WALKING THE TALK: A ROADMAP FOR ACTION AND EXCELLENCE

A ROADMAP TO RESEARCH USES OF ELECTRONIC HEALTH INFORMATION

DON WILLISON, ELAINE GIBSON, AND KIM MCGRAIL

BACKGROUND

Electronic health information, whether from administrative databases or electronic health records, holds potential as an extremely rich resource for researchers. In 2000, Dalhousie University researcher George Kephart and a number of colleagues undertook a research study that required linking the National Population Health Survey, held by Statistics Canada, with hospital discharge abstracts and physician administrative billing records from five provinces to examine socioeconomic differences in access to health care across Canada.[1] The logistical, organizational, and political barriers they encountered stymied their work so badly that, despite years of attempts, they failed to gain the cooperation of one of the provinces. To the frustration of the researchers, the dataset used for undertaking the planned examination was ultimately only partial. This seriously diminished the value of the study.

This complex research proposal involved multiple data providers and jurisdictions, but it is emblematic of barriers still encountered by researchers today. Why are the data not flowing to researchers as anticipated? This chapter examines several reasons and makes suggestions for addressing these challenges that we hope will stimulate discussion and

Data Data Everywhere: Access and Accountability? ed. Colleen M. Flood. Montreal and Kingston: Queen's Policy Studies Series, McGill-Queen's University Press.

debate among researchers and policy-makers.[2] Our specific lens for this paper is Canada, but the issues identified are common to many countries, and the suggestions are general enough to be widely relevant as well.

THE CHALLENGES

In this section, we identify and describe a number of technical or procedural challenges affecting access to personal information[3] for health research. Before turning to these, a few introductory comments are in order.

First, many parties are involved in or affected by the research uses of personal information, including those who draft and revise legislation and ethical codes; those who ensure those laws and codes are followed (chiefly research ethics boards, data custodians/stewards, and privacy commissioners); researchers; and those whose data are being used. Because there are multiple parties, primarily functioning at the provincial and local levels, policies are often inconsistent, and attempts to harmonize policies involve inherently slow and complex multilateral discussions.

Second, while some argue that personal information simply should not be accessed for health research,[4] we believe the greater stumbling blocks are the uncertainty and disagreement among those who support research use of that information regarding how to interpret or operationalize some commonly agreed-upon fundamental overarching principles about how to collect, use, and process individuals' information.[5]

Third, the distinction between research and other secondary uses of data has blurred over time. It is uncontroversial that health information collected in the course of providing health care to an individual is to be used for purposes directly related to care provision. Historically, any secondary use of this information by a care provider or an institution for purposes of service planning, quality improvement, or risk management was assumed to fall within the scope of the intended use for the data. This assumption does not usually extend to research uses of that information. However, it is often difficult to distinguish health research uses from health services planning and quality improvement because of common analytic methods and the shift toward multi-institutional quality improvement activities.[6] Indeed, this distinction becomes even more difficult to make because it is often the same individuals who function both as service providers and as academic researchers. Similar blurring occurs between public health practice and public health research.

Finally, newer approaches to collection of personal information for health research purposes challenge the existing assumptions around the conditions under which exemptions from requiring consent may be granted. Single time-limited studies are being replaced with registries and biobanks, for which one cannot articulate, in advance, all the intended uses of the data. Electronic health record (EHR) systems are being developed, and some institutions are considering how best to glean data from these

systems for research purposes. EHR systems are also being heralded as avenues to screen patients for phase 3 and phase 4 trials.[7] These developments break down existing distinctions between research, clinical care, and other system uses. This in turn creates major challenges in regulating research use of personal information using existing norms and tools.

