NSW PARLIAMENTARY LIBRARY
RESEARCH SERVICE

Information Privacy and Health Records

by

Gareth Griffith

Briefing Paper No 6/2002

RELATED PUBLICATIONS

- Freedom of Information and Open Government by A Rath, NSW Parliamentary Library Background Paper No 3/2000

- Privacy Law Reform: Issues and Recent Developments by G Griffith, NSW Parliamentary Library Briefing Paper No 20/1998

ISSN 1325-5142
ISBN 0 7313 1711 4

April 2002

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

David Clune (MA, PhD, Dip Lib), Manager ..... (02) 9230 2484

Gareth Griffith (BSc (Econ) (Hons), LLB (Hons), PhD),
Senior Research Officer, Politics and Government / Law ..... (02) 9230 2356

Rachel Callinan (BA, LLB), Research Officer, Law ..... (02) 9230 2768

Rowena Johns (BA (Hons), LLB), Research Officer, Law ..... (02) 9230 2003

Roza Lozusic (BA, LLB), Research Officer, Law ..... (02) 9230 3085

Stewart Smith (BSc (Hons), MELGL), Research Officer, Environment ... (02) 9230 2798

John Wilkinson (BA (Hons), MA), Research Officer, Economics ..... (02) 9230 2006

Should Members or their staff require further information about this publication please contact the author.

Information about Research Publications can be found on the Internet at:

www.parliament.nsw.gov.au/WEB_FEED/PHWebContent.nsf/PHPages/LibraryPublications

CONTENTS

EXECUTIVE SUMMARY

The immediate background to this paper was the release in December 2001 of an Exposure Draft of a Health Records and Information Privacy Bill [**the Draft Health Records Bill**]. This was followed on 26 February 2002 by an announcement, in the Governor's Speech, foreshadowing the introduction of legislation to 'protect the privacy of electronic health records'. The issues involved in the proposed legislation are encapsulated in the three 'purposes' of the Draft Health Records Bill: (a) protecting the privacy of an individual's health information that is held in the public and private sectors; (b) enabling individuals to gain access to their health information; and (c) providing an accessible framework for the resolution of complaints regarding the handling of health information. The main findings of this paper are as follows:

- As in other privacy information areas, these issues belong to the larger picture of technological innovation which facilitates the sharing and accessing of data. In the specific context of health information, these developments include Telemedicine and health smart card proposals which may result in information being stored and collected in new ways (p 1).
- A particular concern is the development of a linked Electronic Health Record (EHR), as proposed in the March 2000 Report of the NSW Health Council titled, *A Better Health System for NSW*. Responding to this recommendation, the NSW Health Minister appointed an Advisory Committee to address privacy issues in relation to health information (p 1).
- The Advisory Committee's report titled, *Panacea or Placebo? Linked Electronic Health Records and Improvements in Health Outcomes*, was released on 2 February 2001. Among other things, it recommended that a 'system of linked electronic health records across the State' be developed and that the system be governed by a new Act, the Health Records and Information Privacy Act (p 8).
- Developments at the Commonwealth level include the establishment of a National Electronic Health Records Taskforce. In September 2001 it was reported that the Taskforce had recommended the development of a national health information network to be called Health*Connect*. The recommendation was endorsed by the Australian Health Ministers in July 2000 (pp 9-10).
- The Health Ministers have also established a Health Information Privacy Working Group under the Australian Health Ministers' Advisory Council (AHMAC). Its task is to develop a nationally integrated privacy framework for health information. Comprising Commonwealth, State and Territory representatives, the Working Group is said to be developing a draft National Health Privacy Code with the aim of delivering consistent privacy arrangements across the public and private sectors. The draft Code was due to be distributed for public consultation in January 2002 but, as at 10 April 2002, it is still to be released (p 10).
- A particular area of concern is genetic information privacy. An inquiry into genetic testing and information, to be conducted jointly by the Australian Law Reform Commission and the Australian Health Ethics Committee, was announced in August 2000. An Issues Paper, published in October 2001, posed the question, Should genetic information be treated as being so unique or more powerful than other forms of health information that it requires special legal protection or other exceptional measures?

Under the Draft Health Records Bill genetic information would be treated as a subset of health information (pp 3-5).

- At present, there is no single, comprehensive piece of health information privacy legislation in NSW applying to the private and public sectors. What exists, instead, is a plethora of relevant State and Federal laws. These include: (a) the Federal *Privacy Act 1998*, which now applies to both the Commonwealth public sector as well as to the private sector generally; (b) the NSW *Privacy and Personal Information Protection Act 1998*, which applies to NSW public sector agencies; (c) the NSW *Freedom of Information Act 1989* which also applies to State public sector agencies; (d) such health related regulations as the Private Hospitals Regulation 1996 which provides a patient's right of access to clinical records and for the secure retention of such records by private sector hospitals; (e) health related legislation which contain specific provisions on confidentiality; (f) statutes requiring mandatory reporting, such as section 27 of the *Children and Young Persons (Care and Protection) Act 1998* (NSW); (g) common law medical confidentiality requirements; (h) plus codes and guidelines, such as the NSW Department of Health's *Information Privacy Code of Practice* and the Federal Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector* (pp 13-15).
- The extension of the Federal privacy regime to cover the private sector was achieved by the *Privacy Amendment (Private Sector) Act 2000* (Cth), which commenced on 21 December 2001. In its June 2000 report, the House of Representatives Legal and Constitutional Affairs Committee commented that the Act's coverage of health information proved a particularly controversial issue. Of particular concern to the Committee were the exemptions applying to access to health records in the private sector (pp 18-19).
- In an anomalous position are NSW State owned corporations. These are not covered under the *Privacy and Personal Information Act 1998* (NSW) and would only be covered under the Federal scheme if expressly prescribed by regulation at the request of the State (p 21).
- The Federal Privacy Commissioner has indicated that the Federal privacy regime for the private sector is intended to 'cover the field'. Even if that is not the case, issues of constitutional consistency are raised by the operation of concurrent State and Federal legislation in this field (pp 19-20).
- The ACT and Victoria have already introduced comprehensive legislation dealing with health records and information privacy in the private and pubic spheres, along the lines proposed under the Draft Health Records Bill (p 1).
- It is said that the aim of the Draft Health Records Bill is 'to provide a single State-based scheme for the management of health privacy obligations, imposing the same set of Privacy Principles on information holders in both the public and private sector. The Bill will also provide a readily accessible complaints process and recognise the special issues which arise in the handling of health information'(p 31).
- Unlike the Federal privacy regime, the Draft Bill would extend privacy protection to the health information held on employees'records. This is one area where, it is understood, the Bill may be amended before it is introduced into Parliament (p 33 and p 46).
- There are sure to be differing perspectives on the Draft Health Records Bill. From one standpoint, it could be seen as yet another level of duplication and complexity in a field of law already busy with regulation. From another, it could be argued that it demonstrates the value of bringing public and private health sector privacy regulation under a single piece of legislation (p 45).

1. INTRODUCTION

The immediate background to this paper was the release in December 2001 of an Exposure Draft of a Health Records and Information Privacy Bill [**the Draft Health Records Bill**]. This was followed on 26 February 2002 by an announcement, in the Governor's Speech, foreshadowing the introduction of legislation to "protect the privacy of electronic health [1] The issues involved in the proposed legislation are encapsulated in the three "purposes" of the Draft Health Records Bill, as follows:

- protecting the privacy of an individual's health information that is held in the public and private sectors;
- enabling individuals to gain access to their health information; and
- providing an accessible framework for the resolution of complaints regarding the handling of health information.

