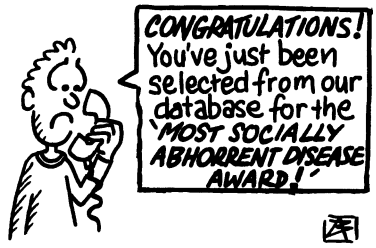
HEALTH on line

Meredith Carter

The implications for privacy of the spread of information technology in the health sector.



A recent Commonwealth House of Representatives Inquiry has found that information technology (IT) offers great potential to improve health care. The Inquiry made sweeping recommendations for the introduction of unique patient identifiers, smart cards and a national database of clinical records. This article outlines these recommendations, explores the potential impact on privacy and the adequacy of the current legal framework to protect consumer interests. It concludes that the Committee's recommendations have great potential, only some of which have anything to do with the interests of health consumers.

Confidentiality of health information

Confidentiality of personal information has traditionally served as the cornerstone of the trust between consumer and health care practitioner. This trust is essential to accurate and safe diagnosis and the development of appropriate recommendations for treatment. It has also served as the major way in which the privacy of consumers' personal information has been protected in the health sector.

A personal health care record today is likely to contain more intimate details about an individual than can be found in any other single document.[1] Clinical information may range from diseases or conditions carrying some social stigma through to details such as life expectancy and, increasingly, information about the individual's genetic make up and predisposition to any particular conditions or illnesses.

In addition, the likely contents of medical records include:

- identification details such as name, address, ethnicity and date of birth;
- financial information such as health insurance status, eligibility for any government benefits, employment status and details;
- social information such as family relationships and arrangements including housing and work history, drug and alcohol use and other lifestyle matters, which can sometimes extend to details of assaults, sexual partners or practices, births outside marriage, contraceptive use and pregnancy terminations.[2]

Traditionally it has been argued that the particularly sensitive nature of personal health data warrants special protection from unnecessary disclosure to third parties. However, many see the relentless capacity for data collection facilitated by information technology as perhaps the greatest threat to personal privacy. Increasingly the privacy issue is not about the sensitivity of the information but the more basic issue of control over the flow of information about oneself and one's identity.[3]

As Microsoft head, Bill Gates, has observed, IT has the capacity to significantly tamper with that identity in a way which is not possible while records remain dispersed and paper based:

> The same digital technology that makes it so easy to communicate around the world also makes it easy to snoop ... Today the scattered nature of

Meredith Carter is the Director of the Health Issues Centre, Melbourne.

information protects your privacy in an informal but real way. Much personal information tends to be kept for only a while, and data from various sources isn't correlated to create a larger portrait.[4]

Policy developments

Although these privacy issues are recognised, a succession of policy documents have identified patient linking systems as critical to improving the quality of health care in Australia. These include the Australian Quality in Health Care Taskforce, the National Health Information Forum, and the Australian Pharmaceutical Advisory Council.

Several States and Territories are already developing data linking systems based on the use of a common patient master index (PMI). These include Western Australia and the ACT as well as some health care networks in Victoria. PMI systems allocate a code number or identifier for each patient to be used each time they receive a service and have been in use in hospitals for many years. Used across a network of services, a PMI would allow an individual's use of health services to be more accurately followed through the health system. When patients attend for treatment, all relevant records can be located with the PMI regardless of where a particular service was received. Thus a PMI could identify records held in public sector agencies such as hospitals and community health centres, with those held by private practitioners such as GPs and pharmacists. It could also locate the records held by agencies such as pathology laboratories or radiology services, day surgeries and private hospitals.

Some PMI proposals go a step further. Instead of the PMI being used simply to identify where information is held, it can be used to access the individual databases holding a consumer's records. Alternatively, the PMI can be used to develop large clinical databases collating centrally all the data relating to each individual health consumer.

Health on Line Committee

The use of a common database to support such systems recently received strong endorsement from the House of Representatives Standing Committee on Family and Community Affairs Inquiry into Health Information and Telemedicine (the Health On Line Committee).[5] In its report *Health On Line,* the Committee recommended the introduction of:

- a patient-held electronic health card supported by a consumer storage system (smart cards);
- a national backup facility (the database);
- use of subsets of the Medicare number as a unique lifetime identifier for each person in Australia.

The combined effect of these proposals suggests reopening the door to the introduction of the Australia card. It was the community's overwhelming rejection of a universal identification card which led to the rejection of the Australia card and the introduction of the Commonwealth *Privacy Act 1988* to guard against surveillance of the populace. Use of the Medicare number, introduced to facilitate payment for health care, on a card designed to facilitate delivery of health care, and further use of the medicare number to create a comprehensive centralised database of the community's use of health services, represents a dramatic expansion of its function. It is this kind of *function creep* the *Privacy Act* was intended to prevent.

