

# Legal Protections of Electronic Health Records: Issues of Consent and Security

*Nola M. Ries & Geoff Moysa*<sup>1</sup>

## **Introduction**

Electronic health records (EHRs) – comprehensive compilations of a person’s health care history, accessible by health care providers and others through electronic networks<sup>2</sup> – are a growing issue in Canada. In 2002, the Kirby Report<sup>3</sup> and the Romanow Report<sup>4</sup> made EHRs hot topics for media and policymakers by recommending their national implementation. While both reports recognized the potential of EHRs to improve health care delivery and enhance health system reform, they were also sensitive to growing concerns over the privacy of personal health information.<sup>5</sup> In this paper, we discuss how health information protection laws in Canada seek to provide specific safeguards for personal health data collected, used and disclosed by electronic means. We begin with an overview of EHR initiatives in Canada and other jurisdictions. Next, we discuss some of the purported benefits and risks associated with EHRs. We then identify and comment on specific legal protections that have been enacted to address concerns regarding privacy and security of health information on electronic networks. In particular, we focus on statutory provisions that permit individuals to limit the inclusion and disclosure of their information via EHRs and that oblige those responsible for EHRs to implement specific technical measures to safeguard against unauthorized access and disclosure. We conclude by commenting on the competing interests legislators must balance in enacting legal protections for EHRs.

## **Overview of EHRs Initiatives in Canada and Abroad**

Even before the Romanow and Kirby recommendations, EHR initiatives were well underway across Canada. Manitoba and Saskatchewan started basic planning in 1995, and by 1999, federal coordination efforts had commenced. In its final report, the Advisory Council on Health Infostructure recommended the creation of Canada Health Infoway, a not-for-profit corporation designed to create and synchronize EHR initiatives nationally.<sup>6</sup> In 2000-2001, the federal government committed \$500 million to Infoway to fulfill this mandate.<sup>7</sup> To date, Infoway has invested \$158 million in 17 initiatives across Canada.<sup>8</sup>

Alberta’s Wellnet program is currently the most comprehensive of these initiatives, aiming to combine medical and prescription histories, allergies and lab test results by 2005. A \$50,000 fine exists for improper use.<sup>9</sup> The Saskatchewan Health Information Network is also reaching an advanced stage, projecting basic EHRs to be available in all regions by 2006.<sup>10</sup> Manitoba had linked five hospitals to its pilot Health Information Network by 1998, but program implementation has since stalled. British Columbia’s *healthnetBC* is a newer project integrating five current EHR initiatives and numerous regional databases.<sup>11</sup> These western provinces, along with Network 99 in the Northwest Territories, Nunavut and Yukon, are coordinated regionally by the Western Health Information Collective.



Ontario established its Smart Systems for Health Agency in 2002, aiming to connect 24,000 sites across the province.<sup>12</sup> In 2004, Quebec became a partner in the Infoway corporation in order to develop an EHR system.<sup>13</sup> The Maritime provinces are all in similar stages of EHR development under the coordination of Health Infostructure Atlantic.<sup>14</sup>

Extensive EHR pilot projects are also being undertaken internationally. In 2003, the United Kingdom's National Health Service completed its three-year Electronic Record Development and Implementation Programme, in which health communities across England carried out detailed trials of EHR use. The trial results are currently being used to shape the construction of the nation-wide Integrated Care Records Services, a public initiative that aims to have a comprehensive EHR system online by 2008.<sup>15</sup>

Trials are underway in Australia for the proposed Health *Connect* system, a national infrastructure intended to coordinate the development of standardized EHRs. Starting in 2001, national, state and territory governments commenced a research and trial phase for the project, with implementation expected to begin in 2005.<sup>16</sup>

European Union countries such as Italy, France and Germany are also currently researching EHR initiatives.<sup>17</sup> Although numerous EHR initiatives exist in the United States, no comprehensive national coordination program exists, nor is one currently in development. However, in April 2004, the Bush administration announced a goal to have a purely voluntary national EHR program implemented within ten years.<sup>18</sup>

## **Benefits and Risks of EHRs**

The pivotal role ascribed to EHRs by Romanow and Kirby may be warranted. Academic and technical literature suggests that EHR implementation could greatly improve health care delivery to individual patients.<sup>19</sup>