Confusion and Uncertainty Regarding Law and Policy

There has been rapid change in Canadian information laws over the past decade. The federal government has enacted the *Personal Information Protection and Electronic Documents Act*.[8] One province has enacted general private sector legislation that does not discriminate between health and non-health information.[9] Five provinces have brought in legislation focusing specifically on issues of personal health information,[10] and in two provinces such legislation is under development.[11] Add to this the pre-existing legislation covering the private sector in Quebec,[12] plus federal and provincial public sector legislation, along with the common law, and we witness a smorgasbord of laws governing personal information. Also in the past decade, and directly relating to research uses of information, the *Tri-Council Policy Statement* (*TCPS*) was implemented by the major federal research funding agencies in Canada: the Medical Research Council (now Canadian Institutes of Health Research), Social Sciences and Humanities Research Council, and National Sciences and Engineering Research Council.[13] Researchers are required by research ethics boards to follow the *TCPS*, but it is a policy statement and not legislation, and therefore carries lesser status in law.

Along with these developments has come a high degree of uncertainty and concern on the part of researchers, research ethics boards, health records departments, and other custodians of personal health information about interpretation of the applicable laws and policies in specific circumstances of research uses. Following the enactment of legislation, there usually follows a period of education, discussion, and the launching of test-case lawsuits seeking clarification as to judicial interpretation of the legislative provisions. This period is still in progress. Add to this the fact that most individuals striving to respect the new laws are not legally trained, and the result is confusion and, at times, misinterpretation of or inaccurate implementation of legal provisions in the resulting policies and procedures. Nobody wants to be on the wrong side of the law, so initial policy interpretations of the legal requirements have tended to err on the side of restricting access.

An additional complicating factor for health researchers and data custodians is the lack of consistency in the legislation. No two pieces of legislation are entirely alike, and the applicability and interactivity between the federal and provincial legislation are at times opaque. Health research is frequently conducted in multiple jurisdictions, and the regional

differences and difficulty in meeting the varying requirements may be jarring or, indeed, may render aspects of comparative research impossible.[14]

Absence of Clarity Regarding Consent for Research Use of Personal Information

One particularly vexing concern within law and ethics is the question of health research uses of personal information without consent. A substantial and increasing amount of research is conducted utilizing database information that was originally collected for treatment or administration. In most circumstances, the individual patient is not notified that the information collected might be used for research.

Understandably, researchers have a keen interest in gaining access to such information in order to conduct their research. Additionally, the risks associated with this breach of confidentiality often appear minimal, and the value of the proposed health research high. Further, the seeking of consent for secondary use of the information may be unmanageable or may give rise to a range of further issues, including the need to re-identify the data to contact the individual for permission to use the data, the risk of introducing bias into the sample, and cost concerns.[15]

On the other hand, the privacy interests of individuals should not get lost in the mix.[16] The problem is exacerbated by the stark and limited options utilized at present: project-specific consent versus exemption from requiring consent (or sometimes even notification) as to research use of the information. Options such as prior authorization or "broad consent"[17] have been suggested, but their status in law is unclear[18] and there has not been a great deal of examination of the ethics of such approaches.

Additionally, current models of consent for research participation are heavily influenced by the clinical trials paradigm and do not translate well to the secondary use of data. The risks to individuals associated with secondary use of personal information are very different from the risks associated with participation in a trial of a new drug, device, or surgical procedure. The former are more concerned with potential breaches of confidentiality whereas the latter are potentially physically invasive.[19]

When consent is sought—for example, if enrolling patients prospectively into a disease registry that will be used for research—an unresolved challenge is how much information to provide patients. It may be impossible for consent to be fully informed, as many of the future research uses may not yet be fully articulated. Even if it were possible to articulate all the potential users, uses, limitations on these uses, risks, and safeguards to mitigate those risks, most individuals would likely encounter decision overload, which could lead to arbitrary decision making, refraining from making any decision, or post-decision regret.[20] At the other extreme, some institutions have implemented blanket consent processes indicating to patients, on admission to the hospital or registration with a clinic, that their

information might be used for research purposes. The legal status of such practices is unclear and their meaningfulness to patients is questionable.

Polls of public opinion do not point to easy policy solutions. Recent survey research suggests that people generally support their health information being used for research, but most wish to retain some control over use of their information, even if that consists only of a reliable system of notification and opt-out.[21] No single approach to consent in the use of personal information for health research receives majority support: about one-third of the population choose conventional project-specific consent, another one-third prefer a broad authorization (opt-in), one-quarter choose a notification and opt-out system if researchers want to use their information for health research, and the remaining 12 percent are unconcerned if researchers use their information without notification.