Apart from their combined effect, each of the *Health on Line* proposals separately raises significant privacy issues. Yet the Committee took the view that privacy concerns expressed to the Inquiry by consumer organisations, the Department of Health and Family Services and the Privacy Commissioner, were overrated. Somewhat astonishingly, the Committee drew on the attitude of the banking industry to consumer consultation to reinforce this view. They noted that:

> ... when the banking industry imposed electronic commerce on its customers it did not provide the opportunity for its customers to raise any privacy or confidentiality concerns ... The committee found no grounds that the confidentiality, privacy and security of individuals will be compromised by a major database. On the contrary, it was acknowledged that the old paper-based method of managing and exchanging health information and data posed greater risks of being breached by illegitimate access.[6]

In deference to community concerns, the Committee recommended that the comprehensive national database of personal health information should be under the control of the Health Insurance Commission because it is subject to the Commonwealth *Privacy Act 1988.* Other than that, the *Health on Line* Committee felt that consumers would be adequately protected by the codes of ethics which have traditionally governed the activities of doctors and other health care professionals.[7] They did not acknowledge the trenchant criticisms to which these codes have been subject in recent times, not least for their failure to deal adequately with privacy issues.[8]

Consumer sovereignty

Confidentiality and security of the record are key aspects of privacy. However, modern privacy principles emphasise consumer control and access to their records as equally important. Indeed in an electronic environment, since absolute security of the record is a myth, the accuracy of the data and informed consent to its exchange become even more important. Consumer access is of course vital to both.

The Health On Line Committee considered consumer control would be adequately protected because each individual would carry his or her own health record on a smart card. This, according to the Committee, meant consumers could determine who could have access, with access protected by a PIN number.[9]

This level of consumer control is, however, most unlikely since for entirely practical reasons each and every health practitioner a consumer attends is likely to create their own record, reflecting or expanding on whatever they put on the consumer's smart card. It would remain up to the practitioner's interpretation of their obligations under the common law duty of confidence as to which third parties they gave access to this information. Increasingly, these individual health service databases will also be electronically networked, bypassing the need to access the consumer's smart card at all.

The Health On Line Committee did not clarify how consumers themselves would have access to the information on their smart card. Consumers may be able to get a printout from the backup database held by the Health Insurance Commission as it is governed by the *Privacy Act.* Information Privacy Principle 6 in the Act requires Commonwealth public sector agencies to provide access to the subjects of any personal data they hold. However, this seems a cumbersome way for consumers to gain access to information that is after all on the plastic card they have in their pocket.

The Commonwealth *Privacy Act* does not apply to the State public sector or to private sector health practitioners. The common law position affirmed by the High Court in *Breen v Williams*[10] is that consumers do not have a right of access to health records created by private sector health practitioners or agencies. This means that under the *Health On Line* proposals, direct consumer access to personal health records remains at the discretion of their health practitioners (who would need card readers and printers to conduct their business). The Committee made no recommendation for legislation to redress this situation and only the ACT has done so to date.[11]

Nor was there any suggestion as to how consumers might control what their health practitioners put on their smart cards. Indeed, under this proposal, far from being empowered by having their record on their person, it is entirely possible that consumers would feel like mere *card couriers*. Their role would be to carry their card between health care providers as required, with no necessary access to or control over its contents. Worse still, the information they courier about may be derogatory, inaccurate or contain the potential for significant discrimination against them.

Other interests in health data

In addition, consumers may or may not have much control over release of data from the backup database. For example, the *Health On Line* Committee also supported the introduction of a Pharmacy Intranet proposal based on the British Columbia PharmaNet system in Canada.[12] This system would involve electronically linking pharmacists to a national database holding profiles of each Australian's consumer's medication use and could be used to pick up both contraindicated prescriptions and drug abuse.

In British Columbia, the program is overseen by national privacy laws. The Health On Line Committee suggested that in Australia this database could be managed by the Pharmacy Guild, a private sector association, not covered by the Commonwealth *Privacy Act*. The Committee recommended the Guild database would need to be tightly linked to the Health Insurance Commission Pharmaceutical Benefit Scheme database for payment purposes.

To date, a far less ambitious proposal focussing on electronic prescriptions and PBS concession eligibility checks, has been introduced on a pilot basis with consumer consent to participate.[13] This, of itself, is interesting in that the proposal has been promoted for its benefits to the quality of care but its development to date only relates to efficiency and cost minimisation purposes of government and providers.