Surveys have shown that medical professionals have long-recognized the need to share accurate patient health

information quickly and easily across different health systems.<sup>20</sup> Lawrence Gostin argues "the ability of the health care system to function effectively depends in part on the accuracy, currency, completeness, and availability of health data."<sup>21</sup> High injury levels occur internationally as a result of medical information errors.<sup>22</sup> Accessible medical records significantly decrease the risk of these events, allowing clear medical information to be shared among health care providers and facilities.<sup>23</sup>

*"By improving and standardizing the communication between patients and health providers, patients can make more informed choices among health options, thus enhancing patient autonomy."*

By improving and standardizing the communication between patients and health providers, patients can make more informed choices among health options, thus enhancing patient autonomy. EHRs also have the potential to advance health care research, improve public health functions such as disease monitoring and cut costs in health systems by scrutinizing areas that need improvement.<sup>24</sup> Some commentators identify a related economic imperative: "the primary driving force behind

health care networks is that they will help institutions survive as economic (even if they are nonprofit) entities."<sup>25</sup>

This increased flow of information, however, raises significant concerns about the privacy and confidentiality of health information. Patient records would no longer be singular paper documents kept in a locked filing cabinet. They would instead be stored on multiple computers and servers, prone to weaknesses in electronic security and human judgment.

Implementation poses one of the most obvious obstacles. Some government agencies and health informatics experts are cautious about implementing a system using current privacy and encryption protocols, citing the "heavy reliance [the Public Key Infrastructure] places on governance and policy management and on users maintaining the confidentiality of their key."<sup>26</sup> Elaine Gibson points out that planning, selection and training are often not carefully executed prior to implementation, resulting in health care providers with weak skills in using EHR systems.<sup>27</sup> Arguments have also been made that rapid health care leadership turnover leads to repeated tactical errors in EHR implementation.<sup>28</sup>



These weaknesses in EHR implementation and security have serious implications for health care and individual patients. Patients' concerns over confidentiality and privacy of their records may erode the trust between patient and physician, potentially discouraging patients from fully disclosing their medical problems.<sup>29</sup> This breakdown makes providing proper medical care impossible.<sup>30</sup>

Beyond basic issues of trust, the improper disclosure of confidential health information can have harmful personal consequences for patients. Certain medical conditions have a powerful stigma attached to them that can have destructive effects on a patient's employment opportunities, insurance coverage, and psychological well-being.<sup>31</sup> This information often makes its way into the databases of thousands of private data mining companies that compile and sell lists of individuals with specific conditions for marketing purposes.<sup>32</sup>

Finally, some commentators have questioned the general consensus that the benefits of EHR will outweigh their inherent risks. There 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.<sup>33</sup>

## Legal Protections

Lawrence Gostin asserts that "[i]f 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."<sup>34</sup> In recent years, several Canadian provinces have enacted health information privacy legislation that establishes rules governing the collection, use and disclosure of personal health information. Manitoba enacted its *Personal Health Information Protection Act*<sup>35</sup> in 1997, Alberta's *Health Information Act*<sup>36</sup> came into force in 2001, and Saskatchewan followed suit implementing its *Health Information Protection Act*<sup>37</sup> in September 2003. Ontario's *Health Information Protection Act* came into force on November 1, 2004.<sup>38</sup> While other jurisdictions in Canada do not have specific health information legislation, they have public sector and/or private sector privacy laws that may also apply to health information.<sup>39</sup> However, we focus here on specific health information statutes.<sup>40</sup>

Interestingly, Canadian health information laws all contain provisions that specifically address EHRs. As discussed below, these provisions address issues of individuals' consent to have their personal health information included and shared in EHR systems as well as the obligations of custodians<sup>41</sup> to take steps to protect the security of this information. While speaking to general provisions of privacy legislation, we focus primarily on these two issues of consent and security. As one commentator suggests:

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.<sup>42</sup>

## Consent

Health information statutes start from a general principle that identifiable health information should only be collected, used and disclosed with the consent of the subject individual.<sup>43</sup> The statutes set out a number of exceptions to this rule. A key area of debate in regard to EHRs is whether individual consent is required before information is included in an EHR and/or disclosed to others through this mechanism.

