

**House of Representatives Standing Committee
on Legal and Constitutional Affairs**

**Inquiry into Privacy Amendment
(Private Sector) Bill 2000**

**Submission by
Health Issues Centre**

May 2000

**Health Issues Centre Inc.
Level 11
300 Flinders St
MELBOURNE VIC 3000
Ph 03 9614 0500
Fax 03 9614 0511
Email hicgen@vicnet.net.au**

TABLE OF CONTENTS

Summary _____	3
Introduction _____	4
Current developments in the health sector _____	5
Privacy problems _____	6
General Framework of the Privacy Bill _____	8
Relationship to state legislation _____	10
Employment Records _____	10
The principles _____	10
Subject Access _____	10
Transfer of records _____	11
Correction _____	12
Disclosure Provisions _____	12
Research _____	13
Identifiers _____	14
Conclusion _____	15

Summary

Health Issues Centre supports the development of a nationally consistent legislative framework for the protection of privacy in Australia and especially in the health sector. We agree that this is especially important in health, given:

- the high level of overlap between public and private health services;
- the particularly sensitive nature of health information; and
- the increasing use of information technology to manage and link health records across a variety of settings including across state boundaries.

The Centre is concerned however that the 'light touch' approach adopted in the Bill will not achieve such a result. Rather it is likely to foster the continuation of the current unsatisfactory interplay of common law, ethical codes and legislative provisions relating to privacy and confidentiality currently applicable to personal health information around Australia. Complaints based regulation of the health sector is also particularly inappropriate in an environment where consumers may not even know that their privacy has been breached.

The attempts made to modify the National Privacy Principles to accommodate health concerns regarding for example, access, disclosure of records and use of identifiers, has served only to reinforce the view that the framework is inappropriate for the health sector. This is particularly so if the framework is to be enforced through industry codes and industry complaints bodies. At best, even if health were to be dealt with under the default scheme, the framework would still leave health practitioners in an uncertain position and consumers with the patchwork of 'protection' they have now.

A national regime for the health sector is required but this should be by way of separate health specific legislation or at the very least, a legislative code within a stronger overarching framework. Either model should build at a minimum on the protections offered by the ACT Health Records (Access and Privacy) Act and the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines

Our comments on the current Privacy Amendment (Private Sector) Bill fall under the following headings:

1. Introduction
2. Current developments in the health sector
3. Privacy problems
4. General framework
5. The Principles
6. Conclusion

Introduction

Health Issues Centre is a not for profit policy analysis group which researches health issues from a consumer perspective and aims to promote reform of the health system to meet the needs of consumers, particularly those most disadvantaged by current arrangements. The Centre is funded through its membership and subscriber base, competitive consultancies and research and project grants. The Centre is also the lead agency in the National Resource Centre for Consumer Participation in Health. The Centre has been very active over the past decade in debates around the benefits and risks of the electronic era in the health sector, particularly highlighting the need for greater attention to consumer privacy.

This has included [organising a number of public seminars on information privacy issues](#) and undertaking consultancies and consultations within the health sector including with health consumers themselves on these issues, such as:

- The Power of Information: Health Providers, Consumers and Treatment Records (1993)
- Report on Better Health Outcomes Through Data Linkage - The Impact On Privacy (1998) for Department of Health and Aged Care Health Outcomes Branch
- Report on Public health law and privacy for Australian Institute of Health Law and Ethics published in Public Health Law in Australia - New Perspectives(1998)
- Report on Current Privacy Regulation and risks relating to the Proposed Health Care Networks clinical data repository (CDR) for a consortium of Victorian health care networks. (1998).
- Report on Consumer attitudes to Information Technology in General Practice (1998) for the Commonwealth General Practice Evaluation Program .
- Retainer on Health Information Privacy for a Victorian Health Care Network (1999/2000)

The Centre has also been a participant in many of the working parties and committees relevant to these issues established at the state and federal level. A sample include:

- [Department of Human Services Victorian Hospital Patients Register Reference Group \(current\)](#)
- [Victorian Consumer Electronic Service Delivery Network \(current\)](#)
- [.General Practice Computing Group Management Committee](#)
- [Department of Health & Aged Care National Health Information Technology Workshop \(1998\)](#)
- [Department of Human Services /Southern Health Care Network Smart Card Trial Consumer & Privacy Issues Subcommittee](#)
- [Department of Human Services Victorian Genetic Services Advisory Committee](#)
- [Standards Australia Health Informatics Committee](#)

The Centre's Director is frequently requested to make presentations and commissioned to write articles addressing these issues. The minor thesis component of her Masters of Law degree was a critique of *Patient Privacy and Health Information Management in a Networked Environment*.

