delivery to a halt and undermine the very benefits that EHRs are designed to provide. However, as suggested above, a patient's interpretation of "circle of care" may differ from that of health care providers, so it is prudent to give patients notice of the range of entities that may be involved in sharing personal information for health care purposes.

The most challenging privacy and consent issues that may arise relate to secondary uses and disclosures of personal information in EHRs for purposes such as research. While most patients accept and support sharing of their personal information to provide them with care, many have concerns about subsequent uses of data. One study indicated that only 31 percent of patients surveyed agreed that researchers "should be able to get their medical records without permission" and only 35 percent support computerized databases to provide data for medical research.[179] If patients could specify who could access the database and were assured security measures to protect the database were effective, support increased to 71 percent. If the database was both secure and contained only de-identified personal information, 85.9 percent of patients expressed approval.[180]

---

178 Steven M. Edworthy, "The problem list: A sacred trust" (March/April 2003) 28:2 *Alberta Doctor's Digest* 25 at 26. The EHR is described as a "societal" record because "it will be accessible at multiple points of care, by individuals who may not have a direct caring role for the patient and, in settings somewhat open to the public, where the record may be seen by others who are only tangentially involved with health care provision" (at 26).

179 Nancy Kass *et al.*, "The Use of Medical Records: What Do Patients Want?" (2003) 31 J.L. Med. & Ethics 429 at 430-31.

180 This study, as well as other studies regarding individual views about participation in health research, are summarized in Caulfield & Ries, *supra* note 37 at 15.

Secondary uses of identifiable health information in EHRs should generally be authorized by informed patient consent.[181] For consent to be informed, an individual must have details regarding the nature of the secondary use and it is likely not legally sufficient for the entity that initially collects the health information simply to advise the patient that information may be used for other purposes, such as research, and imply future consent based on that notification. The more general the consent becomes, the less it complies with legal and ethical principles. It is important to note that information that is not reasonably capable of identifying an individual is outside the scope of privacy laws throughout Canada. As a result, legislative consent rules will not apply, but debate remains about the nature and extent of a patient's interest in de-identified information.[182] When informing patients about potential uses of information in EHRs during the consent process, it would be prudent to advise whether information – both identified or de-identified — may be used for secondary uses and explain what opportunity, if any, the patient will have to consent to those future uses.

VIII. CONCLUSION

As technological capacity advances, it is foreseeable that electronic health records will eventually become the norm for storing and sharing patient health information across various health care providers and facilities, as well as for those engaged in health system planning and research. While this trend has the potential to enhance patient care, it also brings with it the possible diminution of patient privacy.

In the face of increasing public concern regarding privacy of personal information, governments at federal, provincial and territorial levels in Canada have enacted a range of privacy laws across public and private sectors. As EHR systems are still under development in Canada, much remains to be seen as to how privacy legislation will affect implementation of EHRs. At present, there is clearly a lack of national uniformity in regard to legislative regimes that apply to collection, use and disclosure of health information, including via EHR systems. As a result, organizations that seek to advance EHRs must be aware of various legislative rules and develop and follow principles and processes that will satisfy their legal obligations. Continued efforts to develop a pan-Canadian health information privacy framework may assist organizations in this regard. Yet, as the federal Advisory Council on Health Infostructure has stated, "harmonization should not aim at some lowest common denominator with respect to privacy, but toward full, effective and enforceable privacy protection."[183]

It has been suggested that legal and ethical rules are an impediment to the development of EHRs. For example, Gibson has pointed out the following statement in the Kirby Report: "According to witnesses, the implementation and full deployment of the pan-Canadian Health Infostructure faces three major barriers: the protection of personal information, legal

---

181 Some privacy legislation permits waiver of informed consent where it would be impracticable for investigators to contact persons to seek consent. Typically, such a waiver must be approved by a research ethics board or a privacy commissioner. For further discussion, see Caulfield & Ries, *ibid.* at 47.

182 See *e.g.* Gibson, *supra* note 40.

183 Federal Advisory Council on Health Infostructure, *Canada Health Infoway: Paths to Better Health Final Report* (1999), at "Other Requirements," online: Health Canada <www.hc-sc.gc.ca/hcs-sss/pubs/ehealth_esante/1999-paths-voies-fin/index_e.html>.

and ethical issues, and the interoperability of the various systems."[184] However, Gibson observes that "[i]nstead of viewing the protection of information as a 'barrier', strict privacy and security regimes must be understood as essential to maintaining the trust of members of Canadian society that our personal health information is receiving the highest of protection."[185]

The experiences examined in this article suggest that legislators and policy makers who are charged with developing privacy and consent frameworks for EHR initiatives often begin with a strong commitment to stringent consent processes but, over time, tend to attenuate consent rights to achieve less costly and cumbersome implementation of EHRs. To date, we have already seen legislative changes in Alberta's and Saskatchewan's health information laws that have amended consent rules and, in effect, diminished patient control over the collection of their information into EHRs. However, it is arguable that consent rules that impose unrealistic demands on health care providers, and perhaps demand unrealistic decisions from patients, warrant revision.

While there may be legitimate reasons for moving away from strict consent procedures for each collection, use and disclosure of information via EHRs, there is every need to develop and apply stringent security mechanisms to safeguard patient information in EHRs. Indeed, to the extent consent rights are weakened, there is a correspondingly stronger obligation to ensure security of personal information. As Lawrence O. Gostin emphasizes: "If society truly believes the utility of health information warrants building automated and linked systems, it must reckon with the potential diminution in privacy. One method of affording some measure of privacy protection to patients would be to furnish rigorous legal safeguards."[186] As EHRs expand locally, provincially and nationally in Canada, those involved in establishing privacy rules, consent processes and security systems must heed this advice, lest they fuel the criticism that computers – and the humans who run them – just screw things up.

---

184 Kirby Report, *supra* note 23.

185 Elaine Gibson, "Jewel in the Crown? The Romanow Commission Proposal to Develop a National Electronic Health Record System" (2003) 66 Sask. L. Rev. 647 at 665.

186 Lawrence O. Gostin, "Health Information Privacy" (1995) 80 Cornell L. Rev. 451 at 494.