The privacy paradox: laying Orwell's ghost to rest

Ross E.G. Upshur, Benoit Morin, Vivek Goel

The creation of health information systems poses ethical and legal questions regarding the collection, analysis and ownership of data. Recent media stories indicate a public unease with the extent of the sensitive individual data available in computer databases[1] and conjure up images of an Orwellian world void of privacy, with remote and faceless overseers tracking one's every move.

Surveys indicate that Canadians are concerned about the security of their health information and would resist the use of their data without their consent.[2] Although they wish to be informed and to give consent, they do not agree about how this should be done. In a survey in Saskatchewan, 62.9% of respondents agreed that "to receive informed consent, health professionals would need to provide details of every anticipated use of health information."[3] However, 71.4% of respondents also agreed that "to receive informed consent, health professionals should not have to provide details of every anticipated use of personal health information on every occasion, but should be expected to make this information available on request and through pamphlets, brochures and other convenient means." This ambivalent attitude poses difficulties for setting policies for the use of health information.

For a complex health care system to operate effectively, a balance must be struck between protecting privacy and the need to use individuals' information. A paradox looms: Canadians demand high-quality, accessible and efficient health care *and* privacy for their personal health information. Both aims are laudable and serve each other, but only if properly understood.

Recent legislative initiatives in Canada such as the Personal Information Protection and Electronic Documents Act, enacted in April 2000, will set the framework for the manner in which consent is required for the use of health information and will establish the context for exemptions from consent. The status of health information within this legislative framework is currently undecided. Legislation passed in the United States and Europe has strengthened the need for explicit consent for the use of health records in research and audit. Such initiatives are commendable in that the privacy of individual information is of paramount importance, but they may have adverse consequences. Depending on the stringency of such initiatives, many research and audit functions such as health services research and cancer registries may be at risk, as was demonstrated recently in the United Kingdom.[4] Strict consent laws can introduce an important authorization bias[5–8] when patients who release personal health information for health research differ significantly from those who do not. Such a bias may result in an inaccurate estimate of the health status of the population.

The benefits of using health records for both research and program evaluation are well known. These include monitoring the health of the population, identifying populations at risk, determining the effectiveness of treatment, assessing prognosis and the usefulness of diagnostic and screening tests, administrative support, cost-effectiveness analysis, and assessing the appropriateness and adequacy of care.[9] Gordis and Gold[10] emphasized the medical discoveries derived from medical records research, particularly in the fields of cancer, cardiovascular disease, communicable disease and children's health. In Canada, cancer registries and health services research institutes have provided essential information about the health status of Canadians. Studies demonstrating variations in health care use,[11] socioeconomic gradients in health status after myocardial infarction,[12] the impact of influenza vaccination on admissions to hospital of elderly people,[13] and trends in cancer morbidity and mortality,[14] to name but a few, are possible only through the maintenance of population-based databases.

On the other hand, there are few Canadian examples of harms associated with the use of personal health data for administrative and research purposes by publicly funded institutions. In general, health data are well protected by the health care system and provide an admirable example of public trust. Garfinkle,[15] in an American context, documented examples of abuse of personal health information. It must be stated in categorical terms that unwarranted disclosure of health information, regardless of its format, is to be condemned. Health systems managers, researchers and publicly funded institutions must assure individuals that their health information is not only secure but also indispensable to the operation of the health care system and the provision of high-quality care.

The call for explicit consent for the use of health information is intended to respect the autonomy of individuals and recognize their right to self-determination. However, it is unclear whether explicit consent would achieve that intended goal, given that the number of uses of individual data are currently unknown and future uses are unknowable. It is debatable whether individuals wish to give explicit consent every time their health information is accessed or processed. In honouring autonomy, one could unintentionally overburden individuals.

What form should consent take in these circumstances? Models range from full explicit consent for each use of health information to models in which no patient consent is required (Table 1). The issue of the appropriate model of

patient consent for the use of electronic information should be regarded as a research priority.

Looking for solutions: the concept of social trust

The privacy paradox poses a potential threat to the realization of a health care system that meets the highest standards of care and accountability. How then can we overcome the privacy paradox? In general, we see 4 particular avenues of approach, involving transparency and regulation of access and use of information. Together, they may answer public concerns.

Technical considerations

There is reasonable, but not perfect, assurance that security from inappropriate disclosure can be maintained. This derives from both technical and procedural safeguards, as classified by Stallings.[16] In addition to technical safeguards, the codes of ethics for health care professionals recognize the importance of protecting confidentiality. Violations of this code can result in consequences that range from professional reprimand to suspension and revocation of licence. Legislation should provide sanctions against unwarranted disclosure of confidential health information.