To respect individuals' interest in safeguarding the privacy of their health information, some argue that explicit patient consent ought to be required before information is placed on an EHR. For consent to be legally valid, it must be informed, which requires that an individual have adequate information about the nature, risks and benefits of the matter to which they are being asked to consent.<sup>44</sup> To give informed consent to the inclusion of their health information in an EHR, a person would require details about, for example, who will have access to the data and for what purposes, security mechanisms to thwart unauthorized access, and other information relevant to the benefits and risks of consenting. Consent is not necessarily an all-or-nothing proposition. As a result, some EHR systems may permit individuals to exclude sensitive information from the EHR and/or limit access to their record to specified individuals.<sup>45</sup>

The preamble to Manitoba's *PHIA* notes 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.<sup>46</sup> *PHIA*, however, also permits a trustee to disclose 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 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.<sup>47</sup>

*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.<sup>48</sup> It may be arguable that this provision empowers individuals to direct a trustee not to disclose information to a computerized health information network that others may access for the purpose of providing care. However, it can be countered that the right to restrict disclosure only applies to disclosure to a particular person, not to a health information network that likely has multiple purposes, including facilitation of care delivery, as well as program monitoring and payment.

Saskatchewan's *HIPA* allows the Saskatchewan Health Information Network (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 who hold personal health information)<sup>49</sup> to create a full health history for a particular individual that may be accessed by other trustees.<sup>50</sup> When *HIPA* was first implemented, it gave individuals the right to direct that a trustee not store their specified information on the SHIN network.<sup>51</sup> This provision was removed in 2003 and an individual no longer has this explicit right. However, individuals 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.<sup>52</sup>

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<sup>53</sup> or consent is not required.<sup>54</sup> Thus, *HIPA*'s consent

requirements allow both individuals and trustees to exert some control over disclosure of information through SHIN.

When Alberta's *HIA* first came into force, it included a provision, section 59, that required consent from individuals before their health information could be disclosed electronically.<sup>55</sup> For consent to be valid under *HIA*, it must 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.<sup>56</sup>

In 2003, the provincial government removed section 59, an amendment not opposed by the Alberta Information and Privacy Commissioner. Indeed, the Commissioner acknowledged that the costs of complying with this legislative

*"When legislative amendments diminish individual rights to control their information in EHRs, greater attention must be placed on security measures that will protect the confidentiality of personal health information."*



requirement (namely, the extra time spent by health care providers to obtain patient consent) outweighed its value.<sup>57</sup> 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.”<sup>58</sup> Indeed, one report states that in a pilot project for Alberta’s Pharmaceuticals Information Network, “doctors were taking more than 30 minutes to explain the system, driven by concerns about professional liability.”<sup>59</sup> 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.”<sup>60</sup> Consequently, consent can never be truly informed according to legal standards that require full disclosure.

The Canadian experience to date reveals concern on the part of legislators with enacting statutory provisions in health information laws that explicitly address privacy concerns regarding EHRs. By giving individuals legal rights to exercise some choice about the extent to which their information may be included in or disclosed via EHRs, individuals maintain a degree of control. However, legislators are also clearly influenced by operational challenges that arise when the law requires individual consent regarding EHRs. When legislative amendments diminish individual rights to control their information in EHRs, greater attention must be placed on security measures that will protect the confidentiality of personal health information.

## Security

All Canadian health information statutes contain explicit provisions regarding security of EHRs. Manitoba’s *PHIA* requires trustees to adopt “reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy, and integrity” of personal health information.<sup>61</sup> Additional safeguards are required for information held electronically.<sup>62</sup> The Personal Health Information Regulation enacted under *PHIA* requires trustees of health information to ensure that electronic health information systems can generate an electronic record of successful and unsuccessful attempts to access, modify or delete information and record all transmissions of information.<sup>63</sup> Trustees must routinely review these records to identify potential security breaches.<sup>64</sup>

Similarly, in accordance with Saskatchewan’s *HIPA*, trustees “must establish policies and procedures to maintain

administrative, technical and physical safeguards ... [to] protect the integrity, accuracy and confidentiality of” personal health information.<sup>65</sup>

Alberta’s *HIA* imposes an obligation on custodians to “take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards” to protect confidentiality of information and guard against unauthorized access, use or disclosure.<sup>66</sup> The statute stipulates that safeguards “must include appropriate measures (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records”<sup>67</sup> *HIA* also requires custodians to submit to the Information and Privacy Commissioner privacy impact assessments that describe “how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.”<sup>68</sup> The Commissioner’s review of the assessment is required before the custodian implements any new system or practice.<sup>69</sup>

Ontario’s new legislation authorizes the creation of regulations that establish requirements for “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.”<sup>70</sup> The legislation comes into force on November 1, 2004 and no regulations have yet been enacted under the new statute.