Heterogeneity in Institutional Policies and Procedures and in Ethics Review Processes

Research ethics boards (REBs) vary in composition, training of their members, outlook, and application of the *Tri-Council Policy Statement*. Policies and practices therefore differ: research that is readily allowed in one place might be strictly circumscribed or disallowed in another location.[22] While recent years have witnessed substantial progress in these matters,[23] there is still considerable variation in policies and procedures for managing privacy, confidentiality, and security. This variation leads to challenges of inconsistency in execution of multisite studies and considerable frustration on the part of researchers.

Complicating the problem is the fact that many research studies making secondary use of personal health information draw upon data from multiple jurisdictions. In these circumstances, multiple REBs may need to review the research protocol. In some cases, there may also be a separate review by the data custodian's privacy officer. There are two challenges here. First, the process of obtaining REB approval can be very time consuming, sometimes delaying commencement of research by months while incurring substantial up-front costs.[24] Second, there may be substantial variation in judgments over whether consent is required for particular research, or the conditions under which the research may be exempted from requiring consent.[25] If REB requirements differ substantially, there is a risk that the data collected across sites might be incommensurate, which could threaten the validity of the data. The challenge is compounded further when multiple data custodians have different requirements.

"Anonymous" Data and the Challenge of Re-identification

Virtually all privacy laws apply only to data that identify individuals either directly or indirectly. It is difficult, if not impossible, to declare

definitively that non-aggregated data are truly "anonymous" because it may remain possible to use combinations of the remaining data to indirectly re-identify individuals through matching these variables with other files that contain identifying information. The classic example was that of a graduate student at the Massachusetts Institute of Technology who was able to identify the Governor of Massachusetts from an "anonymized" dataset by matching the combination of sex, date-of-birth, and full postal code with information available on a public voters' registry.[26] It becomes more difficult to prevent re-identification when one is dealing with a rich dataset with dozens of variables about, for example, health care services use, especially if the dataset includes multiple dates like admission, discharge, and when specific procedures were conducted.

One can minimize the risk of re-identification using statistical or other technological procedures, such as switching values of variables.[27] These methods, however, are designed for producing high-level statistical tables. Their impact is unknown if more complicated analyses, such as statistical modelling of cause-and-effect associations, are undertaken.

Insufficient Capacity for Secure Management of Data

Several large data repositories are exemplary in their secure management of data for research purposes.[28] In these cases, there has been significant investment in the physical plant to ensure that "intruders" are identified and stopped before there is any possibility of access to data.[29] Security systems can be custom built, managed, and controlled, ensuring adherence to high standards and adaptability even as those standards change. However, this requires ongoing investment in highly skilled staff who are capable of developing these systems, keeping up with technology and privacy standards, linking and de-identifying data, and analysing data. Costs of infrastructure development and ongoing compliance, which are substantial, are often not covered through operating grants available to researchers.[30]

Currently, these kinds of laboratories are not available at every university in the country. In fact, much academic research is done by small research teams that lack equivalent structures available to researchers who work in secure data enclaves. However, powerful personal computers and the gradual expansion of clinical electronic health records in the inpatient and outpatient settings make the development of smaller ad hoc research databases both easy and inexpensive to assemble.

The result is heterogeneity in the level of safeguards for personal information used in research. A researcher at a large data repository may expect to encounter a high level of data protection, including formalized training in privacy policies and procedures, and constant checks and

balances on activities. In contrast, access to similar data in a smaller research unit may involve a researcher putting data onto a laptop with few or no safeguards in place. The result can be a substantial security breach, as was the case with the theft of a researcher's computer containing the fully identifiable records of thousands of patients participating in several research studies.[31] This is not to impugn the best intentions of researchers regardless of their work locations. Instead, it raises the question of how best to extend or ensure secure research environments for all researchers.