There are many other proposals for the use of IT to create data linkages and profiles of consumers for funding, quality assurance, service planning and various public health purposes which are increasingly reliant on access to identifiable consumer records and data matching between various agencies. The Health Insurance Commission alone now has responsibility for at least five different databases including the immunisation register and the detection of so called *doctor shoppers*. This is the term used to describe people who attend multiple doctors in order to get access to and abuse prescription medications. In relation to the latter function, the Health Insurance Commission has noted that it cannot be assumed that consolidating information in this way will result in accurate profiles. Thus, the Health Insurance Commission acknowledges that in attempting to track down *doctor shoppers*:

> We would inevitably pick up patients who were very sick and therefore making high claims, but no further action would be taken.[14]

In confidence

The enthusiasm of the Health On Line Committee for the mass collation of personal health information is in stark contrast to the findings only two years previously of another Commonwealth Parliamentary Committee (the Melham Committee).

The Melham Committee was formed specifically to inquire into the protection of confidential personal and commercial information held by the Commonwealth. The Melham Committee's report *In Confidence,*[15] expressed serious reservations about the extent to which government organisations demonstrate any serious commitment to the protection of privacy. It referred to the findings of the New South Wales Independent Commission Against Corruption which exposed widespread trading in personal health information by both public and private sector agencies such as the Department of Social Security, banks and the Health Insurance Commission. The Melham Committee's Inquiries produced further evidence of its own. It concluded that although the Health Insurance Commission had improved its performance in terms of protecting privacy, other organisations dealing with personal information, including the Commonwealth Health Department, had been slow to do so.

There are two levels of threat to be considered in relation to networked records and computerised databases: internal and external. Internal threats include the people who have been authorised to have some level of access to the records, for example health practitioners and their administrative staff. There may be a lack of understanding by authorised users of the concept of privacy itself and the harm that can result if this is undermined. Whilst a range of different restrictions on access are generally imposed according to the function the authorised person is required to perform, simple browsing through computer records by employees is a recognised problem, for example.[16]

The extent of the problems authorised users can create is reinforced when one considers the numbers involved, given that it has been estimated that in any one standard episode of hospital care, between 40 and 160 people may have legitimate cause to access an individual patient's records.[17] Increasingly, however, IT is also supporting the integration of health (and often other community services) into multi-agency networks such as the Victorian Health Care Networks. Thus by way of comparison, in one large multi-campus *hospital* with a computer-based medical records system in the United States, there are 5100 users of the hospital's information system. Of these users, 3700 people (mostly nurses) have access to the clinical information subsystem.[18]

External threats include those whose intentions are patently unfair or illegal. As the Victorian Government has noted in its recent Discussion Paper, *Information Privacy in Victoria,* information, such as that likely to be maintained on a computerised database, is just as valuable and the technology is just as readily available to those whose interests are not legitimate as to those whose interests are.[19]

Need for protection

Whether the threats are internal or external, many other commentators have also warned against the significantly

increased risks of illegitimate access presented by centralised collections of personal health data and the need for a comprehensive legislative framework to deal with these challenges.[20] The Victorian Government has stated its intention to enact data protection legislation in this State, pointing out that:

> In Australia there is no general legislative or common law protection of information privacy in existence that could underpin the development of suitable privacy policies for the information age.[21]

Thus at the State level, in addition to the duty of confidence, consumers are left with a spectrum of statutory provisions found in Health Acts constraining disclosure of personal health information collected by public sector agencies.[22] These provisions are coming under significant stress as the capacity for electronic data linkage expands the potential uses of health data. The need for reform is discussed further in 'Can You Keep a Secret?' (also in this journal). However, a particular concern is that currently, health consumers have little avenue for redress of any complaints they may have about any breach of their privacy even in the public sector.

For example, in Victoria complaints can be made to the Health Services Commissioner but she has limited jurisdiction and cannot make enforceable determinations. In addition, consumers are likely to be completely unaware that a breach of privacy (such as browsing, illicit trading in personal data or other unauthorised disclosure) has occurred. Prevention and detection of IT abuse relies on adequate systems being in place including detailed privacy policies and security measures, such as audit trails and staff education. Without any legislative obligations to develop such systems or any overarching body responsible for monitoring them on behalf of the public, implementation of such systemic responses is likely to be patchy and inconsistent.

The adequacy of the regulatory infrastructure is crucial to consumer and community confidence that emerging uses of information technology to manage health information are sufficiently privacy protective. Without it, consumers who are not confident that their privacy will be respected may not seek treatment or may give unreliable information to their health care providers. This puts at risk not only the health of the individuals concerned but also undermines broader strategies to promote public health.