The Centre has also been keen to promote consumer participation in the electronic age and has not only developed its own websites but also the Information Technology and Health Promotion project (the Chronic Illness Alliance On Line project), which won the 1999 VICHealth Health Promotion in the Community Award.

Current developments in the health sector

Over the last decade, the use of information technology has increasingly been promoted as a means to improve delivery of services and better allocation of resources for health care. These efforts are gathering increasing momentum and in the last six months two major national reports have been endorsed by Australian Health Ministers which will concentrate these efforts.

Health On Line (1999) is the report of the National Health Information Management Advisory Council which sets out *A Health Information Action Plan for Australia*. This report envisages the electronic linkage of data for better co-ordinated care. It also envisages the creation of enhanced data linkages between existing data sets and the creation of a new national clinical/administrative data set. Other aims include the expansion of the Pharmacy Intranet "Getting Connected" project (which involves eligibility checking for PBS concessions). *Health On Line* also envisages the use of "increasingly sophisticated mechanisms such as the use of 'pseudo-identifiers' which can allow data about an individual to be linked to other data about the same individual but still protect his/her identity"¹. The report stresses the need for robust privacy protection.

Health On Line has been followed by the release of an Issues Paper by the National Electronic Health Records Taskforce in March 2000. This document canvasses the feasibility of one of the major building blocks underpinning *Health On Line*. Following release of the Issues Paper, the Taskforce will be making recommendations to the Australian Health Ministers in July this year on the appropriate framework for a national system of electronic health records. Both reports note the development of the Privacy Bill for the Private Sector. *Health On Line* specifically suggests the possibility that additional measures may be necessary to allow initiatives to proceed in a robust privacy framework, in the area of communicating information for better coordinated care and in linking data for better policy and planning.²

It is certainly our view that the current Bill is inadequate for this task but we reject the suggestion that its inadequacies can simply be remedied at a later date. We

¹ National Health Information Management Advisory Council, *Health On Line* (November 1999), Part 6.2.1 p.77

² National Health Information Management Advisory Council, *Health On Line* (November 1999), Part 3.1.1 p.21.

are concerned that a range of pilot projects aimed at fostering the use of information technology in the health sector is already in place without an adequate privacy framework to support them. The speed with which developments in this area are taking place suggests that the appropriate legislative framework must be one of the first building blocks to be developed and implemented, before any steps are taken under the National Health Information Action Plan to escalate these efforts. It is clearly time to ensure that appropriate measures to protect patient privacy are in place. This requires enacting effective information privacy legislation specific to the health sector or at the very least, enhancing the current Bill including the development of a health specific legislative code.

Privacy problems

Our research and consultations with consumers over the last decade have highlighted over and over again the need for a strong framework of privacy protection. As the Independent Commission Against Corruption noted in 1992, there is widespread commercial trade in personal information including Medicare data between (officers of) government agencies and other institutions which do know better, such as banks, insurance companies and debt collectors³. These findings were reaffirmed by the Commonwealth, In Confidence, House of Representatives Standing Committee on Legal and Constitutional Affairs Report of the Inquiry into the Protection of confidential personal and commercial information held by the Commonwealth, (1995).

Abuses of privacy perpetrated by the federal Health Department in the Creutzfeldt Jakobs Disease (CJD) scandal were documented in detail in the Allars Report.⁴ In this case, women who received fertility treatment using hPG were discovered to be potentially at risk of CJD. The Department of Health's poor privacy practices included both a reluctance to provide potentially affected persons access to their own records and at the same time a willingness to override their privacy rights in order to protect another group of the public whose health might be put at risk. In this regard the Department released the names of the women potentially at risk to all Australian blood donation and organ banks with the result that a significant number of women only discovered they were at risk of CJD when they went to donate blood.⁵

However, it should be noted that these problems are not restricted to government agencies, hackers or other third parties outside the health sector. This is indicated by a small survey undertaken by the AIDS Council of NSW, used to inform the development of the National HIV/AIDS Privacy Guidelines⁶. They found 231 complaints about privacy breaches and noted that hospitals and health professionals were the main offenders. This reinforces a widely held view that it is

³ Ian Temby Unauthorised Release of Government Information - A Report by the NSW Independent Commission Against Corruption. in 14th International Data Protection and Privacy Commissioners' Conference Proceedings, Sydney: 1992: 187

⁴ Commonwealth, Inquiry into the use of Pituitary derived hormones in Australia and Creutzfeldt-Jakob Disease, Report (1994) (the Allars Report).