While these provisions are expressed in broad language, they are notable in placing clear obligations on custodians to implement appropriate security measures to protect personal health information. The specific references to risks associated with EHRs reflect the concern that

[m]odern 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.<sup>71</sup>

In light of these risks, Canadian legislators have chosen to emphasize that special attention to EHR security is neces-



sary. Custodians who fail to implement reasonable safeguards may be subject to investigation and penalty by the provincial Information and Privacy Commissioner.<sup>72</sup>

## Striking a Balance

Legislation directed specifically at health information is still relatively young in Canada and EHR projects are similarly in relatively early stages of development and implementation. Consequently, the practical benefits and limitations of both remain largely to be seen. Even in this early stage, though, it is clear that legislators must strike a balance between competing interests. While EHRs may hold promise for improving health care delivery, they also raise concerns regarding privacy and confidentiality. Similarly, health information statutes that impose consent requirements for collection and disclosure of information via EHRs may create operational challenges for custodians. Again, an appropriate balance must be struck to preserve some individual control over personal health information while remaining conscious of the resources necessary to administer an EHR system in which individuals can place various restrictions on inclusion and disclosure of information. As individual control over personal health information attenuates, custodians must focus greater attention on security mechanisms to preserve a necessary degree of confidentiality. If implemented prudently, and within an appropriate legislative regime, EHRs will potentially improve health care delivery while safeguarding individuals' interests in their personal health information.

1. Nola M. Ries is a research associate with the University of Alberta Health Law Institute and an instructor with the School of Health Information Science at the University of Victoria. Geoff Moysa is a law student at the University of Toronto and a former student research assistant with the Health Law Institute.
2. EHRs are to be distinguished from electronic patient records, which are held by individual health care providers and reflect only a portion of the patient's health care history.
3. Canada, Standing Senate Committee on Social Affairs, Science and Technology, *The Health of Canadians – The Federal Role*, vol. 6 (Ottawa: Standing Senate Committee on Social Affairs, Science and Technology, 2002) (Chair: Hon. Michael J.L. Kirby) [Kirby Report].
4. 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.), online: Commission on the Future of Health Care in Canada <<http://www.healthcarecommission.ca>> [Romanow Report].
5. For example, the Romanow Report suggested an amendment to the *Criminal Code of Canada* to make the abuse of private health information a criminal offence. For a critique of this proposal, see Elaine Gibson, *infra* note 27.
6. Canada, Advisory Council on Health Infostructure, *Canada Health Infoway: Paths to Better Health. Final Report* (Ottawa: Advisory Council on Health Infostructure, 1999), online: Health Canada eHealth Resource Centre <[http://www.hc-sc.gc.ca/ohih-bis/about\\_apropos/hcpubssc\\_e.html#reports](http://www.hc-sc.gc.ca/ohih-bis/about_apropos/hcpubssc_e.html#reports)>. For a more detailed overview of Canadian EHR initiatives, see Amanda Cornwall, "Connecting Health: A Review of Electronic Health Record Projects in Australia, Europe and Canada," (2003) online: Public Interest Advocacy Centre <[http://www.piac.asn.au/publications/pubs/churchill\\_20030121.html](http://www.piac.asn.au/publications/pubs/churchill_20030121.html)> [Cornwall].
7. The Kirby Report recognized that to achieve such a system, Infoway will need substantially more than this initial contribution, and has recommended a combination of private investment and an additional federal contribution of \$2 billion. *Supra* note 3 at 177.
8. Canada Health Infoway, online: Investments: Project Portfolio <<http://www.infoway-inforoute.ca/investments/portfolio.php?lang=en>>.
9. "Alberta patients' medical data available online" *Globe and Mail* (22 October 2003), online: Globe and Mail <<http://www.globeandmail.com/servlet/ArticleNews/TPStory/LAC/20031022/URECON/TPHealth/>>. See also Alberta Wellnet, online: <<http://www.albertawellnet.org>>.
10. Saskatchewan Health Information Network, online: <<http://www.shin.sk.ca>>.
11. *healthnetBC*, online: <<http://healthnet.hnet.bc.ca/>>.
12. Smart Systems For Health Agency, online: <<http://www.ssha.on.ca/>>.
13. Canada Health Infoway, News Release, "Quebec Joins Infoway" (6 February 2004), online: <<http://www.infoway-inforoute.ca/news-events/index.php?loc=20040206&lang=en>>.