As in other privacy information areas, these issues belong to the larger picture of technological innovation which facilitates the sharing and accessing of data. In the specific context of health information, these developments include Telemedicine and health smart card proposals which may result in information being stored and collected in new ways. A particular concern is the development of a linked Electronic Health Record (EHR),[2] as proposed in the March 2000 Report of the NSW Health Council titled, *A Better Health System for NSW*. Responding to this recommendation, the NSW Health Minister appointed an Advisory Committee chaired by the NSW Privacy Commissioner, Chris Puplick, to address privacy issues in relation to health information. The Advisory Committee's report titled, *Panacea or Placebo? Linked Electronic Health Records and Improvements in Health Outcomes*, was released on 2 February 2001. The subsequent release of the Draft Health Records Bill is the Government's response to that report.

These local developments must be placed in a broader Australian context. With the further extension of Commonwealth privacy law over the private sector, under the *Privacy Amendment (Private Sector) Act 2000* (Cth) which commenced on 21 December 2001, that regime now extends to all non-government health service providers. It is also the case that specific health records legislation, dealing with privacy and access matters, has been passed in the ACT[3] and Victoria.[4] The Draft Health Records Bill is similar in scope and intent to its Victorian counterpart. An obvious issue arising from this concerns the relationship

---

1 *NSWPD*, 26 February 2002, p 4.

2 An electronic health record is a 'single, complete patient record of all health care information which relates to an individual. It records all information about treatments that an individual has received – including hospital admissions – and diagnostic information such as test NSW Health Council, *A Better Health System for NSW*, March 2000, p 23.

3 *Health Records (Privacy and Access) Act 1997* (ACT).

4 *Health Records Act 2001* (Vic). Note that as at 5 March 2002 not all provisions of the Act have been proclaimed to commence. However, under section 2 (2) of the Act, all uncommented provisions will come into operation on 1 July 2002.

between any State-based scheme and the federal privacy regime. Questions of overlap and complexity must also be addressed in this context.

This paper begins with a review of the key issues and developments. This is followed by an overview of the present legal position in NSW. Next, the Federal privacy legislation is discussed. The paper then presents a commentary on the draft Health Records and Information Privacy Bill 2001 **[the Draft Health Records Bill]**.

Note that the paper uses the terms 'medical records' and 'health records' interchangeably.

2. ISSUES IN THE DEBATE

2.1 Definitional issues –

Privacy and health: Privacy relates to a bundle or collection of rights which all stem from the idea that, subject to certain legitimate qualifications, in a liberal democracy the individual has a right 'to be let alone'.[5] In more specific terms, the Australian Privacy Charter stated:

> People have a right to privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person), and freedom from surveillance.[6]

Discussion of privacy in a health context usually concentrates on two of the above categories: first, the privacy of the body; and, secondly, information privacy. The physical privacy of the person typically requires a person's consent for the carrying out of a medical procedure which in any way invades the person's physical integrity. In a similar vein, information privacy can be said to require the authorised use and storage of a person's medical records to be made subject to the requirement of the patient's individual consent.

Personal information privacy: Personal information privacy is a subset of privacy. It 'involves the right of individuals to determine when, how and to what extent they will share personal information about themselves with others'.[7] It is said in this regard that 'information privacy' involves the notion that people, at least to some extent, should be able to regulate the way information about themselves is gathered, stored and used.[8] The underlying question in this context therefore is whether business and government operate in a way that protects the privacy of the personal information they collect and use. Medical and police

---

5 LD Brandeis and SD Warren, 'The right to privacy' (1890) 4 *Harvard Law Review* 193 at 195.

6 'The Australian Privacy Charter' (1995) 2 *Privacy Law and Policy Reporter* 44.

7 Canadian Task Force on Electronic Commerce, *The Protection of Personal Information: Building Canada's Information Economy and Society*, January 1998, p 28 - http://canada.justice.gc.ca

8 Legislative Assembly of Queensland, Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland, Report No 9*, April 1998, p 9.

reports, employment and criminal records, information concerning political or religious affiliations and refused licence applications are all instances of the kind of personal information which data protection laws and principles have sought to protect.

The guiding philosophy behind these laws is that personal information is of such a character that an individual may reasonably expect to control its disclosure.[9] For most people, such an expectation would apply in respect to information about their health.

Health information privacy: Health information is a subset of personal information, one that is usually thought to involve information of a particularly 'sensitive' kind. As Chief Justice Gleeson acknowledged recently, the line between what is 'private' and 'public' can be hard to draw, but he went on to say that 'Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private.'[10] That is not to say that all health information is equally sensitive. As the New Zealand Law Commission has observed, 'An individual may have no wish to conceal the fact that he or she has a broken rib, but may not wish to disclose that he or she is HIV positive.'[11] It is a fact that health information about individuals is collected by many organisations and practitioners and that the information collected varies in nature, from details of minor injuries, to what may be highly sensitive information on social and lifestyle factors about an individual.

A major issue in the health privacy debate is whether, as a result of its particular sensitivity, health information is one privacy area which requires its own legislative scheme. That is what is proposed under the Draft Health Records Bill for NSW. It is already in place in Victoria and the ACT. Federally, on the other hand, the protection of health information is subsumed under the general privacy regime. In fact the Commonwealth Privacy Act identifies health information as one form of 'sensitive information' attracting higher privacy standards for the purposes of the application of the National Privacy Principles to the private sector.

Genetic information privacy:[12] Considerable discussion has also centered on the appropriate legislative protection for genetic information. On 11 March 1998 the then Deputy Leader of the Australian Democrats, Senator Stott Despoja, introduced the Genetic

---

9 New Zealand Law Commission, *Preliminary Paper 49 – Protecting Personal Information from Disclosure: A Discussion Paper*, February 2002, p 19. It is noted that the expectation rule 'is one that leaves little room for conclusive generalisation'.

10 *ABC v Lenah Game Meats* (2001) 185 ALR 1 at 13 (para 42) He went on to observe that 'The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private'.

11 New Zealand Law Commission, n 9, p 19.

12 It was said in the Governor's Speech that the Government will introduce legislation in this parliamentary session to include NSW 'in a national scheme for regulating gene technology' *NSWPD*, 26 February 2002, p 4.

Privacy and Non-Discrimination Bill 1998 into the Senate. The main purposes of the Bill were to: (a) establish an enforceable right to privacy of genetic information; (b) prevent the collection of a DNA sample for genetic analysis without the authorisation of the individual concerned; and (c) make discrimination based on genetic information unlawful. The Bill was subsequently referred to the Senate Legal and Constitutional Legislation Committee. The Committee reported in March 1999 recommending that the Bill not proceed pending further examination.

In its report the Committee presented a detailed analysis of the implications of the emerging genetic technology for both health care and medical research. A specific privacy issue discussed in relation to health care concerned 'information contained in a collection of tissue samples originally collected for some other purpose, when later access is sought to the collection for the purpose of genetic testing'. Several submissions had drawn the Committee's attention to the longstanding practice of taking blood samples from all newborn babies as part of newborn screening programs:

> The samples, known as 'Guthrie spots' are stored on cards, and all babies born in Australia are tested by the programs which means that, in NSW for example, cards are now in storage for persons up to the age of 28 years. These large collections have become inadvertent DNA sample banks, and these submissions pointed to the need for appropriate controls over access to and use of the samples.[13]

Specific privacy issues relating to medical research were also considered, including the potential for research to reveal previously unknown information that an individual or family did not want, or intend to become known, such as the existence or absence of a genetic relationship. A further privacy consideration, according to the Committee, stems from the use of 'record linkage' as a research tool: 'Record linkage involves the combination of data from disparate data sources (often collected for other purposes) by matching on individual identifiers, to produce a new data set that contains more accurate details about each individual.'[14]

An inquiry into genetic testing and information, to be conducted jointly by the Australian Law Reform Commission and the Australian Health Ethics Committee, was first announced in August 2000.[15] An Issues Paper, published in October 2001, posed the question, 'Should genetic information be treated as being so unique or more powerful than other forms of health information that it requires special legal protection or other exceptional measures?' The paper commented in this respect:

---

13 Senate Legal and Constitutional Legislation Committee, *Provisions of the Genetic Privacy and Non-Discrimination Bill 1998 (as introduced in the 38th Parliament)*, March 1999, p 11.