Low Comparability of Data

The *Canada Health Act* provides a federal framework for the provision of health-care services, but the management of the health-care system falls primarily under provincial or territorial jurisdiction. This structure has provided a natural "laboratory" for the comparative evaluation of health-care policies across provinces and territories; indeed, the deployment of different health-care policies across the country has been called the "great experiment."[32] Despite this obvious natural laboratory for comparative analysis, relatively little comparative research has actually been done. In some cases this is because of the difficulty of gaining access to data from multiple jurisdictions, but in other cases proposals are not even developed because of current challenges in comparing data generated in different provincial/territorial health-care systems.

The Canadian Institute for Health Information has made substantial progress in improving comparability of hospital data[33] and is working on developing other data sources, for example a National Ambulatory Care Reporting System and a National Pharmaceutical Drug Utilization Information System. But there are obvious challenges in such development. For example, some data are problematic because of variations between provinces (and, over time, within provinces) in who and what is covered by public programs. This is particularly the case with coverage for pharmaceuticals provided out-of-hospital and home health-care services because these services fall outside of the *Canada Health Act*. There are also challenges with interjurisdictional and interinstitutional variation in the operationalization of certain policy-critical statistics such as "wait times."

Perhaps the biggest challenge, however, rests with physician data. Fee schedules across jurisdictions are incommensurate, fee negotiations use different processes, the diagnostic codes used for billing have questionable validity for research purposes, and the mix of remuneration methods varies. And all of these things have been shifting—sometimes substantially—within jurisdictions. To date, little has been done to respond to these challenges, even though physician data are fundamental to understanding health status and health-care services use.

Failure to Design Research Use into the Common Interoperable Electronic Health Record (EHR) Infrastructure

Many people have put a great deal of stock in the emergence of a common interoperable electronic health record system for Canada, implicitly (or explicitly) assuming that the development of the EHR will replace administrative data sources for conducting research.[34] Certainly, the EHR is *an* answer, and in many respects a positive development, for reasons of patient care as well as the extraordinary research possibilities. However, it is not *the* answer for health services and policy research. In the best-case scenario, the EHR will still take many years to roll out, and there will still likely be administrative datasets that provide information useful for research (e.g., on characteristics of providers).

There will be many challenges encountered on the road to accessing data from the EHR for research purposes. Not least of these challenges is that, to date at least, researchers have had little involvement in the development of the EHR or the systems that house it. Without some influence on development, it is quite likely that the ultimate value of the data may not be what it could be, at least in terms of research.

More fundamentally, however, without researcher input, the issues of *how* and under *what conditions* researchers might have access to these data are unlikely to be addressed. It is looking more and more that the approach taken will be to develop the information systems for patient care, and then retrofit to make the data usable for research.[35] This is problematic for addressing the interests of both researchers (as discussed above) and those whose information will be accessed for research. Kosseim and Brady have labelled this "policy by procrastination."[36]

Political Hurdles

Even if the above issues of data privacy, quality, and comparability could be resolved, there would still remain several political challenges. For example, there have been long-standing sensitivities over federal-provincial sharing of data. Provinces are sensitive to increasing unilateral efforts at the federal level to effect health policy changes while cutting back on federal funding for health. As health care is primarily the purview of the provinces and territories, they have resisted federal government requests for data, direction on uses of additional funds, and federally initiated comparisons among provinces.[37]

Provincial governments are also reticent to allow more open access to researchers. There are three principal reasons behind this. First, governments are accountable to their citizens to ensure the safe handling of information that has been entrusted to them—including data made available to researchers. Thus, governments must ensure that researchers have the capacity to manage the data securely, understand the requirements of the

law and why certain safeguards need to be maintained, and understand how to use the data to draw reasonable inferences.

Second, governments are also keenly aware of the potential for political embarrassment every time a report is produced with findings that speak to some aspect of the quality, distribution, or amount of services provided in their province. Indeed, substantial time goes into briefing ministers and preparing for media responses when a new research report or paper is issued. The amount of work involved in responding to a new report is not necessarily related to the quality or reliability of the research. If independent researchers were to gain easier access to data, the time spent in responding to reports (and the corresponding risk of issues management fatigue) would increase proportionately. This would certainly increase governments' reluctance to provide more open access to these data.