⁵ Commonwealth, Inquiry into the use of Pituitary derived hormones in Australia and Creutzfeldt-Jakob Disease, Report (1994) (the Allars Report), 665.

⁶ Commonwealth, Privacy and HIV/AIDS Working Party Report, 1992

not just people with sinister intentions hacking into the system we should be concerned about - people with the best intentions also inadvertently breach privacy. These included, release of an assault victim's HIV status to the police resulting in release and publication of this fact by the media. Other examples they found included inappropriate disclosure of information by health services to superannuation funds and to employers.

A sample of specific problems reported to Health Issues Centre (except as otherwise indicated) include:

- Continued resistance to consumer access to health records of which they are the data subject, even in the public sector (despite the existence of legislative rights under Freedom of Information legislation)
- Refusals to transfer records from one practitioner to another where a consumer changes doctor including where the doctor has retired
- Transfer of records from one practitioner to another without consent, for example with the sale of a practice
- Inappropriate use of health information by employers, for example a refusal to pay sick leave for a pre-existing condition disclosed on an employment application;
- Inappropriate use of personal information to market services by a government department, such as for example, sending a congratulatory letter and new mothers information pack to a mother whose baby was stillborn;
- Unauthorised creation of medical records, including the creation of a psychiatric file for the parent of a child patient, leaving the consumer forever tagged with the stigma of a psychiatric 'history' despite successful FOI action, because the file itself cannot be deleted under the FOI legislation.
- Inappropriate disposal of records, for example following transfer of services to Monash Medical Centre, large numbers of medical records were found by squatters at the old the Queen Victoria Hospital site.⁷

These examples are in an environment where the use of information technology in the health sector is still relatively limited. However examples of the risks which have eventuated to date are as follows:

- Notation by a hospital of patients' HIV status on computer, even where the admission is for a procedure unrelated to HIV/ AIDS so that the theatre lists projected on computer screens in the hospital sometimes listed both the names of the patient and their HIV status⁸
- Failure to check that a computerised record was up to date with the result that the patient received the wrong treatment and suffered a stroke.
- Inappropriate notification across police networks of persons suspected of being infected with HIV/AIDS⁹
- Information from Comcare (workers compensation) records including details from cases before the Administrative Appeals Tribunal, publicly disclosed after

7

8 Roger Magnusson 'Privacy, Confidentiality and HIV/AIDS health care' (1994) 18:1 Australian Journal of Public Health, 51,54.

9 Mark Irving, 'Police Keep HIV Data on Computers' The Australian, 3 July, 1990.

- an unknown person retrieved it from a stolen portable computer.¹⁰
- Health Insurance Commission employees browsing identified patient records.¹¹

It is likely that with the shift to wide scale use of information technology in the management of health records, the associated risks will increase. A recent example from the United States is the inadvertent exposure of several thousand records at the University of Michigan Medical Centre for two months of on public Internet sites. This oversight was not uncovered by the hospital despite the security protocols they had in place, until journalists notified the medical centre.¹²

General Framework of the Privacy Bill

It is with this background in mind that we have considered the appropriateness of the general framework of the Privacy Bill. Health Issues Centre has serious concerns that a complaints based framework managed by industry bodies is totally inappropriate. Most health complaints are now dealt with by the Health Complaints Commissions established under the Medicare Agreement in all states and territories. Their charter generally includes dealing with complaints regarding health information privacy. If the Privacy Commissioner himself is not to deal with these complaints under the new Bill, it makes little sense to create yet another body/bodies, which will inevitably be seen as less independent, to deal with such complaints.