14 Senate Legal and Constitutional Legislation Committee, n 13, p 14.

15 The inquiry's terms of reference were settled in February 2001.

> Genetic information is most often collected from clinical genetic testing for the purposes of providing medical and other health services to the individual being tested or to a genetic relative. Therefore for many purposes, genetic information may be considered a subset of health information. Nevertheless, genetic information has a range of characteristics that may be seen as differentiating it from most other health information.[16]

Obviously the subject raises complex issues of a practical and ethical kind. In Victoria, at least, it is clear that 'genetic information' is to be treated, for privacy purposes, as a subset of 'health information'. Thus, under the Victorian *Health Records Act 2001* the definition of 'health information' expressly includes 'genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or any of his or her descendants'.[17] In the Second Reading speech for the legislation the Victorian Minister for Health said that:

> While new technology brings many benefits for individuals and the community as a whole, the potential exists for technology to be misused, and for people to suffer discrimination or other kinds of harm as a result. Nowhere is this more evident than in the case of health information, particularly in light of the increase in the use of genetic tests to predict the likelihood of future illness.[18]

The same approach has been adopted under the Draft Health Records Bill.[19] The difference in detail is that, whereas the Victorian legislation refers only to 'descendants' in this context, the NSW Draft Bill throws a wider net over the genetic information it seeks to protect by referring to 'any *sibling, relative* or descendant of the individual'. In other words, protection is extended to an individual's present, as well as future, family members.[20]

2.2 E-health issues

Electronic information systems and health privacy: The challenges facing individual privacy in the health sector at present arise from many quarters, including the structural changes in the delivery of health services. On this last point the Federal Privacy

16 ALRC, *Protection of Human Genetic Information, Issues Paper 26*, October 2001, p 126.

17 *Health Records Act 2001* (Vic), section 3.

18 *VPD* (Legislative Assembly), 23 November 2000, p 1906.

19 Draft Health Records and Information Privacy Bill (NSW), clause 6 (d).

20 Note that reference is currently made to personal information relating to 'genetic characteristics' under section 4 (2) of the *Privacy and Personal Information Protection Act 1998*. Further to the Draft Health Records Bill, such information would be excluded from the NSW privacy legislation, at least to the extent that it would be included under the definition of 'health information' in the Draft Bill. In other words, genetic information would be part of the distinct legislative schema in place for health information.

Commissioner has commented that, 'as a consequence of the increasing complexity of health care there is a move away from single medical practitioners towards larger teams of health care professionals who may all legitimately have access to patient's medical records.'[21] The Federal Privacy Commissioner has also commented on the fact that many people other than doctors hold health information, including gymnasiums, alternative therapists, allied health professionals, superannuation providers and insurance companies: Some bodies that are now collecting personal health information are not bound by professional codes of ethics or common law duties of confidentiality.'[22]

Emphasis in the recent debate has rightly focussed on the developments in electronic communications and technological advances. Particular attention has focused on the issues raised by the development of systems able to electronically link and integrate personal health records. The hope is that such developments will promote more comprehensive, coordinated and safer health care for individuals and promote better monitoring and planning for the community. The countervailing concern is that, along with the potential for improved health care, such developments also carry significant privacy risks. It is recognised that health records can involve personal information which is both highly sensitive and wide-ranging in nature and that, with the shift away from a paper-based world, minor security breaches can lead to an invasion of privacy affecting any number of individuals at the same time.[23] According to Meredith Carter, Executive Director of the Health Issues Centre:

> The breadth of information contained in many health records can provide a much more detailed picture of the individuals concerned than may be commonly realised. Indeed, once compiled as an integrated, longitudinal record, these records are likely to be of interest to many other parties, quite outside those who might be considered to have legitimate public health interests.[24]

Fundamental to the dilemma is the ability of electronic information systems to deliver to third parties information that can be traced back to an identifiable individual and afterwards used by the third party for commercial or other benefit. Carter referred in this context the findings of the 1992 ICAC report, *Unauthorised Release of Government Information*. That investigation, while not dealing specifically with health information, disclosed 'a massive illicit trade in government information.'[25] The third parties interested in such information, Carter explained, 'range from health care providers to agencies such as pharmaceutical

---

21 Senate Legal and Constitutional Legislation Committee, n 13, p 10.

22 M Crompton, Federal Privacy Commissioner, 'Privacy, technology and the healthcare sector', *Paper presented at the Australian Financial Review 4th Annual Health Congress*, Sydney 25-28 February 2002.

23 M Carter, 'Protecting consumers' interests in their health records' (July/August 1999) 6 *Privacy Law and Policy Reporter* 13.

24 M Carter, n 23, p 13.

25 ICAC, *Unauthorised Release of Government Information, Volume 1*. August 1992, p 3.

companies and agencies that have no health care role at all, such as employers, banks and superannuation companies.'[26]

An important distinction as regards health information is between demands for access to data for primary purposes, notably the provision of health care to the individual, and demands for secondary uses, including research and public health monitoring. As the then Federal Privacy Commissioner, Kevin O'Connor, observed in 1996 'The use of identified information for purposes other than the direct health care is a major area of growth and requires careful management to ensure that the privacy of health information is not eroded.'[27] Developments in e-health can only intensify the concerns which underlie this statement.

Confirming this view of things, in a recent review of health research, privacy and data linkage issues, Roger Magnusson commented:

> As medical records move 'on-line' and the centralisation and coordination of health data becomes possible, the demands for third party access, the potential benefits of providing such access, as well as the privacy risks for individual patients, will all increase.[28]

E-health developments in NSW: Over the past few years the focus of the health privacy debate in NSW has been on the development of electronic medical records. As noted, development of a linked Electronic Health Record (EHR) was proposed in the March 2000 Report of the NSW Health Council titled, *A Better Health System for NSW*. An EHR is a complete patient record of all health care information relating to an individual, including hospital admissions and diagnostic information such as tests results. As the Health Council recognised, to be effective the development of such a computerised recording system would require the use of what are called Unique Patient Identifiers (UPIs). These have, in fact, already been developed in at least four Area Health Services in NSW, the difficulty being that different Areas have set up different systems. As stated in the Draft Health Records Bill, an identifier is usually (but need not be) a number; it must, however, consist of more than a person's name.[29] The advantage of a UPI is that it would allow health service providers to identify with certainty the particular patient they are dealing with, irrespective of where and when the patient entered the health system.[30] The Health Council outlined an implementation process based around demonstration projects to be established in at least two Area Health

---

26 M Carter, n 23, p 13.

27 Senate Community Affairs References Committee, *Report on Access to Medical Records*, June 1997, p 62. Reference was made to 'numerous public health pressures to use personal health information', including the use by medical and epidemiological researchers, and in such public health initiatives as screening programs and registers of immunisation.

28 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *The Sydney Law Review* 5 at 9. Magnusson presents a comprehensive account of the legal framework and the

29 Draft Health Records and Information Privacy Bill (NSW), clause 4.

30 NSW Health Council, n 2, p xvii.

Services. It also recommended that the introduction of the EHR must be on a voluntary basis, following on from proper evaluation and negotiation of relevant privacy issues.[31]

Updating developments in this area, in December 2000 the NSW Ministerial Advisory Committee on Privacy and Health Information noted that a Government Action Plan for health had been developed, which included plans for the roll-out of an EHR and UPI. At that stage, the following reflected the status of the EHR proposal:

- NSW Health had proposed to implement a State-wide UPI by November 2002. This would be preceded by Area UPIs by June 2002.[32] This approach would support any initiatives taken at the national level to implement a national unique identifier.[33]
- The UPI was recognised to be an essential precursor to the EHR. A detailed strategy for the introduction of UPIs, produced in November 2000 by the NSW Health Information Management Implementation Co-ordination Group (IMICG), recommended that their introduction should await the outcomes of the work of the Ministerial Advisory Committee.