Finally, as more and more data are created, various parties demand access to the data for a myriad of secondary purposes. The expansion in uses of data over time is called "information usage creep" or "function creep." A challenge for any regulator is limiting access to health information for these secondary purposes. Governments may restrict access for research due to concern that they not set a precedent for accessing data for other secondary uses.

MOVING FORWARD

We have identified numerous challenges that are both complex and intertwined: confusion and uncertainty regarding law and policy; absence of clarity regarding consent for research use of personal information; heterogeneity in institutional policies and procedures and in the ethics review processes; insufficient capacity for secure management of data; low comparability of data; failure to design research use into the common interoperable electronic health record infrastructure; the proliferation of electronic databases; and political hurdles. Given these daunting challenges, a comprehensive solution for increasing researcher access to data may not be within our grasp at the present time. However, we offer a number of suggestions that may provide at least a partial roadmap for getting to that ultimate destination. At minimum, we anticipate that our comments will stimulate discussion and debate among researchers and policy-makers as to possible directions forward.

Rethinking the Place of Research Vis-à-vis Other Secondary Uses of Personal Health Information

As research becomes increasingly blurred with quality improvement, systems planning, and public health, it has been argued that we should be evaluating *all* secondary data uses—including research, quality improvement, systems planning, and public health—proportionate to the risks

CONCLUDING STATEMENT

All of the efforts described above would work toward securing the trust of all parties involved, including governments and other agencies who are data stewards. There is much to be done to improve access to data for research purposes in Canada. The primary need is to develop a plan for action. The issues involved are complex, touching on the interests of many stakeholders. Piecemeal developments have proven effective in some cases, but we need now to think about the larger endeavour. Variations in health-care systems across Canada provide a natural laboratory that has the potential to make enormous contributions to our understanding of what makes and keeps people healthy. It is our challenge to find a way to develop and use this laboratory that is consistent with privacy legislation and acceptable to everyone involved.

NOTES

1. G. Kephart, *Barriers to Accessing and Analyzing Health Information in Canada* (Ottawa: Canadian Institute for Health Information, 2002).
2. Throughout this chapter, our framing of "research uses" is restricted to those approaches consistent with health services/health policy research and population and public health research. Other uses—for example, for recruitment for clinical trials or translational bioinformatics—fall outside the scope of this discussion.
3. "Personal information" refers to information that either directly identifies an individual (e.g., name, address, social insurance number) or contains some combination of elements that allows indirect identification of an individual (e.g., date of birth combined with sex and postal code). This definition is adapted from Canadian Institutes of Health Research Privacy Advisory Committee, *CIHR Best Practices for Protecting Privacy in Health Research* (Ottawa: Public Works and Government Services Canada, 2005), http://www.cihr-irsc.gc.ca/e/documents/pbp_sept2005_e.pdf. In this chapter, we discuss both use of personal information for *health* research and use of personal *health* information for research. The former makes broad reference to research that includes the effect of non-medical factors—e.g., income and education—on the health of populations. The latter refers specifically to research uses of health sector holdings and electronic sources of health information.
4. D.J. Willison, L Schwartz, J Abelson, C. Charles, M. Swinton, D. Northrup, and L. Thabane, "Alternatives to Project-Specific Consent for Access to Personal Information for Health Research: What Is the Opinion of the Canadian Public?" *Journal of the American Medical Informatics Association* 14, no. 6 (2007): 706-12.
5. These "fair information principles" are the foundation of most privacy laws and policies in Western industrialized nations. See the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada*, CAN/CSA-Q830-96 (Mississauga, ON: Canadian Standards Association, 1996). These principles have been developed, in large part, out of recognition by regulators that individuals will permit the use of

their personal information only if they are confident that it is being reasonably protected. Central to these fair information principles are the following:
(a) Information about individuals is to be collected, used, or disclosed to others with a clear and finite purpose in mind.
(b) Unless impracticable, this collection, use, or disclosure should be done with the express consent of the individual. Exceptions may apply to this consent requirement, but these exceptions should be for specific purposes and should not go on for an indefinite time.
(c) Personal information collected for one purpose should not be used for another purpose unless consent is obtained from the individual, again with exemptions.

