Editorial

Éditorial

Dr. Willison is Senior Scientist, Centre for the Evaluation of Medicines, St. Joseph's Hospital, (affiliated with McMaster University Faculty of Health Sciences, Hamilton, Ont.), Chair of the US–Canada Data Privacy Working Group of the International Society for Pharmacoepidemiology and a member of the Canadian Institute for Health Information Partnership for Health Informatics/ Telematics, Project Team on Privacy Legislation and Guidelines.

CMAJ 1998;159:1378-80

Health services research and personal health information: privacy concerns, new legislation and beyond

Donald J. Willison, ScD

In Canada, health information networks are being developed in every province to enhance patient care and manage an increasingly complex health care system. Researchers and policy-makers are trying to establish common community-level indicators of health, to be linked with health care and social services utilization data. Following the recommendation of the National Forum on Health,[1] the Canadian Population Health Initiative is being established to serve as a national health surveillance network and a population health clearinghouse, combining health, social and economic indicators of well-being. The Advisory Council on Health Info-structure has recently released an interim report, outlining its vision for the integration and coordination of information systems in Canada across the entire spectrum of health care services.[2] The raw data for this work will come from longitudinal records, specific to individuals, maintained by provincial and territorial health systems and from other administration systems.

The stage is being set for improved coordination in the provision of health care and for superior information to be made available for health services planning, policy analysis and research. At the same time, these developments have raised concerns about the potential for breach of privacy. (Privacy rights may be defined as the right to control the circulation of personal information about oneself, freedom from unreasonable interference in one's private life and the right to the protection of personal data against misuse or unjustified publication.[3]) In his last 2 annual reports, the federal privacy commissioner expressed concern over the establishment of a Canadian health surveillance network.[4,5] At stake is the loss of individual control over who has access to personal health and socioeconomic information. Health information is considered to be especially sensitive, and the conditions under which personal information may be disclosed without the explicit consent of the individual is particularly contentious. How, then, will access to such information be controlled?

The CMA has recently adopted a Health Information Privacy Code[6] that stands firmly behind the patient's right to privacy and places the physician in the role of gatekeeper of any information collected in the course of the physician–patient encounter. In light of the trust relationship between the physician and the patient, this clearly makes sense. However, depending on how the code is implemented the use of health information without individual consent could become extremely difficult — or even impossible — for such purposes as quality-of-care assessment and health-systems improvement, as envisioned by the Advisory Council on Health Info-structure.

Many acknowledge the fundamental need for privacy but recognize that there may be circumstances under which the benefits to the public outweigh the cost of some limited loss of privacy. The challenge is in determining where to draw the line. This question is currently occupying the attention of legislators in Canada and throughout the world as existing laws are being redrafted.

Legislation in Canada and abroad

In recent months, several provinces in Canada have either introduced or passed legislation governing the protection of personal information.[7–12] Some of the leg-

islation is specific to personal health information.[7–10] Prince Edward Island has new legislation regulating access to its province-wide pharmaceuticals database.[13] In January 1998, the federal government issued a discussion paper on protecting personal information[14] and, in October, it introduced draft legislation expanding the protection of personal information to include the private sector.[15] Outside Canada, New Zealand and the European Union passed legislation several years ago,[16,17] and the US has several bills in draft form.[18,19] At the core of much of the new legislation are the "fair information practices" of the 1981 Organization for Economic Co-operation and Development guidelines, which have been refined and enhanced by the Canadian Standards Association.[20,21] Under these guidelines, information about a person should be collected only after the purpose of collecting the information is identified and (with limited exceptions) after consent has been obtained. Collection of personal information is restricted to the minimum needed to accomplish the identified purpose. Personal information cannot be used for secondary purposes without consent unless authorized by law. The data subject (i.e., the patient) may access and challenge the information being held. Also, custodians of personal information must disclose and be accountable for the types of personally identifiable information in their possession, who has had access to the information and the safeguards taken to ensure the confidentiality and security of that information. The bills introduced by the provinces vary in the degree of stringency with which they have applied these fair information practices, as exemplified in the lists of permitted disclosures without consent.