In the same report, which was released in February 2001, the Ministerial Advisory Committee recommended that a ‘system of linked electronic health records across the State’ be developed and that the system be governed by a new Act, the Health Records and Information Privacy Act. The introduction of a system of UPIs was also recommended, to be generated by either the Department of Health itself, or in a coordinated fashion by the Area Health Services. It was further recommended that the Medicare number not be used for this purpose and the State-wide UPI should not be linked directly to the Medicare number.[34]

National developments: E-health initiatives have implications for all levels of Australian government. At the Commonwealth level, various responses have been made to the

---

31 NSW Health Council, n 2, p 27 and p 89. The possibility of introducing a Health Smart Card was also discussed in the report. This has not been taken up by the Government.

32 Ministerial Advisory Committee on Privacy and Health Information, *Panacea or Placebo? Linked Electronic Health Records and Improvements in Health Outcomes*, December 2000, p 28. In a later section the report noted that, whereas the Commonwealth Department of Health and Aged Care was said to support a national UPI strictly limited to use in the health sector, NSW Health has proposed a multi-layer system based on individual Area Health Service UPIs, which could then be matched against a State UPI.

33 The Health Council report had recognised that the development of electronic health records would raise questions of a cross-jurisdictional kind, noting the absence at present of ‘mandated requirements or strategies to link patient identification systems between the Commonwealth- and State-funded services’ - NSW Health Council, n 2, p 25.

34 Ministerial Advisory Committee on Privacy and Health Information, n 32, p 30. It was said that when the Medicare number was introduced assurances were made that these records would not be linked with health data relating to individuals. Thus, ‘Any extension of the Medicare number that involves linkage to individual health data would constitute a breach of trust with the Australian people’. The report also noted that the Medicare number on a card may cover a number of different people. On the other hand, the Health Insurance Commission has a separate and distinct UPI for each individual covered under that card (page 29).

challenges posed by such issues. One response, already in operation, is Medicine*Connect*, which involves the establishment of a database that records prescriptions written for individual patients by different prescribers and dispensed by different pharmacists. Under the *National Health Amendment (Improved Monitoring of Entitlements to Pharmaceutical Benefits) Act 2000*, a scheme has been introduced[35] which requires all prescriptions to be linked with a Medicare number. As explained in the Second Reading speech:

> Doctors will be authorised, but not required, to put the Medicare number on prescriptions and store the number with patient consent. Pharmacists will also be authorised to request and to store a patient's Medicare number and its expiry date on the system, again with patient consent.[36]

A second response has been the establishment of a National Electronic Health Records Taskforce. This followed a recommendation of the National Health Information Management Advisory Council (NHIMAC) in its November 1999 report, *Health Online – A Health Information Action Plan for Australia*.[37] In a second edition of the report, released in September 2001, it was noted that the Taskforce had recommended the development of a national health information network for Australia, to be called Health*Connect*. In the form proposed by the Taskforce, such a network would allow personal health information to be collected, stored and exchanged, but only with the permission of the individual health consumer. Under Health*Connect*, health related information about an individual would be collected in a standard, electronic format at the point of care (such as at a hospital or a general practitioner's clinic). This information would take the form of 'event summaries'- not all the notes that a health care provider may choose to keep about a consultation.

The Taskforce's Health*Connect* recommendation was endorsed by Australian Health Ministers in July 2000 when there was unanimous support for: (a) adopting a national approach to electronic health records in Australia; (b) the secure networking of health information more generally; and (c) subject to budget constraints, jointly establishing a health information network for Australia, Health*Connect*, as the best way to achieve these aims. At a subsequent meeting in November 2000, the Health Ministers agreed to undertake two years of development work to test the Health*Connect* concept and also to undertake additional work on developing the necessary infrastructure. The Health*Connect* Program Office was established for this purpose, based in the Commonwealth Department of Health and Aged Care, but involving State and Territory government representatives.[38]

---

35 It commenced in July 2001.

36 *Commonwealth Parliamentary Debates* (House of Representatives), 6 September 2000, p 20197.

37 NHIMAC was established by Australian Health Ministers in April 1999 as the peak body for dealing with information issues in the health sector. It represents Commonwealth and State and Territory governments, clinical practice, the information technology industry, the private health sector and consumer interests. The Federal Privacy Commissioner is also a member.

38 NHIMAC, *Health Online: A Health Information Action Plan for Australia*, 2nd edition, September 2001, pp 81-83.

Concerns have been expressed about the balance of compulsory and voluntary elements in the proposed Commonwealth scheme. For example, in a discussion paper released in November 2000 the NSW Ministerial Advisory Committee on Privacy and Health Information commented that Health*Connect* has been described as a scheme based on voluntary individual participation, on one side, but that on the other it would be based on assigning a Unique Personal Identifier to every newborn. The Advisory Committee went on to say:

> It appears that what is emerging at the Commonwealth level is a combination of a ‘compulsory’ and ‘voluntary’ model. That is, it is compulsory for every person to be registered, but voluntary what information is included on the electronic network. However, the true extent to which the proposal is voluntary or compulsory remains unclear.[39]

The privacy implications of such e-health initiatives as Health*Connect* have of course been recognised at the national level, with the further establishment by the Health Ministers of a Health Information Privacy Working Group under the Australian Health Ministers’ Advisory Council (AHMAC). Its task is to develop a nationally integrated privacy framework for health information. Comprising Commonwealth, State and Territory representatives, the Working Group is said to be developing a draft National Health Privacy Code with the aim of delivering consistent privacy arrangements across the public and private sectors. The draft Code was due to be distributed for public consultation in January 2002 but, as at 10 April 2002, it is still to be released.[40]

2.3 Legal issues

No common law right of access to health records: The leading case is *Breen v Williams*[41] in which the High Court dismissed the claim that patients have a right of access at common law to the health records complied about them by their doctors. The plaintiff, Ms Breen, had variously contended that the nature of her right to access resided in:

- a patient’s right or interest in the information contained in the medical records;
- an implied term of the contract between doctor and patient;
- a fiduciary relationship between doctor and patient.

All these claims were unanimously rejected. In effect, *Breen v Williams* confirmed that the view that, at common law, a private medical practitioner in general or specialist practice

---

39 NSW Ministerial Advisory Committee on Privacy and Health Information, *Privacy and Health Information – A Discussion of Issues*, November 2000, p 10; NSW Ministerial Advisory Committee on Privacy and Health Information, n 32, p 30.

40 NHIMAC, n 38, p 28.

41 (1995-1996) 186 CLR 71.

'owns' and therefore controls access to the medical records relating to his/her patients. Owning a medical record in private medical practice confers power and ultimate control over access to information held in a record.[42]

In their joint judgment Gaudron and McHugh JJ concluded it was not possible, 'without distorting the basis of accepted legal principles, for this Court to create an unrestricted right of access to medical records, or a right of access, subject to exceptions. If change is to be made, it must be made by the legislature.'[43]

As explained in the next section of this paper various legislative initiatives have taken place in NSW to secure patient access to their medical records. The Draft Health Records Bill is in fact the latest and most comprehensive of these initiatives. The point is also made that access has often been granted in the recent past because it is regarded as good professional practice. It was said in 1996, for example, that the Royal Australian College of General Practitioners had adopted a policy that 'patients should be permitted to have access to their medical record upon request *except* where access is likely to cause serious harm or distress...'[44]

No common law tort of breach of privacy: Just as the common law does not recognise a right of access to medical records, nor it seems does it recognise a right to privacy. That is not to say that the Australian common law contains no protection at all of the right of privacy: in special situations, as in the relationship between a doctor and a patient, where a duty of confidentiality exists between two parties, then disclosure of information to a third party may be a breach of confidence. However, the general point to make is that, unlike in the USA for example, Australian law recognises no over-arching general concept of privacy as an interest worth protecting for its own sake.[45] The leading Australian case is *Victorian Park Racing and Recreation Grounds Co Ltd v Taylor*[46] which is generally accepted as authority for the proposition that a cause of action for breach of privacy does not exist at common law.[47]

That proposition was reconsidered by the High Court recently in *ABC v Lenah Game Meats Pty Ltd*.[48] While it was not actually necessary for the Court to decide whether a tort of

---

42 Senate Community Affairs References Committee, *Report on Access to Medical Records*, June 1997, p 28.

43 (1995-1996) 186 CLR 71 at 115.