Finally, whilst some States and Territories are beginning to act, the failure of the Federal Government to extend the Commonwealth *Privacy Act* to the private sector is a major impediment to the development of consistent approaches to the protection of privacy in health care. The Australian population is a mobile one and as noted above, proposals for the utilisation of health care information are not bounded by State borders.

Consumer organisations support the efforts of the Privacy Commissioner to fill the breach by negotiating a national voluntary code specific to the health sector. However, achieving this is likely to be a herculean task given the entrenched opposition in the health sector to fundamental principles, such as consumer access. Meantime health care consumers are left with no consistent framework for protection or redress in an environment where the potential uses of IT are beginning to be realised with enormous risks both to privacy and because of this, enormous risks to public health promotion strategies too.

References

1. Klugman, Ellen, Toward a Uniform Right to Medical Records: A Proposal for a Model Patient Access and Information Practices Statute, (1983) 30 *UCLA Law Review* 1317–1377 at 1349.
2. The Commentary to the New Zealand Health Information Privacy Code (1994), Rule 4 sets out a useful list of the types of sensitive information which may be found in health records.
3. See Australian Law Reform Commission, 'Unfair Publication, Defamation and Privacy, 1979, para. 243.
4. Gates, Bill, 'Privacy Laws a Step Behind Technology', *The Age* (Melbourne), 19 September 1995.
5. Commonwealth, *Health on Line*, House of Representatives Standing Committee on Family and Community Affairs Inquiry into Health Information Management and Telemedicine Report, 1997.
6. House of Reps, *Health on Line*, para. 5.26–5.27.
7. House of Reps, *Health on Line*, para. 5.38.
8. For example, O' Connor, Kevin, 'Privacy in Practice, Especially in the Caring Professions', in Third Annual Conference of the Australian Association for Professional and Applied Ethics held in Wagga Wagga, October 1996, *Proceedings*, 79, 90; Kuhse, Helga, 'Confidentiality and the AMA's New Code of Ethics: An Imprudent Formulation?' (1996) 165 *Medical Journal of Australia* 327; Komesaroff, Paul, 'Confidentiality and the AMA's New Code of Ethics: An Imprudent Formulation?' (1997) 166 *Medical Journal of Australia* 221.
9. House of Reps, *Health on Line*, para. 5.71–5.72.
10. 1996 (186) CLR 71.
11. *Health Records (Privacy and Access) Act 1997* (ACT). Although NSW now has a Data Protection Bill before Parliament and Victoria is also promising legislation in the imminent future.
12. House of Reps, *Health on Line*, p.xvi and pp.69-71.
13. The National Pharmacy Intranet Demonstration Project, an initiative of the Pharmacy Guild of Australia, through Guild Commercial, in partnership with the Department of Health and Family Services and the Health Insurance Commission, which seeks to demonstrate the technical feasibility, cost-effectiveness and acceptability of a pharmacy intranet, 'Getting Connected', project circular, 15 September, 1998.
14. Comment by the Health Insurance Commission's Director of Compliance reported in 'HIC Targets Patient Fraud' (1996) 8(7) *Australian Medicine* 1.
15. Commonwealth, House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence*, 1995.
16. O'Connor, Kevin, 'Meeting Public Concerns', Paper presented to Joint Australian/OECD Conference on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure, 7-8 February 1996, Canberra, 4. See also the measures developed to avoid this problem in Safran, Charles, Rind, David, Citroen, Mieke and others, 'Protection of Confidentiality in the Computer-based Patient Record', (1995) 12(3) *Clinical Computing* 187.
17. Nisselle, Paul, 'Privacy in Medicine: Issues Old and New', (1991) 154 *Medical Journal of Australia* 207, 209.
18. Safran, Charles and others, above, ref. 16.
19. Victorian Government, *Information Privacy in Victoria: Data Protection Bill*, Discussion Paper, 1998, 7.
20. Crowe, Bernard, *Telemedicine in Australia*, Australian Institute of Health and Welfare Discussion Paper, 1993; US Congress Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information*, Report OTA-TCT-576, 1993; Minor, William, 'Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections', (1995) 28 *Columbia Journal of Law and Social Problems* 253; and Gostin, Lawrence and others 'Privacy and Security of Personal Information in a New Health Care System', (1993) 270(20) *Journal American Medical Association* 2487.
21. Victorian Government, *Information Privacy in Victoria: Data Protection Bill* Discussion Paper, 1998, p.8.
22. For example, s.141 *Health Services Act 1988* (Vic.).