So far, the Canadian research community has not been unduly restricted by these new laws. Specific provisions have been made in each province's legislation for research uses of health data, subject to approval of a research ethics board or equivalent. Nonetheless, a number of points should be noted.

- Generally, under the new legislation, databases must either be destroyed or stripped of any identifiers after the data have been used for their original purpose. Should researchers hold or have access to identifiable information from a previous study, they will likely have to request approval from their institution's review board before using that dataset again, unless it is for a purpose consistent with the original reason for collecting the information. In the case of large administrative datasets, it will be necessary at the very least to specify any additional intended uses, such as research, quality assurance, utilization management and planning.
- Under the new legislation in Manitoba and the draft legislation in Alberta and Ontario, custodians of personal health information are required to maintain a record of the disclosure of the information. The Manitoba legislation and the Ontario draft legislation also specify that a record of the destruction of the dataset be maintained.
- The Alberta and Ontario draft legislation require that custodians of personal health information request permission from a health information and privacy commissioner before linking their identifiable records with those of another data custodian.
- The draft laws in both Alberta and Ontario have "lock-box" provisions, under which patients may specify that certain information not be shared with care providers without their consent. Although the intention is to make such information accessible when administrative datasets are being used for research purposes, the logistical hurdles are as yet unknown. This has implications for the research of diseases with high stigma.
- Most new legislation makes provision for the flow of personal information from one jurisdiction to another. The provincial legislation being introduced requires that the laws of the province of origin be upheld beyond its borders. The 1995 European directive[17] prohibits transfer of personal information to jurisdictions deemed to have "inadequate" privacy legislation. Currently, Canada's standards are not as stringent as those of Europe. The implications for multicentre studies will not become known until some time after October 1998.

Beyond the legislation

Legislators have granted researchers relatively open access to health information, subject to review board approval. This places the responsibility of ensuring a high level of confidentiality and security with researchers, their institutions and their review boards. Indeed, the interim report of Advisory Council on Health Info-structure has recommended increased attention to technologies and procedures to enhance data security.

What kinds of measures need to be taken to prepare for this new research environment? First and foremost, all individuals who work with personal health information should be held strictly accountable for the maintenance of confidentiality and security, and sanctions should be implemented in the event of a breach. At the institutional level, review boards must address privacy concerns about personal information as thoroughly as they currently address potential physical and emotional harm. Some review boards may require continuing education to sensitize their members to privacy, confidentiality and security issues. In addition, review boards may need to extend their mandate to include overseeing the auditing of confidentiality and

security practices within the institution. This has implications for the workload in a system that is already heavily burdened. Researchers who work with personal health information should examine their information-use practices in light of the Tri-Council policy statement on the code of ethical conduct of research involving humans,[22] the CMA Health Information Privacy Code,[6] and the discussion paper on the principles for the protection of personal health information, soon to be released by the Canadian Institute for Health Information Partnership for Health Informatics/Telematics.[23]

At another level, there is a need for informed discussion with the public as to who may access personal health information, for what purposes, and under what circumstances. Although many forums and working groups have emerged to address technical issues, policy discussions have been dominated by organized stakeholder groups.

Focus on the confidentiality and security of data will increase the cost of conducting research. This is a necessary and worthwhile investment. The public has been sensitized to the potential for breaches of privacy. Linkage of administrative records, for example, is one of the greatest privacy concerns of Canadians.[24] It is our responsibility to ensure the confidentiality and security of information used for health policy analysis and health services research. Failure to demonstrate good stewardship of personal information could lead to a loss of public confidence on a scale equal to the recent tainted blood scandal in Canada[25] and result in the imposition of severe restrictions on our ability to conduct research that will benefit the public. We can — and must — meet this challenge.