44 RACGP, *Interim Code of Practice for Computerised Medical Records in General Practice*, February 1996, section 5 – quoted in A Cornwall, 'Whose medical records?' (August 1996) 5 *Australian Health Law Bulletin* 1 at 2.

45 G Taylor, 'Why is there no common law right of privacy?' (2000) 26 *Monash University Law Review* 235 at 238.

46 (1937) 58 CLR 479.

47 For a commentary on recent developments see – R Martin and J Macdonnell, 'Privacy after Lenah Game Meats' (2001) 5 *TeleMedia* 106.

48 (2002) 185 ALR 1.

privacy is recognised at common law, in various comments it was suggested that such a development was not out of the question. Chief Justice Gleeson said 'The law should be more astute than in the past to identify and protect interests of a kind which fall within the concept of privacy'.[49] In qualifying remarks he observed, first, that the 'lack of precision of the concept of privacy is a reason for caution in declaring a new tort' and, secondly, that complications arise from 'the tension that exists between interests in privacy and interests in [50] Gummow and Hayne JJ, with whom Gaudron J agreed, stated that the *Victoria Park Racing* case did 'not stand in the path of the development' of a tort of privacy.[51] Whereas Callinan J, expressing 'tentative views' on the tort of privacy, said:

> It seems to me, having regard to current conditions in this country, and developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made.[52]

As to the question of a statutory tort of privacy invasion, Gummow and Hayne JJ observed that 'The Privacy Act 1988 (Cth), particularly since its amendment by the Privacy Amendment (Private Sector) Act 2000 (Cth), confers some enforcement power upon the Federal Court and the Federal Magistrates Court, but the legislation stops short of enacting what might be called a statutory tort of privacy invasion'.[53] That situation is unlikely to change in the foreseeable future. More likely is the recognition of a common law tort which would operate in addition to existing and proposed legislative remedies.

3. OVERVIEW OF THE EXISTING LEGAL FRAMEWORK

Before discussing various legislative initiatives in more detail brief note can be made of the range of privacy related laws which apply at present to health information. The point is made in this respect that there is 'no single, comprehensive piece of privacy legislation in NSW applying to the private and public sectors'.[54] What exists, instead, is a plethora of relevant laws at State and Federal level. These include:

---

49 (2002) 185 ALR 1 at 12 (para 40).

50 (2002) 185 ALR 1 at 13 (para 41).

51 (2002) 185 ALR 1 at 31 (para 107).

52 (2002) 185 ALR 1 at 95 (para 335). Callinan J was also of the view that, if such a tort is recognised, it may apply to corporations (at para 328). However, the balance of opinion was that such a tort is unlikely to extend to corporations (Gummow and Haynes JJ at para 132; Kirby J at 190).

53 (2002) 185 ALR 1 at 31 (para 106); *Privacy Act 1988* (Cth), section 55A.

54 NSW Ministerial Advisory Committee on Privacy and Health Information, n 39, p 20.

3.1 The Federal Privacy Act 1988

Since the commencement of the *Privacy Amendment (Private Sector) Act 2000,* the Federal *Privacy Act 1988* applies to both the Commonwealth public sector and (with certain exceptions) to the private sector generally. The Act is discussed in more detail in the next section of this paper.

3.2 The NSW Privacy and Personal Information Protection Act 1998

This applies to State public sector agencies.[55] In the relevant Second Reading speech it was said that the introduction of data protection laws for the private sector 'should be done in a uniform manner on a national basis.'[56]

Structurally, the Act is similar to other legislative privacy models. Part 2 is headed Information protection principles'(IPPs) and it sets out 12 principles of the kind found in most privacy legislation, including the Federal and New Zealand Privacy Acts, all of which are based on the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The Act makes provision for specific exemptions from these IPPs, for law enforcement and other agencies. These IPPs apply to 'personal information' a term defined to mean 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.' Personal information is said to include such things as 'an individual's fingerprints, retina prints, body samples or genetic characteristics.'

Part 3 then provides for the making of privacy codes and management plans, which can allow an exemption from, or modification to, any of the IPPS in the Act. Codes must be first submitted for consultation to the NSW Privacy Commissioner and be approved by the Minister. The NSW Health Department has made a Code under the Act, modifying the way a number of the IPPs apply to its public sector health activities. Agencies are also required to prepare a Privacy Management Plan outlining how they plan to comply with the requirements of the Act. The NSW Health Privacy Management Plan was issued as Circular 2000/62 on 26 July 2000.

---

55 State owned corporations, such as State Rail, are not covered under the *Privacy and Personal Information Act 1998* (NSW) and would only be covered under the Federal scheme if expressly prescribed by regulation at the request of the State. This is discussed in a later section of this paper.

56 *NSWPD*, 17 September 1998, p 7601. State owned corporations are not covered. However, there is provision in the Act for people to complain to the NSW Privacy Commissioner about alleged breaches of privacy by private sector organisations and individuals. For a more detailed outline of the Act see – G Griffith, *Privacy Law Reform: Issues and Developments*, NSW Parliamentary Library Research Service Briefing Paper No 20/1998. For contrasting comments on its operation upon commencement see – N Waters, 'Was it worth it?' (March 2000) 6 *Privacy Law and Policy Reporter*141; C Puplick, 'Codes and consultation in NSW' (August 2000) 7 *Privacy Law and Policy Reporter* 53.

Part 4 establishes the office of the NSW Privacy Commissioner and sets out the complaints mechanism. Enforcement provisions are then established under Part 5. In brief, individuals have the right to seek a review by an agency where the individual believes their privacy has been breached. The main responsibility for the review lies with the agency, although if requested by the agency the Privacy Commissioner can undertake a review on its behalf. Where an individual is not satisfied with the outcome of an internal review, they can appeal to the Administrative Decisions Tribunal.

3.3 The NSW Freedom of Information Act 1989

This, too, applies to State public sector agencies, with section 16 providing that 'A person has a legally enforceable right to be given access to an agency's documents in accordance [57] This is qualified by section 31 (4) which provides that, in relation to medical or psychiatric records concerning the applicant and where, in the agency's opinion, disclosure may have an adverse effect on the applicant's physical or mental health, then it is enough for the agency to give access to a registered medical practitioner nominated by the applicant.

The issue of the overlap between the State privacy and FOI regimes is discussed in a later section of this paper.

3.4 Health-related regulations

Several health related regulations are in operation covering records held in private hospitals, day procedure centres and nursing homes[58] For example, clause 42 of the *Private Hospitals Regulation 1996* provides for a 'patient's right of access to clinical records'. Exemption is made where 'the medical practitioner or dentist in charge of the patient's care advises that the request should be refused' and if the private hospital is satisfied that the access sought would be 'prejudicial to the patient's physical or mental health'. Clause 41 requires the retention of clinical records for 7 years (in the case of adults) and 25 years (in the case of children). This provision is mirrored in proposed section 24 of the Draft Health Records Bill.