6. W.E. Thurston, A.R. Vollman, and M.M. Burgess, "Ethical Review of Health Promotion Program Evaluation Proposals," *Health Promotion Practice* 4, no. 1 (2003): 45-50. See also Alberta Research Ethics Community Consensus Initiative, *Protecting People While Increasing Knowledge: Recommendations for a Province-wide Approach to Ethics Review of Knowledge-Generating Projects (Research, Program Evaluation, and Quality Improvement) in Health Care* (Edmonton: Alberta Heritage Foundation for Medical Research, 2005).
7. National Center for Research Resources, Agency for Healthcare Research and Quality, and FasterCures, "Ensuring the Inclusion of Clinical Research in the Nationwide Health Information Network," Meeting Report (Washington, May 2006), http://www.fastercures.org/objects/pdfs/meetings/FC_AHRQ-NCRR_report.pdf . See also *UKCRC R&D Advisory Group to Connecting for Health: Report of Research Simulations* (UK Clinical Research Collaboration, 2007), http://www.ukcrc.org/pdf/CfH report June 07 full.pdf.
8. *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 50.
9. British Columbia, *Personal Information Protection Act*, S.B.C. 2003, c. 63.
10. The five provinces are Alberta (*Health Information Act,* R.S.A. 2000, c. H-5), Manitoba (*Personal Health Information Act,* C.C.S.M. c. P33.5), Ontario (*Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sch. A.), Saskatchewan (*Health Information Protection Act*, S.S. 1999, c. H-0.021), and most recently Newfoundland and Labrador (*Personal Health Information Act,* S.N.L. 2008, c. P-7.01 (to be proclaimed).
11. Nova Scotia (http://www.gov.ns.ca/health/phia/default.asp) and New Brunswick (http://www.gnb.ca/0051/personal_health_information/index-e.asp).
12. Quebec, *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1
13. Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Human Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 1998 (with 2000, 2002, 2005 amendments)* (Ottawa: Public Works and Government Services Canada, 2005).
14. G. Kephart, *Barriers to Accessing & Analyzing Health Information in Canada* (Ottawa: Canadian Institute for Health Information, 2002). See also Subgroup on Procedural Issues for the TCPS (ProGroup): A Working Committee of the Interagency Advisory Panel on Research Ethics (PRE), "Ethics Review of Research in Multiple Settings and/or Involving Multiple REBs (Previously

Multicentred Ethics Review): A Discussion Paper and Recommendations" (Interagency Panel and Secretariat on Research Ethics, Ottawa, 2008).