14. See, for example, Health Infostructure Atlantic, online: <<http://www.gov.ns.ca/health/hia/>>; Nova Scotia Hospital Information System, online: <<http://www.gov.ns.ca/health/nshis/>>; Newfoundland & Labrador Centre for Health Information, online: <<http://www.nlchi.nf.ca/>>.
15. NHS Information Authority, online: <<http://www.nhsia.nhs.uk/erdip/>>.
16. HealthConnect, online: <<http://www.healthconnect.gov.au/>>.
17. See EHTEL, online: <<http://www.ehtel.org/>>.
18. "Bush calls for electronic medical records" *CNN News* (28 April 2004), online: <<http://www.cnn.com/2004/ALLPOLITICS/04/27/bush.healthcare.ap/>>.
19. See Canada, Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, *Report of the Commission of Inquiry into the Confidentiality of Health Information* (1980) (3 vols.).
20. Mark Weitz *et al.*, "In Whose Interest? Current Issues in Communicating Personal Health Information: A Canadian Perspective" (2003) 31 *J.L. Med. & Ethics* 292 at 293.
21. Lawrence O. Gostin, "Health Information Privacy" (1995) 80 *Cornell L. Rev.* 451 at 451-52.
22. Cornwall, *supra* note 6 at 14.
23. See Peter Winn, "Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law" (2002) 33 *Rutgers L.J.* 617 [Winn].
24. Phillip C. Buttell, "The Privacy and Security of Health Information in the Electronic Environment Created by HIPAA" (2001) 10 *Kan. J. L. & Pub. Pol'y* 399 at 405 [Buttell].
25. R.L. Simpson, "Ethics and Privacy in a Technologically Driven Health Care Network," (1996) 21:1 *Nursing Administration Quarterly* 81 at 81.
26. Cornwall, *supra* note 6 at 22.
27. Elaine Gibson, "A Colloquy on the Romanow Report: Jewel in the Crown? The Romanow Commission Proposal to Develop a National Electronic Health Record System" (2003) 66 *Sask. L. Rev.* 647 at 658-59.
28. Michael Guerriere, "The Editor's Focus" (2003) 2:2 *Electronic Healthcare* 3, online: Longwoods Publishing <<http://www.longwoods.com/eh/eh22/EH22editorial.html>> at 3.
29. Buttell, *supra* note 24 at 406.
30. Winn, *supra* note 23 at 622
31. *Ibid.*
32. Mike Hatch, "HIPAA: Commercial Interests Win Round Two" (2002) 86 *Minn. L.Rev.* 1481 at 1490. This article also provides some disturbing examples of how EHR information has been abused recently in the United States.
33. Cornwall, *supra* note 6 at 14.
34. *Supra* note 21 at 493. Of course, legal rules are part of a broader mix of mechanisms – including technical safeguards and organizational policies – that are key to protecting EHRs. For discussion of technical and organizational approaches, see *e.g.* National Research Council, *For the Record: Protecting Electronic Health Information* (Washington, D.C.: National Academy Press, 1997) online: <<http://www.nap.edu/books/0309056977/html/index.html>>.
35. C.C.S.M. c. P33.5 [*PHIA*].
36. R.S.A. 2000, c. H-5 [*HIA*].
37. S.S. 1999, c. H-0.021 [*HIPA*].
38. S.O. 2004, c. 3 [*PHIPA*].
39. See *e.g.* British Columbia's *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165; the federal *Personal Information and Protection of Electronic Documents Act*, S.C. 2000, c. 5; and Québec's *Act respecting the protection of personal information in the Private Sector*, R.S.Q., c. P-39.1.
40. As we focus here on statutory protections, we do not address other legal mechanisms (such as tort or constitutional litigation) that individuals may use to advance privacy claims in the health information context.
41. We use the term "custodian" to refer to persons and organizations who have custody and/or control of health information. This is the term used in the Alberta and Ontario health information legislation. The Saskatchewan and Manitoba statutes refer to "trustees."
42. Cornwall, *supra* note 6 at 16
43. See *e.g.* Saskatchewan *HIPA*, *supra* note 37, Preamble: "wherever possible, the collection, use and disclosure of personal health information shall occur with the consent of the individual to whom it relates."
44. For a general discussion of consent in the health care context, see *e.g.* Erin Nelson, "The Fundamentals of Consent" (111-128) and Bernard M. Dickens, "Informed Consent" (129-156) in Jocelyn Downie, Timothy Caulfield & Colleen Flood, eds., *Canadian Health Law and Policy*, 2d ed. (Markham, Ont.: Butterworths, 2002).
45. For example, a 2002 Australian discussion paper regarding consent and electronic health records recommends that legislation establishing the HealthConnect system ought to explicitly address how individuals would give consent, rules regarding access and disclosure, and complaint mechanisms. See HealthConnect