References

1. National Forum on Health. *Canada health action: building on the legacy. Final report of the National Forum on Health*. Ottawa: The Forum; 1997.
2. Advisory Council on Health Info-structure. *Connecting for better health: strategic issues*. Ottawa: Health Canada; 1998. Available: www.hc-sc.gc.ca/ohih-bsi/achis/int-rpt_e.html (accessed Oct. 28, 1998).
3. Partnership for Health Informatics/Telematics. *Working Group 3: privacy, confidentiality, data integrity, and security. Background document (revised)*. Ottawa: Canadian Institute for Health Information; 1997.
4. Privacy Commissioner of Canada. *Annual report, Privacy Commissioner, 1996-97*. Ottawa: The Commissioner; 1997. p. 14-8.
5. Privacy Commissioner of Canada. *Annual report, Privacy Commissioner, 1997-98*. Ottawa: The Commissioner; 1998. p. 18-9.
6. Canadian Medical Association. Health information privacy code [policy summary]. *CMAJ* 1998;159(8):997-1006.
7. Bill 30, *Health Information Protection Act*, 1st sess., 24th Leg., Alberta, 1997. A discussion of the Bill is available at: www.health.gov.ab.ca/public/document/hipa/index.htm (accessed Oct. 28, 1998).
8. Bill 51, *The Personal Health Information Act*, 3d sess., 36th Leg., Manitoba, 1997.
9. *The Health Information Protection Act* [working draft]. Regina: Saskatchewan Health; June 1998.
10. Ontario Government, Ministry of Health, *Personal Health Information Protection Act: Draft for Consultation* (Queen's Printer for Ontario, 1997). Available: www.gov.on.ca:80/health/english/pub/legis/phipa/draft.doc (accessed Oct. 28, 1998).
11. Bill 50, *The Freedom of Information and Protection of Privacy and Consequential Amendments Act*, 3d sess., 36th Leg., Manitoba, 1997.
12. Bill 55, *Protection of Personal Information Act*, 3d sess., 53d Leg., New Brunswick, 1998.
13. Bill 87, *Pharmaceutical Information Program Act*, 1st sess., 60th Gen. Assem., Prince Edward Island, 1997.
14. Electronic Commerce Task Force. *The protection of personal information: building Canada's information economy and society*. Ottawa: Industry Canada and Justice Canada. Available: strategis.ic.gc.ca/SSG/pv01169e.html (accessed Oct. 28, 1998).
15. Bill C-54, *Personal Information Protection and Electronic Documents Act*, 1st sess., 36th Parl., 1997-98.
16. *Privacy Act* (N.Z.), 1993. Available: www.privacy.org.nz/slegis.html (accessed Nov. 4, 1998).
17. European Parliament and Council of the European Union. *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 1995. Available: www2.echo.lu/legal/en/dataprot/directiv/directiv.html (accessed Oct. 28, 1998).
18. *Health Care Personal Information Nondisclosure Act of 1998* [draft]. Washington (DC); 1998.
19. *Medical Information Protection Act of 1998* [draft]. Washington (DC); 1998.
20. Organization for Economic Co-operation and Development. *Guidelines on the protection of privacy and transborder flows of personal data*. Paris: The Organization; 1981.
21. Martin A, editor. *Model code for the protection of personal information*. Mississauga (ON): Canadian Standards Association; 1996.
22. Medical Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada. In: *Tri-Council policy statement: ethical conduct for research involving humans*. Ottawa. The Councils; 1998. Available: www.mrc.gc.ca/ethics/code/english/section3.html (accessed Oct. 28, 1998).
23. Project team on privacy legislation and guidelines. *Principles for the protection of personal health information. A discussion paper*. Ottawa: Canadian Institute for Health Information Partnership for Health Informatics/Telematics; 1998.
24. *Privacy revealed. The Canadian privacy survey*. Ottawa: Ekos Research Associates Inc.; 1993.
25. *Commission of Inquiry on the Blood System in Canada*. Final report. 3 vols. Ottawa: Health Canada; 1997. Available: www.hc-sc.gc.ca/english/krever/ (accessed Oct. 28, 1998).