15. CIHR Working Group on Case Studies, *Secondary Use of Personal Information in Health Research: Case Studies* (Ottawa: Public Works and Government Services Canada, 2002), http://www.cihr-irsc.gc.ca/e/pdf_15568.htm.
16. E. Gibson, J. Downie, G. Kephart, L. Schwartz, and D. Willison, "Conceptual Paradigms Responding to Privacy and Access Challenges in Health Research," submitted to the CIHR Ethics Office (2007).
17. The terms "prior authorization" and "broad consent" refer to authorization for use of one's information beyond a single application, to encompass a range of potential uses. This type of consent may come with restrictions, such as "use for stroke-related research." This is distinct from the term "blanket consent," which does not include restrictions on those uses. An example here would be consent "for research" with no qualifiers. The legal status of all these alternatives to project-specific consent is unclear.
18. T. Caulfield, R.E.G. Upshur, and A. Daar, "DNA Databanks and Consent: A Suggested Policy Option Involving an Authorization Model," *BMC Medical Ethics* 4 (2003): 1-4. See also T. Caulfield, N. Ries, and T.C. Bailey, "Consent, Privacy and Confidentiality in Longitudinal, Population Health Research: The Canadian Legal Context," *Health Law Journal Supplement* (University of Alberta Law Institute, 2004).
19. N.C. Manson and O. O'Neill, *Rethinking Informed Consent in Bioethics* (New York: Cambridge University Press, 2007).
20. N. Ram, "Tiered Consent and the Tyranny of Choice," *Jurimetrics* 48, no. 3 (2008), ssrn.Com/Abstract=1112364 (accessed 10 November 2009).
21. Willison et al., "Alternatives to Project-Specific Consent."
22. D.J. Willison, C. Emerson, K.V. Szala-Meneok, E. Gibson, L. Schwartz, K.M. Weisbaum, F. Fournier, K. Brazil, and M.D. Coughlin, "Access to Medical Records for Research Purposes: Varying Perceptions across Research Ethics Boards," *Journal of Medical Ethics* 34, no. 4 (2008): 308-14.
23. Canadian Institutes of Health Research, *CIHR Best Practices*. See also P.M. Slaughter, P.K. Collins, N. Roos, K.M. Weisbaum, M. Hirtle, J. Williams, P.J. Martens, and A. Laupacis, *Harmonizing Research & Privacy: Standards for a Collaborative Future. Privacy Best Practices for Secondary Data Use (SDU)* [CD-ROM] (Manitoba: Institute for Clinical Evaluative Sciences and Manitoba Centre for Health Policy, 2006).
24. C. Metcalfe, R.M. Martin, S. Noble, J.A. Lane, F.C. Hamdy, D.E. Neal, and J.L. Donovan, "Low Risk Research Using Routinely Collected Identifiable Health Information without Informed Consent: Encounters with the Patient Information Advisory Group," *Journal of Medical Ethics* 34, no. 1 (2008): 37-40.
25. Willison et al., "Access to Medical Records."
26. L. Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," *Journal of Law Medicine & Ethics* 25, no. 2&3 (1997): 98-110.
27. Statistical Policy Office, "Report on Statistical Disclosure Limitation Methodology," Statistical Policy Working Paper 22 (Statistical Policy Office, Office of Information and Regulatory Affairs, and Office of Management and Budget, Washington, May 1994). See also G.T. Duncan and S. Mukherjee, "Optimal Disclosure Limitation Strategy in Statistical Databases: Deterring

Tracker Attacks Through Additive Noise," *Journal of the American Statistical Association* 95, no. 451 (2000): 720-29; K. El Emam, E. Jonker, S. Sams, E. Neri, N. Neisa, T. Gao, and S. Chowdhury, "Pan-Canadian De-identification Guidelines for Personal Health Information," Report produced for the Office of the Privacy Commissioner of Canada (Ottawa, 2007), http://www.ehealthinformation.ca/documents/OPCReportv11.pdf.

28. Slaughter et al., *Harmonizing Research & Privacy* [CD-ROM].
29. For example, the Institute for Clinical Evaluative Sciences, the Manitoba Centre for Health Policy, the Centre for Health Services and Policy Research, and Population Data BC have all used awards from the Canada Foundation for Innovation to build secure physical premises with state-of-the-art server rooms, moated areas for programmers, and surveillance and security systems protecting the perimeters.
30. Slaughter et al., *Harmonizing Research & Privacy* [CD-ROM].
31. A. Cavoukian, *Order H0-004* (Toronto: Information and Privacy Commissioner of Ontario, 2007), http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf.
32. M.J. McGregor, R.B. Tate, K.M. McGrail, L.A. Ronald, A.-M. Broemeling, and M. Cohen, "Care Outcomes in Long-Term Care Facilities in British Columbia, Canada: Does Ownership Matter?" *Medical Care* 44, no. 10 (2006): 929-35.
33. Canadian Institute for Health Information, *Quality Assurance Processes Applied to the Discharge Abstract and Hospital Morbidity Databases* (Ottawa: Canadian Institute for Health Information, 2007).
34. R.J. Romanow, *Building on Values: The Future of Health Care in Canada – Final Report* (Ottawa: Commission on the Future of Health Care in Canada, 2002), http://www.hc-sc.gc.ca/hcs-sss/alt_formats/hpb-dgps/pdf/hhr/romanow-eng.pdf. See also M.J.L. Kirby and M. LeBreton, *The Health of Canadians – The Federal Role Final Report*, vol. 6, *Recommendations for Reform* (Ottawa: Standing Committee on Social Affairs, Science and Technology, 2002), http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/soci-e/rep-e/repoct02vol6-e.htm.
35. Infoway revised its Blueprint document in 2006 to include uses of the data for public health surveillance (see Canada Health Infoway, "EHRS Blueprint," http://knowledge.infoway-inforoute.ca/en/knowledge-centre/ehrs-blueprintv2.aspx). However, the capacity to conduct more sophisticated population-level analyses is, as yet, unclear.
36. P. Kosseim and M. Brady, "Policy by Procrastination: Secondary Use of Electronic Health Records for Health Research Purposes," *McGill Journal of Law and Health* 2 (2008): 5-45.
37. T. McIntosh, "Intergovernmental Relations, Social Policy and Federal Transfers after Romanow," *Canadian Public Administration* 47, no. 1 (2004): 27-51.
38. Alberta Research Ethics Community Consensus Initiative, *Protecting People While Increasing Knowledge*.
39. A good starting point may be found in Section 3 of the CIHR privacy best practices document (see Canadian Institutes of Health Research, *CIHR Best Practices*).
40. Canada Health Infoway, "EHRS Blueprint."
41. Advisory Council on Health Infostructure, *Canada Health Infoway: Paths to Better Health* (Final Report) (Ottawa: Health Canada Publications, 1999).