Program Office, *Consent and Electronic Health Records: A discussion paper* (July 2002) online: <[http://www.health.gov.au/healthconnect/pdf\\_docs/cons\\_dp.pdf](http://www.health.gov.au/healthconnect/pdf_docs/cons_dp.pdf)>. The discussion paper emphasizes the importance of giving individuals a choice as to whether to participate in HealthConnect and permitting them some control over who has access to what information. For example, the discussion paper recommends that individuals be able to refuse inclusion of sensitive health information and limit who has access to their EHR. The report also acknowledges the need to ensure consent requirements do not impede the operation of the system.

46. *Supra* note 35.
47. *Ibid.*, s. 22(2)(h).
48. *Ibid.*, s. 22(2)(a).
49. See *HIPA*, *supra* note 37, s. 2.
50. *Ibid.*, s. 18.1(1).
51. *Ibid.*, s. 8(1).
52. *Ibid.*, s. 8, as am. by S.S. 2003, c. 25.
53. Section 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.”
54. Section 27(4) describes circumstances in which individual consent is not required for the disclosure of personal health information.
55. *HIA*, *supra* note 36, s. 59, as rep. by *Health Information Amendment Act*, S.A. 2003, c. 23, s. 3.
56. *HIA*, *supra* note 36, s. 34(2). Saskatchewan’s *HIPA*, *supra* note 37, s. 6, also stipulates certain requirements for valid consent, as does the Ontario *PHIPA*, *supra* note 38, s. 18.
57. See Office of the Information and Privacy Commissioner, News Release, “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 <[http://www.oipc.ab.ca/ims/client/upload/Repeal\\_of\\_s.59.pdf](http://www.oipc.ab.ca/ims/client/upload/Repeal_of_s.59.pdf)>.
58. *Ibid.*
59. Cornwall, *supra* note 6 at 19.
60. *Supra* note 57.
61. *Ibid.*, s. 18(1). In determining what is a “reasonable” measure, trustees must consider the sensitivity of the information: see s. 18(4).
62. *Ibid.*, s. 18(3).
63. Man. Reg. 245/97, s. 4(1).
64. *Ibid.*, s. 4(2).
65. *HIPA*, *supra* note 37, s. 16.
66. *HIA*, *supra* note 36, s. 60(1).
67. *Ibid.*, s. 60(2) [emphasis added].
68. *Ibid.*, s. 64(1).
69. *Ibid.*, s. 64(2). The Alberta Commissioner has reviewed a number of privacy impact assessments regarding electronic patient records (which we earlier distinguished from electronic health records) and maintains an online registry of privacy impact assessments: <<http://www.oipc.ab.ca/pia/registry.cfm>>.
70. *Supra* note 38, s. 73(1)(h).
71. James G. Hodge, Jr., Lawrence O. Gostin & Peter D. Jacobson, “Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability” (1999) 282 *Journal of the American Medical Association* 1466 at 1467.
72. In Manitoba, the provincial Ombudsman monitors compliance with *PHIA*.