3.5 Health-related legislation

Several health related statutes contain specific provisions on confidentiality, including section 22 of the *Health Administration Act 1982* which is binding on all persons working in the NSW health system.[59] More specifically, section 17 of the *Public Health Act 1991* (NSW) makes special provision for the confidentiality of HIV/AIDS related information'.

3.6 Mandatory reporting requirements

---

57 Section 5 of the *Privacy and Personal Information Protection Act 1998* (NSW) defines the relationship between itself and the FOI Act by stating the latter is not affected by the former.

58 *Private Hospital Regulation 1996* (NSW); *Nursing Homes Regulation 1996* (NSW); *Day Procedure Centres Regulation 1996* (NSW).

59 Similar confidentiality provisions are found in the *Mental Health Act 1990* (NSW) (section 289) and the *Public Health Act 1991* (NSW) (section 75).

Also relevant to the debate about privacy and health information are various laws requiring the mandatory reporting of information by medical practitioners, including public health and child protection legislation. An example is the mandatory reporting requirement under section 27 of the *Children and Young Persons (Care and Protection) Act 1998* (NSW) for paid providers of health care where there are reasonable grounds to suspect that a child is at risk of harm. Conversely, under section 36 of the *Public Health Act 1991* (NSW) a person to whom a public health order applies has the right to inspect, and make copies of, their medical records.

3.7 Common law medical confidentiality obligations

Relevant non-statutory requirements include common law medical confidentiality obligations applying to the practitioner-patient relationship.

3.8 Codes and guidelines

Alongside and in addition to this multi-layered legal framework various codes and guidelines also operate in this area, many produced by governmental bodies, some by professional organisations. Most important at the State governmental level is the NSW Health Department's *Information Privacy Code of Practice*, introduced originally in May 1996 and, as noted, updated in a second edition in December 1998 in conformity with Part 5 of the *Privacy and Personal Information Protection Act 1998*.

Of national significance are the Federal Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector*, issued in November 2001.[60] Further, with the approval of the Federal Privacy Commissioner, guidelines for the protection of privacy in the conduct of medical research have been issued by the National Health and Medical Research Council (NHMRC) under section 95 (public sector)[61] and section 95A (private sector) of the *Privacy Act 1988* (Cth).[62]

4. THE FEDERAL PRIVACY ACT 1988 AND HEALTH INFORMATION

As noted, since the commencement of the *Privacy Amendment (Private Sector) Act 2000*, applies to both the Commonwealth public sector and (with certain exceptions) to the private sector generally. The Federal private sector privacy regime is designed to protect 'personal information'. Some personal information is defined to be 'sensitive information' which attracts higher privacy standards. Under this scheme, 'health information' is a sub-set of sensitive personal information.

The privacy regimes for the public and private sectors operate separately under the Act, a distinction which is reflected in the following discussion.

---

60 These and other guidelines are not legally binding.

61 First issued in July 1991, these guidelines have been revised regularly since then. In their current form the guidelines were issued in February 2000.

62 The first guidelines were issued in December 2001.

4.1 The public sector

Prior to the enactment of the *Privacy Amendment (Private Sector) Act 2000* (Cth), which commenced on 21 December 2001, the federal privacy regime was largely confined to the public sector. In effect, it protected personal information held by the federal public sector and tax file numbers wherever held; it also regulated the collection, use and disclosure of consumer credit information by private sector organisations.

The Privacy Act was passed in 1988 against a background of the failure of the Australia Card legislation. It was enacted pursuant to the external affairs power and implements Australia's obligations under Article 17 of the *International Covenant on Civil and Political Rights* and the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The concept of 'privacy' itself is not defined under the Act. Instead, it establishes Information Privacy Principles (IPPs) which apply to 'agencies', a term defined to cover persons and bodies in the federal public sector. The IPPs are based largely on the OECD Guidelines.[63] There are 11 in total, as follows:

- Manner and purpose of collection of personal information (IPP1)
- Solicitation of personal information from individual concerned (IPP2)
- Solicitation of personal information generally (IPP3)
- Storage and security of personal information (IPP4)
- Information relating to records kept by record-keeper (IPP 5)
- Access to records containing personal information (IPP6)
- Alteration of records containing personal information (IPP7)
- Record-keeper to check accuracy etc of personal information before use (IPP8)
- Personal information to be used only for relevant purposes (IPP9)
- Limits on use of personal information (IPP10)
- Limits on disclosure of personal information (IPP11)

A mechanism is established to deal with cases where a waiver from strict compliance with the IPPs is desirable in the public interest. These are referred to as 'public interest determinations'. These operate where the Federal Privacy Commissioner is satisfied that 'an act or practice of an agency breaches, or may breach, an Information Privacy Principle'.[64] The Commissioner also has power conduct privacy audits,[65] to make enforceable determinations as to liability under the Act in the event of a breach, as well as to award damages.[66]

---

63 Privacy principles for consumer credit reporting are set out in Part IIIA of the *Privacy Act 1988* (Cth). There is, in addition, a Credit Reporting Code of Conduct.

64 *Privacy Act 1988* (Cth), section 72.

65 *Privacy Act 1988* (Cth), section 27 (1)(h) and section 28 (1)(e).

66 *Privacy Act 1988* (Cth), section 52.

Although no specific mention is made of health information, the public sector provisions cover the collection, use and disclosure of health records for research or other purposes by all Commonwealth government agencies. Regulated in this way is the handling of health related data held by agencies such as the Department of Health and Aged Care and the Health Insurance Commission.[67] IPP1, for example, ensures that the collection of personal information is subject to the requirements that, first, the information is collected for a 'lawful purpose directly related to a function or activity of the collector' and, secondly, the collection is 'necessary for or directly related to that purpose'. Access to records is also covered under IPP6 which, first, grants an individual a broad right of access to a record containing their personal information and, secondly, makes this right subject to any exceptions operating under a Commonwealth law by which access is restricted. As noted, section 95 makes provision for the issuing of public sector medical research guidelines by the National Health and Medical Research Council, with the approval of the Privacy Commissioner.

4.2 The private sector

Background: Passage of the *Privacy Amendment (Private Sector) Act 2000* (Cth) was the result of a lengthy debate which took place at the State, national and global levels. Globally, the most significant development in recent times was the European Union Directive on data protection which came into force in October 1998. It establishes comprehensive protection of personal information held in any form by the public and private sectors. The EU Directive has become the international benchmark for privacy protection, not least because countries without what the Directive describes as an 'adequate' level of data protection will be excluded from personal information flows. Exactly how rigorously the EU applies the 'adequacy' test to Australia remains to be seen. It has been argued by Professor Graham Greenleaf that, in accepting the US Safe Harbor privacy Principles, the European Commission 'accepted a weak and fragmented standard of privacy protection in the US as "adequate" in order not to endanger trade between the EU and the US.'[68] But, as Professor Greenleaf, went on to say, the same approach may not be adopted in relation to Australia. In any event, the Commonwealth Government made it clear that a major intention behind its private sector legislation was to ensure that the scheme:

> is compatible with the European Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data to remove any potential barriers to international trade.[69]

---

67 In addition, under the *National Health Act 1953* (Cth), the Federal privacy Commissioner is required to issue guidelines covering the storage, use and disclosure of information referring to claims made by individuals under the Pharmaceutical Benefits Scheme and the Medicare program.

68 G Greenleaf, 'Safe harbor's low benchmark for "adequacy": EU sells out privacy for U (August 2000) 7 *Privacy Law and Policy Reporter* 45.

69 Commonwealth Attorney-General, 'Information Paper on the introduction of the Privacy Amendment (Private Sector) Bill 2000' (March 2000) 6 *Privacy Law and Policy Reporter* 147.