Further it is difficult to see why consumers would have much confidence in the neutrality of health industry bodies. This is one reason why the statutory health complaints commissions were established to complement the existing medical and other boards dealing with miscreant practitioners. In addition, much of the health sector is not comfortable with the notion of consumer privacy rights, and particularly access to the information in their health records and current health industry codes reflect this ambivalence to varying degrees. This example is illustrative of why the utilisation of an industry body/bodies to manage a code in which complaints about just such an issue are likely to feature, is inappropriate.

Guidelines developed by the Privacy Commissioner are unlikely to advance this position given the experience of other health complaints handling bodies around Australia which have called for the introduction of an enforceable legislative right of consumer access for personal health information held in the private sector. Industry ambivalence is of course the key reason the ACT enacted its own Health Records (Privacy and Access) Act in 1987 and it should be noted that the Australian Medical Association has continued to disparage the legislation since its enactment.

¹⁰ Noted in Commonwealth, In Confidence, House of Representatives Standing Committee on Legal and Constitutional Affairs Report of the Inquiry into the Protection of confidential personal and commercial information held by the the Commonwealth, (1995) para 10.1.2.

¹¹ Ben Hart "Bored whiz tapped files" Herald Sun, January 28, 2000

¹² David Wahlberg, "Patient records on Web 2 months' Ann Arbor News, Feb 11, 1999, <http://aa.mlive.com/news/index.ssf?/news/stories/records2.frm>

It is also disappointing that in legislation relying on the development of industry based codes, the need to involve and gain support from all stakeholders is not more explicitly addressed. A real consultation process needs to be explicitly required in the legislation, addressing both the development of any codes and then addressing the Commissioner's approval of the codes. Without such requirements, the danger is that consultation will take the form of perhaps an opportunity to comment once a code has been drafted. The onus should be on the code drafters to actively seek input - it is unacceptable that consumers can be left on the outer until the last minute or that the onus should be on under-resourced consumer and community organisations to take the initiative.

Assurances that the Privacy Commissioner's role in approving industry codes will result in either a strong consumer protection focus or standardisation are not persuasive, particularly without any requirements for strong consumer participation in the development of the Codes. However, if as seems likely, the field is unable to agree on an industry Code acceptable to the consumer movement and the Commissioner, this may leave consumers dependent on the default scheme which itself is completely inadequate. A particular problem is that the scheme is complaints based rather than a pro-active watchdog and audit function.

This can be illustrated by considering the example of the recent prosecution of a Health Insurance Commission employee who was browsing the records of women of Asian backgrounds and those who had been on IVF programs.¹³ It is unlikely that any of those women knew that their privacy had been breached and accordingly in a complaints based system, it is possible that no action would ever have been taken to stop this behaviour. However, the Health Insurance Commission is subject to an enforceable code issued under s135AA National Health Act 1953. The code, called the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines was specifically introduced to deal with computerised claims information¹⁴ and has the force of law. A critical aspect of this code is that it requires regular audit of the Health Insurance Commission data bases which will reveal inappropriate access patterns. Compliance with the code is directly supervised by the Privacy Commissioner. Further non-compliance can and clearly does from time to time lead to criminal prosecution for breaches of consumer privacy.

In contrast under the Privacy Bill, the Privacy Commissioner has at best uncertain powers to approve, audit and discipline recalcitrant players. Further the appeal mechanisms are inadequate. It is vital that the Commissioner has clear authority to step in where either industry codes, complaints before industry bodies or specific determinations made by them, raise matters of public interest. . Credible penalties/sanctions must also be applicable. We strongly support the recommendations of the Australian Consumers Association for amendments to address these inadequacies in the Bill.

¹³ Ben Hart "Bored whiz tapped files" Herald Sun, January 28, 2000

¹⁴ Privacy Commissioner, Medicare and Pharmaceutical Benefits Programs Privacy Guidelines, May 1997.

We note that the National Health Act imposes criminal sanctions for breach of privacy and that the Australian Institute of Health and Welfare (AIHW) is also subject to stringent privacy regulation under the AIHW Act 1987 (C'th). Whilst we are pleased to note that these important public sector agencies dealing with health records will continue to be subject to vigorous regulation we fail to see why consumers whose records are held in the private sector, deserve less protection.