42. As noted above, there are consent options beyond the traditional dichotomy of conventional project-specific consent versus exemption from requiring consent. Other options include "broad opt-in to a range of research with restrictions" and "notification with opt-out." See P. Singleton and M. Wadsworth, "Consent for the Use of Personal Medical Data in Research," *British Medical Journal* 333, no. 7561 (2006): 255-58. See also D.J. Willison, M. Swinton, L. Schwartz, J. Abelson, C. Charles, D. Northrup, J. Cheng, and L. Thabane, "Alternatives to Project-Specific Consent for Access to Personal Information for Health Research: Insights from a Public Dialogue," *BMC Medical Ethics* 9, no. 18 (2008), doi:10.1186/1472-6939-9-18.
43. Canada Health Infoway, "EHRS Blueprint."
44. Health Canada, *Pan-Canadian Health Information Privacy and Confidentiality Framework* (Ottawa: EKOS Research Associates Inc., 2005), http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php.
45. Canada Health Infoway, "EHRS Blueprint."
46. Health Canada, *Pan-Canadian Health Information Privacy and Confidentiality Framework*.
47. Slaughter et al., *Harmonizing Research & Privacy* [CD-ROM].
48. The Institute for Clinical Evaluative Sciences, for example, is creating satellite centres outside Toronto in Ontario, so that researchers can have access without travelling to Toronto.
49. See, for example, the Population Data BC website, www.popdata.bc.ca. Population Data BC is developing a different hybrid model where data are held centrally, but access is allowed (to approved research datasets) through "virtual private network" type facilities over the Internet. In this model, researchers are not bounded by geography (within Canada), university, or research centre affiliation.
50. *Concept Dictionary* (2009), http://umanitoba.ca/faculties/medicine/units/mchp/resources/concept_dictionary.html.
51. Subgroup on Procedural Issues for the TCPS, "Ethics Review of Research in Multiple Settings."
52. "The Research Data Centres Program" (2009), available on the Statistics Canada website, http://www.statcan.gc.ca/rdc-cdr/index-eng.htm.
53. J.M. Paterson, G. Carney, G. Anderson, K. Bassett, G. Naglie, and A. Laupacis, "Case Selection for Statins Was Similar in Two Canadian Provinces: BC and Ontario," *Journal of Clinical Epidemiology* 60, no. 1 (2007): 73-78. See also M. Mamdani, L. Warren, A. Kopp, J.M. Paterson, A. Laupacis, K. Bassett, and G.M Anderson, "Changes in Rates of Upper Gastrointestinal Hemorrhage after the Introduction of Cyclooxygenase-2 Inhibitors in British Columbia and Ontario," *CMAJ Canadian Medical Association Journal* 175, no. 12 (2006): 1535-38. See also notes 39 and 40.