The Commonwealth Government had indicated in 1997 that a self-regulatory regime would be introduced for the private sector. Due in part to a suggestion by the Victorian Government in 1998 that it intended to introduce private sector legislation if the Commonwealth Government failed to legislate, the decision was taken in December 1998 to introduce what was called a 'light touch' national legislative scheme, which would provide for a default set of privacy standards in the absence of industry codes to be approved by the Federal Privacy Commissioner. Proposed legislation along these lines was tabled in Federal parliament in April 2000 and subsequently reviewed by the House of Representatives Legal and Constitutional Affairs Committee and the Senate Legal and Constitutional Legislation Committee. After amendments in the Senate, widening the Act's application to pre-existing data and strengthening the role of the Federal Privacy Commissioner, the legislation was passed on 21 December 2000, coming into effect on 21 December 2001.[70]

Controversy over health information: Health information proved a particularly controversial issue in the debate over the extension of Federal privacy legislation to the private sector. In its June 2000 report, the House of Representatives Legal and Constitutional Affairs Committee commented in this respect:

> The inclusion of health information has proven to be the most contentious aspect of the Bill. The Committee has received a large number of submissions focussed solely on the issue of the coverage of health information. These submissions have generally concentrated on two issues: firstly, whether health information should be covered by the Bill at all and, secondly, the more specific issue of individuals' access to their own health information.[71]

For its part, the Committee was of the view that health information should be part of the Bill, on the basis that it would provide 'an interim acceptable level of privacy and access rights throughout Australia'. However, it went on to note its concerns about the intermingling of the private and public health sectors and, following on from that, the need for the 'privacy principles applicable to the two sectors to be harmonised as much as possible and the principles applicable to the public sector be applied in the private sector'.[72] Of particular concern to the Committee in this context were the exemptions applying to access to health records in the private sector.

Intended constitutional scope: Section 3 of the Federal Privacy Act makes it clear that its public sector provisions were intended to operate alongside concurrent State and Territory laws. On the other hand, in defining its objects, the *Privacy Amendment (Private Sector) Act*

---

70 This summary is based on – T Dixon editor, *Private Sector Privacy Handbook: A Guide to Private Sector Privacy Law and Practice*, CCH Australia Ltd 2000, at [3-050]. For an analysis of the amendments see – G Greenleaf, 'Private sector privacy Act passed (at last)' (December 2000) 7 *Privacy Law and Policy Reporter* 125.

71 House of Representatives Legal and Constitutional Affairs Committee, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*, June 2000, p 63.

72 House of Representatives Legal and Constitutional Affairs Committee, n 71, p 72.

2000 expressly states its intention to establish a single comprehensive national scheme'. Does this create something of a constitutional conundrum as far as State health information laws are concerned?

One line of argument adopted by the Federal Privacy Commissioner suggests that it does. Indeed, he has said that the operation of State and Territory privacy laws is restricted to the regulation of State and Territory public sectors and the regulation of private sector organisations that are exempt from the Privacy Act. If so, this leaves little, if any, scope for the State regulation of the private health sector. Speaking in February 2002, the Federal Privacy Commissioner said that, while the Victorian and ACT health records legislation were 'broadly consistent' with the Federal Privacy Act, 'some specific inconsistencies' also existed: For example, in Victoria the privacy protections offered are sometimes stronger and sometimes weaker than the Privacy Act. As a result, health service providers may be regulated by two similar, but not entirely consistent, privacy protection frameworks'. After commenting on the potential cost implications arising from this overlapping scheme of health privacy laws, the Federal Privacy Commissioner went to note that his Office 'has an obligation to consider investigation of all complaints which come under the Privacy Act, including those relating to health information in the Victorian, Australian Capital Territory and New South Wales private sectors'.[73] The implication seems to be that State-based private sector privacy regimes, for health information or otherwise, are fraught with difficulty. According to the Federal Privacy Commissioner, 'The need for clarification in this area is paramount'.[74]

Technically, the legal issue at stake here is what constitutes inconsistency of laws for the purposes of section 109 of the Australian Constitution. Three tests have been applied in this context, as follows:

- Direct inconsistency - if it is logically impossible to obey both laws (one law requires that you must do X, the other that you must not do X);
- Direct inconsistency - if one law purports to confer a legal right, privilege or entitlement which the other law purports to take away or diminish (one law says that you can do X, the other that you cannot do X);
- Covering the field - if the Commonwealth law evinces a legislative intention to 'cover the field', in which case there need not be any direct contradiction between the federal and State enactments. What is imputed to the Commonwealth parliament is a legislative intention that its law shall be all the law there is on that topic.[75]

Clearly, either of the 'direct inconsistency' tests may apply in certain circumstances where, as in the field of privacy law, the Commonwealth and the States exercise concurrent powers. As to the 'covering the field' test, this might also seem to apply in circumstances where the

---

73 M Crompton, Federal Privacy Commissioner, n 22, p 3.

74 M Crompton, Federal Privacy Commissioner, n 22, p 3.

75 This formulation is based on – T Blackshield and G Williams, *Australian Constitutional Law and Theory: Commentary and Materials*, 3rd edition, The Federation Press 2002, p 371.

Commonwealth has stated an intention to 'establish a single comprehensive national scheme' for the protection of personal information by the private sector. However, as it was explained by the Federal Attorney-General in the relevant Second Reading speech, State and Territory laws will continue to operate to the extent that they are not directly inconsistent with the terms of the bill.'[76] Presumably, in the context of a Bill dealing specifically with the private sector, this statement refers to State privacy legislation regulating that sector, in addition to its own public sector agencies.

Note, too, that NPP 2.1(g) makes an exception for health information where 'the use or disclosure is required or authorised by or under law'. As the Federal Privacy Commissioner's Guidelines have acknowledged in this context, 'Law' includes Commonwealth, State and Territory legislation, as well as the common law.[77] The implication to be drawn from this is that the NPPs are not intended to codify the way health information (or personal information generally) can be used. From this, the argument has been put that State legislation would remain valid in so far as it *extended* the categories of disclosure permitted by the NPPs.'[78] Specially in relation to the operation of the Victorian *Health Records Act 2001* it has been said:

> It is envisaged that the Commonwealth's new privacy and access provisions will operate alongside any State-based regime, and where there is inconsistency, the Commonwealth provisions will apply.[79]

Coverage: Just as the public sector provisions of the Commonwealth Privacy Act establish a scheme for the regulation of 'agencies', the new private sector provisions set up a regime for the regulation of 'organisations'. The term is defined broadly to include an individual, body corporate, partnership, an unincorporated association or a trust; but to exclude:

- a small business operator;
- a registered political party;
- an agency; a State or Territory authority;
- or a prescribed instrumentality of a State or Territory.[80]

The regime is not intended, therefore, to cover the State public sector, including State public hospitals and other State administered medical facilities. This field of regulation is left to

---

76 *Commonwealth Parliamentary Debates (House of Representatives)*, 12 April 2000, p 15751.

77 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector*, 8 November 2001, p 20.

78 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *The Sydney Law Review* 5 at 35.

79 F McKenzie and J Smith, 'Health records in Victoria: new legislation' (April 2002) 76 *Law Institute Journal* 50 at 53.

80 *Privacy Act 1988* (Cth), section 6C.

State legislation.[81] In an anomalous position are NSW State owned corporations. As noted, these are not covered under the *Privacy and Personal Information Act 1998* (NSW) and would only be covered under the Federal scheme if expressly prescribed by regulation at the request of the State. [82]

The Commonwealth privacy scheme does, however, cover the private health sector. Even 'small business' private sector health providers are covered. This is because the 'small business operator' exclusion does not apply to health service providers. The exclusion applies generally to businesses with an annual turnover of $3,000,000 or less. However, various exceptions to the rule are made, including where a small business operator '*provides a health service to another individual and holds any health information except in an employee record*'.[83] In other words, health data held by a private nursing home with an annual turnover of less than $3,000,000, to take one example, would be covered under the Commonwealth privacy scheme, except in respect to any health information it held on an employee record.[84] These records and any health information stored on them would lie outside the scope of the Commonwealth Privacy Act.