Relationship to state legislation

We are also extremely concerned that the deficiencies of the federal legislation may undermine state based efforts to introduce appropriate protection for health consumers. In this regard we note that the ACT Health Records Privacy and Access Act 1997 has now been in place for several years and applies consistently across both the public and private sectors. Other states have also been considering complementary legislation. Health Issues Centre considers that national consistency is appropriate but not at the level of the lowest common denominator and not in a way which is so inconsistent with the protection applicable in the public sector. In our view, the ACT legislation requires improvement given the increasing emphasis on electronic management and linkage of health records. At the very least, where it is inconsistent with the ACT legislation the federal legislation needs to be strengthened, not the other way round.

Employment Records

Health Issues Centre also wishes to expressed serious concern about the proposed exclusion of employment records from the ambit of the scheme. Employers not infrequently hold extensive health information regarding staff in their personnel files. Examples include comprehensive health status assessments and histories obtained as a condition of employment. The Bill should be amended to specify that personal health information held by employers does not fall within the definition of employee records. There is no reason to assume less potential for misuse of personal information health records obtained via an employer than those obtained direct from the health care practitioner who created them.

The principles

In addition to the general framework of the Bill, we are concerned that the attempt to modify the national principles to include health would with hindsight appear to have been misguided. Some necessary health specific principles have not been considered and other principles as discussed below create new problems for health consumers.

Subject Access

The Subject Access provisions in Principle 6.1 are an example of how the attempt to modify the national principles has not worked. Only some of the grounds on which access can be refused explicitly relate to health. If the other reasons for refusing access also apply (as would prima facie appear to be the case) the access

provisions would appear to be dramatically weaker than health consumers rights of access to records kept in the public sector. This leaves a private patient in a hospital bed with less rights of access to their records than the public patient in the bed next to them!

The failure to address this issue is particularly intolerable given that the Australian Law Reform Commission has recommended that the Freedom Of Information provisions which cover consumer access to their health records in the public sector, are themselves in dire need of strengthening.¹⁵ The need for a strong legislative statement of consumer entitlement to access records created based on their personal health information was soundly endorsed by the recent Senate Access to Records Inquiry.¹⁶

Indeed without a strong right of access some commentators suggest data protection or confidentiality laws are of little use. This view is especially persuasive in an electronic environment. As the Australian Institute of Health & Welfare (AIHW), has pointed out, since absolute security in this environment is a myth the best security is ensuring the individual record is accurate. Personal access and a right of challenge and correction are basic ways to help ensure accuracy.¹⁷

In addition, access to records and effective notice and informed consent are inextricably linked. Effective notification and truly informed consent to disclosure require that individuals know and understand the contents of the record in question, who will have access and how any information disclosed to third parties might be used.¹⁸

It is not surprising then that major reports addressing the infrastructure required suggest that the current legal and ethical positions concerning patient access to records of which they are the subject, are significant barriers to the successful implementation of electronic health records.¹⁹

Transfer of records

In addition it is not only consumer access to their records which is problematic in the health sector. Problems also arise when consumers ask for their records to be forwarded on to a new treating doctor either because they have changed doctors or their previous doctor has retired or died. The health specific ACT legislation incorporates two additional principles to addresses these issues which we understand are well utilised. The Commonwealth Privacy Bill also needs to include such principles for health records.

¹⁵ Australian Law Reform Commission submission to Commonwealth, Access to Medical Records, Senate Community Affairs Legislation Committee, Report (1997).

¹⁶ Commonwealth, Access to Medical Records, Senate Community Affairs Legislation Committee, Report (1997).

¹⁷ Bernard Crowe Telemedicine in Australia Australian Institute of Health and Welfare (AIHW) Discussion Paper (1993) 9.

¹⁸ Kevin O'Connor 'Confidentiality, Privacy and Security Concerns in the Modern Health Care Environment' (1994) 26:3 The Australian Computer Journal, 70.

¹⁹ For example, David Anthony and others, 'Report for Broadband Expert Services Group, Department of Communications and the Arts' by the Communication Centre, Queensland University of Technology in Demand for Broadband Services Consultancy Reports (1994), 381-2; Commonwealth, Senate Community Affairs Legislation Committee Access to Medical Records, Report (1997).

Correction

It is our understanding that the European Union Data Directive provides not just for correction of inaccurate data on the primary record but also requires advice of the correction to be provided to third parties to whom the data has been disclosed. This is particularly important in health where data is commonly shared for treatment purposes for example between hospitals and private specialists or GP's etc outside the hospital. As the electronic era increases the ease with which health data can be electronically shared, stored and cross linked with other data, it becomes even more important that corrections of data are forwarded on. The Bill needs to include such a principle for health records.