Process and safeguards

There are sets of procedural changes that organizations entrusted with health care information can explicitly endorse. These include, but are not limited to, the following:

- The adherence to agreed standards of fair information practices.
- The appointment by organizations of a "data guardian" who would be responsible for the security of data and approval of its uses. The office of the data guardian would also consult with the ethics review board and the office of the privacy commissioner when necessary.
- The assurance that personal health information will not be used for profit or marketing purposes without explicit consent.
- The mapping of the flow of personal information within the health care system. A process similar to the Caldicott Committee's identification of data flows[17] should be undertaken.

Information directives

There is also a need to enhance the understanding of privacy rights, that is, autonomous individual control over personal information, and to educate health care consumers and providers about the range of uses of health information. The idea of advanced directives has gained currency for facilitating end-of-life care and articulating patient preferences. Two of us have developed an analogous health information directive that describes the range of health care information uses and permits the patient to authorize the use of various elements of health care information.[18] Schoenberg and Safran[19] recently described a patient-controlled medical record accessible on the World Wide Web that permits the patient, in consultation with the health care provider, to agree about which elements of

Table 1: Summary of models for consent to use health information

Model	Description	Strengths and weaknesses	Jurisdictions
Full consent	Full explicit consent is required for each use of an individual's data. In this model, people are asked to consent to each use of personally identifiable information, including audits, quality assurance, reminder notices and research.	• Administratively onerous • Expensive • May impose unnecessary burdens on consumers	Theoretical
Opt in	Participants give explicit consent on initial contact with health care program and sign a waiver for the use of information, with suitable assurances of confidentiality. In this model, individuals are registered in the program, provided with information about all the potential uses of the information and asked to sign a form for the use of personal information. There is an option to opt out at any time.	• Consistent with certain interpretations of fair information practices • Administration may impose unwelcome burdens on practitioners • May have unfavourable cost:benefit ratio • Authorization bias	Minnesota
Opt out	Participants are assumed to want to contribute health information and are given the opportunity to opt out of the program at their request.	• Most likely to achieve high coverage rates • No burden on practitioners • Information about the use of the data is available to consumers • Not regarded as consent by consumers	Australia Icelandic genetic database
No consent	No consent is sought for the use of personal information, but it is held in trust, with assurances of confidentiality. In this model, information is routinely collected and used with very strict protection and security.	• Information about the use of the data is not made available to consumers • No consent • Unclear whether registrants are aware of the	Cancer registries New Zealand Northern Ireland

clinical content should be included in an accessible patient record and what level of security is required.

Social trust

The argument for the social utility of health records usage is stated clearly by Gostin and Hadley.[20]

Despite the importance of explicit informed consent in protecting patient autonomy, requiring such consent before allowing any personal health data to be obtained would discourage and even halt much socially valuable research. The cost and effort of obtaining previous approval for large scale statistical analyses that use data from tens of thousands of patients would be burdensome.

We all derive benefit from a health information system that has extensive coverage and linkages. Our privacy rights are, however, maximized by restricting access to health information. The more access is restricted, the more privacy is protected. However, if everyone followed this course, the system would fail and no one would derive benefit from a health information system. Hence, we may be worse off if everyone exercises the right to privacy to its fullest extent. Trust, cooperation and recognition of the common good are required.

Health care is a publicly funded enterprise. As such, we are all responsible for its governance. The potential risk of invasion of privacy or unwarranted disclosure of confidential health information can be kept low. Because confidentiality concerns can be addressed by both technical and procedural methods, they should not serve as a card to trump social needs. We would argue that social utility supersedes these concerns.

Conclusion

The security of health information and personal privacy is a priority for all Canadians. Thus far, researchers, administrators and health care providers in Canada have an excellent record of protecting the confidentiality of health data. Health care consumers can reciprocate by allowing the collection and use of health information for program administration, quality control and research. When viewed as a joint trust and common good, the promises of the information age can be achieved.

This article has been peer reviewed.

Dr. Upshur is with the Primary Care Research Unit, the Departments of Family and Community Medicine and of Public Health Sciences, and the Joint Centre for Bioethics, University of Toronto, and the Sunnybrook & Women's College Health Sciences Centre — Sunnybrook Campus, Toronto, Ont. Dr. Morin is with the Joint Centre for Bioethics, University of Toronto, Toronto, Ont. Dr. Goel is with the Department of Health Administration, University of Toronto, Toronto, Ont.

Competing interests: None declared.

Contributors: Dr. Upshur originated the idea and sketched out the initial arguments and participated in the writing of each draft of the manuscript. Dr. Morin performed literature searches, contributed arguments and participated in the writing of each draft of the manuscript. Dr. Goel contributed ideas, arguments and references and participated in the writing of each draft of the manuscript.

Acknowledgements: We thank Dr. Verna Mai, Director of Screening, Cancer Care Ontario and the Ontario Cervical Screening Program for support and critical feedback on this project.

Dr. Upshur is supported by a Research Scholar Award from the Department of Family and Community Medicine, University of Toronto, and a New Investigator Award from the Canadian Institutes of Health Research.

References

1. Delete Big Brother files, Quebec says. *Globe and Mail* [Toronto] 2000 May 18;A1.
2. *Canadians highly value the privacy and confidentiality of their health information*. Ottawa: Canadian Medical Association; 1999 Nov 29. Available: www.cma.ca/advocacy/news/1999/11-29.htm (accessed 2001 July 6).
3. Policy and Planning Division, Saskatchewan Health. *Consultation paper on protection of personal health information*. Available: www.health.gov.sk.ca/ph_br_health_leg_phiq/default.htm (accessed 2001 July 9).
4. Kmietowicz Z. *Confusion reigns as data law continues to threaten research*. BioMedCentral; 2001 May 16. Available: www.biomedcentral.com/news/20010516/03 (accessed 2001 July 6).
5. Yawn BP, Yawn RA, Geier GA, Xia X, Jacobsen SJ. The impact of requiring patient authorization for use of data in medical records research. *J Fam Pract* 1998;47:361-5.
6. Jacobsen SJ, Xia Z, Campion ME, Darby CH, Plevak MF, Seltman KD, et al. Potential effect of authorization bias on medical record research. *Mayo Clin Proc* 1999;74:330-8.
7. McCarthy DB, Shatin D, Drinkard CR, Kleinman JH, Gardner JS. Medical records and privacy: empirical effects of legislation. *Health Serv Res* 1999;34:417-25.
8. Woolf S, Reptemich S, Johnson R, Marsland DW. Selection bias from requiring patients to give consent to examine data for health services research. *Arch Fam Med* 2000;9:1111-8.
9. Melton LJ III. The threat to medical-records research. *N Engl J Med* 1997;337:1466-9.
10. Gordis L, Gold E. Privacy, confidentiality and the use of medical records in research. *Science* 1980;207:153-6.
11. Goel V, Williams JI, Anderson GM, Blackstein-Hirsch P, Fooks C, Naylor CD, editors. *Patterns of health care in Ontario. The ICES practice atlas*. 2nd ed. Ottawa: Canadian Medical Association; 1996.
12. Alter DA, Naylor CD, Austin P, Tu J. Effects of socioeconomic status on access to invasive cardiac procedures and on mortality after acute myocardial infarction. *N Engl J Med* 1999;341:1359-67.
13. Fedson DS, Wajda A, Nicol JP, Hammond GW, Kaiser DL, Roos LL. Clinical effectiveness of influenza vaccination in Manitoba. *JAMA* 1994;270:1956-61.
14. *Canadian cancer statistics 2000*. Toronto: Canadian Cancer Society; 2000. Available: www.cancer.ca/stats/index.html (accessed 2001 July 6).
15. Garfinkle S. To know your future. In: *Database nation: the death of privacy in the 21st century*. Cambridge (MA): O'Reilly; 2000. Available: www.oreilly.com/catalog/dbnationtp/chapter/ch06.html (accessed 2001 July 6).
16. Stallings W. *Network and internetwork security: principles and practice*. Englewood Cliffs (NJ): Prentice-Hall; 1995.
17. Caldicott Committee. *Report on the review of patient-identifiable information, December 1997*. London: NHS Executive; last updated 1999 Apr 24. Available: www.doh.gov.uk/confiden/crep.htm (accessed 2001 July 6).
18. Upshur REG, Goel V. The health care information directive. *BMC Medical Informatics and Decision Making* 2001;1:1. Available: www.biomedcentral.com (use search engine) (accessed 2001 July 10).
19. Schoenberg R, Safran C. Internet based repository of medical records that retains patient confidentiality. *BMJ* 2000;321:1199-203.
20. Gostin L, Hadley J. Health services research: public benefits, personal privacy and proprietary interests. *Ann Intern Med* 1998;129(10):833-5.

Correspondence to: *Dr. Ross E.G. Upshur, Sunnybrook & Women's College Health Sciences Centre — Sunnybrook Campus, Rm. E349B, 2075 Bayview Ave., Toronto ON M4N 3M5; fax 416 480-4536; rupshur@idirect.com*