Disclosure Provisions

Whilst consumer access is hamstrung with exceptions to their own access, it is ironic that at the same time very broad provisions for disclosure to third parties are envisaged in NPP2.1. The Privacy Commissioner's Report on the Application of the National Principles for the Fair Handling of Personal Information to Personal Health Information (1999) notes that these provisions are broader than many health codes and, (in our view of particular concern) than the ACT Health Records (Privacy and Access) Act 1997.²⁰

We note that these provisions are in the face of the objections of the Department of Health and Aged Care.²¹ The Department's has expressed the view that these provisions are likely to undermine the willingness of some people, to seek timely and appropriate treatment. This could have a serious adverse impact on public health efforts. For example, if people at risk are not confident that their records are confidential and do not seek voluntary HIV/AIDS testing and Hepatitis C testing, the whole community is put at greater risk of infectious disease. The Bill ignores nonetheless the body of experience developed over the last two decades particularly, in relation to the importance of community trust that health records are maintained in strict confidence, to the success of public health strategies.

Further the Bill ignores the concerns expressed by many medical professionals, colleges such as the Royal College of Nursing, government health departments and consumer groups, that the common law imposes a significantly higher threshold for disclosure than that set out in the Bill. It is unrealistic to suggest that health professionals are entitled to defy the disclosure demands of law enforcement officers, either because the practitioners believe the common law sets out a higher threshold than this legislation²², or because they 'reasonably believe' that the use or disclosure is not 'reasonably necessary' in the terms of NPP 2.1(h). This approach relies on health professionals to have a highly sophisticated understanding of both the interaction of legislation and the common law and of

²⁰ Privacy Commissioner, Report on the Application of the National Principles for the Fair Handling of Personal Information to Personal Health Information (1999) p.30.

²¹ Privacy Commissioner, Report on the Application of the National Principles for the Fair Handling of Personal Information to Personal Health Information (1999) p.31&32.

²² As unfortunately the new Privacy Commissioner did in Privacy Commissioner, Report on the Application of the National Principles for the Fair Handling of Personal Information to Personal Health Information (1999) p.32.

what level of disclosure is reasonably necessary for law enforcement purposes. The breadth of disclosure provisions in NPP2.1 are clearly bad public policy from a number of perspectives.

The likelihood of misuse is reinforced by media reports which surface from time to time of police behaviour in relation to personal records. For example, despite the concerns expressed about the practice by a Parliamentary Select Committee, the Western Australian police department intended to continue a computerised warning system accessible to all police officers giving details of HIV positive persons in the community (including those merely suspected of having that status).²³ In another case police allegedly had held for more than nine months computerised medical records in identifiable form relating to approximately 1.2million people. The records were seized from a NSW pathology laboratory as part of a medifraud investigation.²⁴

Research

A particular concern is the complex and confusing interplay between NPP's 1, 2 and 10. It appears that despite the requirement in NPP 2.1 that an organisation may not use or disclose personal health information for secondary purposes unless they are directly related to the primary purpose of collection, clause 10 envisages just such usage. Indeed, it appears that though health information is specifically defined as particularly sensitive, NPP10.3 is expressly intended to allow personal information to be collected about people which is irrelevant to their health treatment and without their consent. The basic intention seems to be to provide a broad exception to allow collection, disclosure and use of health records for public health or safety research and other purposes such as funding, management or monitoring of a health service.

The provisos to this are vague assurances. For example, the private sector agency collecting the information must have determined that it is 'necessary' for either their research interests or those of a third party, or for funding or other purposes. If the collection is not mandated by law, they must comply with rules established by as yet unidentified 'competent health or medical bodies', that have issued confidentiality guidelines by which they are bound. NPP 10.4 appears to be an attempt to create some additional boundaries by requiring that before this non-treatment related information is disclosed to a third party, reasonable steps must be taken to permanently de-identify the data.

This really is an outrage. It is much broader than the s95 exemption for use/disclosure of health information by public sector bodies in the current Privacy Act! The current s95 exemption itself has been widely criticised. We would argue that the regime allowing disclosure of medical records for research purposes should at least involve enforceable guidelines issued and supervised by the Privacy Commissioner. As discussed above a precedent is the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines issued under s135AA National Health Act 1953 (Cth).

²³ Mark Irving, 'Police Keep HIV Data on Computers' The Australian, 3 July, 1990.

²⁴ Jo Chandler, 'Police holding confidential medical records' The Age, 16 May, 1990.

Further, it appears from the Privacy Commissioner's own report that the proposed use of personal health information for research purposes creates an anomaly.²⁵ Researchers won't have such a privileged position in relation to less sensitive data! We disagree with the suggested solution he foreshadows: amend the National Principles and s95 of the Privacy Act even further to reduce the protection afforded to other records as well!

Identifiers

NPP7 appears to restrict use and disclosure of identifiers. The catch is that if the use or disclosure falls within any of the paragraphs (e) to (h) under Principle 2.1, then NPP7 does not apply. It would appear that if this applies to health information it could allow health identifiers to be released for data matching exercises based on purposes as vague as the 'prevention' and 'detection' of non-criminal offences and improper conduct. Use of health identifiers for such exercises should be subject to much greater scrutiny and specifically subject to the discretion of the Privacy Commissioner to issue public interest determinations. It is noted that the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines include principles regulating the use of personal identification numbers²⁶ and it is again worth noting that breach of those Guidelines would appear to result in more serious sanctions than breach of the proposed Privacy Bill. The Privacy Commissioner has noted that this Principle will need to sit alongside any specific legislation addressing specific proposals for collection, use and disclosure of a unique identifier and for data matching.²⁷ Given the existing pilots and increasing interest in just such activities involving health data it is urgent that these issues are not left to the development of voluntary guidelines developed by the Privacy Commissioner and administered by industry bodies.

The issue of identifiers again raises the issue of whether the Bill is appropriate to the health sector when there are 'a myriad of initiatives' involving information technology to manage health data, 'currently underway or on the drawing board in every State and Territory, and across the public and private sectors'²⁸ In particular, we note the recent federal budget allocation of \$22million in the first year and \$16 million in the second for an opt-in electronic medication record to be shared by patients, doctors and pharmacists.

There is clearly also a pressing need for enforceable guidance to delimit the circumstances in which health information can be linked between unrelated or non-health related databases. For example, consumers subject to decisions made on the basis of automated data linkage must have a right of review before an adverse decision is implemented against them. Other necessary principles required in the health sector suggested by the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines include principles to ensure that long term retention of data in identifiable form is avoided including protocols to be followed where reidentification

²⁵ Privacy Commissioner, Report on the Application of the National Principles for the Fair Handling of Personal Information to Personal Health Information (1999) p.36

²⁶ Guideline 2.

²⁷ Privacy Commissioner, Report on the Application of the National Principles for the Fair Handling of Personal Information to Personal Health Information (1999) p.55.

²⁸ National Electronic Health Records Taskforce, 'A National Approach to Electronic Health Records for Australia' (March 2000), foreward.

of records is necessary. Similarly under 1996 Amendments to the Guidelines, data created by linking, comparing or combining records must be destroyed within three months of being generated. .

Conclusion

There are many other points which could be made in relation to this Bill as it relates to health. Some of them have been made in other submissions such as those by the Australian Consumers Association, the Consumers Health Forum and the Australian Privacy Charter Council. However, the general conclusion to be drawn is that at the least the Bill requires substantial revision, if we are to have any confidence that these proposals will generate positive outcomes for health consumers. At this point it would appear that the Bill does not provide the kind of high level benchmarks for consumer protection those of us who participated in the Privacy Commissioner's Health Consultation were looking for.

The emphasis is not on consumer protection and a nationally coherent scheme. Rather it is a confusing document which maintains the distinctions between public and private sector privacy protection and appears to offer numerous rationales for not providing health consumers with access, and for undermining their control over the collection, use and disclosure of their personal information by private sector agencies. It is recommended that the Bill should not apply to the health sector. Either health specific information privacy legislation should be developed or a separate legislative code for personal health information developed within a stronger overarching framework. Either model should build at a minimum on the protections offered by the ACT Health Records (Access and Privacy) Act and the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines.

Meredith Carter
Executive Director
Health Issues Centre
Level 11/300 Flinders St
MELBOURNE VIC 3000
Email hicgen@vicnet.net.au