A co-regulatory scheme: As noted, the scheme now in place at the Commonwealth level is a 'light touch' co-regulatory model which allows organisations covered by the legislation to choose to be bound by a privacy code of practice approved by the Federal Privacy Commissioner or, where such a code is not in place, by the National Privacy Principles (NPPs). The NPPs are broad legislative principles, rather than highly specific legal rules and, as such, they are intended to operate as a default framework in the absence of industry codes. Also, they are be drafted in a way that is electronically neutral, with the result that

---

81 Private sector health service providers working under contract for a State government are not subject to the Federal Privacy Act: ALRC, n 16, p 130.

82 On this jurisdictional issue generally the relevant Second Reading speech commented: 'The bill is not intended to cover State and Territory public sector agencies, as this is a matter for the States and Territories themselves. The bill recognises that State and Territory government business enterprises, or GBEs, take many forms and the dividing line between the public and private sectors is not always clear. In order to ensure certainty, the bill provides that GBEs that are incorporated under the Corporations Law will automatically be covered by the bill unless they are prescribed otherwise by regulation. Those GBEs not incorporated under the Corporations Law, such as statutory corporations, will not be covered by the bill. To meet the varying requirements of State and Territory governments, however, the bill also provides a flexible opt-in opt-out mechanism for prescribing State or Territory instrumentalities. This will be achieved by regulation and will be done only at the request of the State or Territory government' – *Commonwealth Parliamentary Debates (House of Representatives)*, 12 April 2000, p 15751; *Privacy Act 1988* (Cth), section 6C.

83 *Privacy Act 1988* (Cth), section 6D (4)(b). 'Health service' is defined under section 6 (1).

84 'Employee record' is defined to include 'health information about the employee' – *Privacy Act 1988* (Cth), section 6 (1). A general exemption for employee records is made under section 7B (3) read with 7 (1)(ee). This exemption resulted from the Commonwealth Government's belief that employee records are more appropriately dealt with under workplace relations legislation : Senate Legal and Constitutional Legislation Committee, *Inquiry into the provisions of the Privacy Amendment (Private Sector) Bill 2000*, October 2000, p 14.

they apply equally to conventional, electronic and digital environments.

The National Privacy Principles (NPPs): Ten NPPs are set out in Schedule 3 to the Privacy Act. They have been summarised in this way:

- *Collection of personal information (NPP1)*: Collection must be necessary for an organisation's activities, information must be collected lawfully and fairly, and as a general principle must be collected with the individual's consent.[85]

- *Use and disclosure of personal information (NPP2)*: As a general principle, information can only be used or disclosed for its original purpose unless the person has consented to its use or disclosure for another purpose. Exemptions apply to initial contact for direct marketing (if consent was not practicable originally) and other situations such as when there are issues of law enforcement, public safety or protecting the company from fraud.

- *Accuracy of personal information (NPP3)*: Organisations must take reasonable steps to ensure that they keep personal information accurate, complete and up-to-date.

- *Security of personal information (NPP4)*: Organisations must take reasonable steps to protect the personal information which they hold from misuse, loss unauthorised access, modification or disclosure.

- *Openness in relation to the organisations practices (NPP5)*: Organisations which collect personal information must be able to document their practices and must make this information available on request.

- *Access and correction rights (NPP6)*: As a general principle, organisations must give individuals access to their personal information and must allow them to correct it or explain something with which they disagree, unless disclosing this would have an unreasonable impact on someone else's privacy. This principle is subject to exemptions such as if this disclosure would compromise a fraud investigation.

- *Use of government identifiers (NPP7)*: Organisations cannot use government agency's identifier as their identifier. This would cover items such as Medicare numbers, a Tax File Number (which in any case is covered by other legislation) or any future identity numbers assigned by a Commonwealth government agency.[86]

- *Anonymity (NPP8)*: Organisations must give people the option of entering into transactions anonymously where it is lawful and practicable. For example, this would apply to using a smart card to travel on a bus, but not to opening a bank account.

---

85 But note that no direct reference is made to consent in this context . Under the Privacy Act generally consent may be either express or implied.

86 Thus, a private health insurance fund is prohibited from using a person's Medicare number for its own data collection purposes.

- *Restrictions on transborder data flows (NPP9)*: As a general principle, organisations can only transfer the personal information about an individual to a foreign country if they have consent, or legal protections are in place covering the country to which the information is transferred such as a law or a contract which upholds privacy principles similar to the NPPs.

- *Special provision for sensitive personal information (NPP10)*: A higher level of privacy protection applies to sensitive personal information, which includes information about a person's health, political or religious beliefs or affiliation, and sexual preference. This information must, generally, only be collected with the individual's consent.[87]

Health information and the NPPs: Health information'is defined in the Act to mean:

> (a) information or an opinion about:
> (i) the health or a disability (at any time) of an individual, or
> (ii) an individual's expressed wishes about the future provision of health services to him or her; or
> (iii) a health service provided, or to be provided, to an individual;
> that is also personal information; or
> (b) other personal information collected to provide, or in providing, a health service; or
> (c) other personal information about an individual collected in connection with the donation, by the individual of his or her body parts, organs or body substances.

Further, 'health information about an individual'is treated as a distinct type of 'sensitive information', a term which is defined under section 6 (1) of the Act.[88] Note that the information must be 'about an individual'. It must therefore be personal in nature and related to an identifiable individual.[89] As 'sensitive information' under NPP 10, information concerning an individual's health is said to attract higher privacy standards. Basically NPP10 makes the collection of sensitive information (including health information) subject to individual consent, although in the case of health information important exceptions apply and these are discussed below.

The term ***health service***'is defined broadly under the Federal Privacy Act to mean:

---

87 *Private Sector Privacy Handbook: A Guide to private Sector Privacy Law and Practice*, n 70 at [3-1000].

88 Other examples of 'sensitive information' include information or an opinion about an individual's racial or ethnic origin, criminal record or political opinions.

89 The provision does not encompass aggregated research information about, for instance, the comparative incidence of lung cancer amongst different socio-economic groups

> (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
> (i) to assess, record, maintain or improve the individual's health; or
> (ii) to diagnose the individual's illness or disability; or
> (iii) to treat the individual's illness or disability or suspected illness or disability; or
> (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

As the Federal Privacy Commissioner has said, under the Act providers of health services 'range from hospitals, pharmacists and general practitioners to gyms and weight loss clinics'.[90] The guidelines released by the Privacy Commissioner are not explicit on the point, but it would seem that private health insurers are 'health service' providers under the Act, on the basis that they 'record' health information.[91]

However, it needs to be emphasised that any 'organisation' under the Privacy Act, be it a health service provider or otherwise, is subject to the provisions which apply to the way organisations generally handle health information under the federal privacy regime. For example, NPP2 (Use and disclosure) applies to the way all organisations handle health information; but under NPP2.4 special provision is made for health service providers who may, in certain circumstances, disclose health information to a person responsible for an individual, notably where an individual lacks the capacity to consent to the disclosure, or cannot communicate his or her consent. Thus the privacy requirements applying to health information are modified in some circumstances where health service providers are concerned. As discussed below, the operation of NPP10.2 also applies only to health service providers, in this case in respect to the collection of health information without consent.

Health information held before 21 December 2001: The Federal Privacy Commissioner has explained that only some of the NPPs apply to information collected before 21 December 2001. These include NPP4 (on data security), NPP5 (on openness), NPP7 (on identifiers), and NPP9 (on Transborder data flows). NPP6 (on access) also applies to information already collected, but only where the information is still in use, and if giving access would not pose an unreasonable administrative burden or expense on the health service provider.[92]

---

90 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector*, 8 November 2001, p iii.

91 Based on telephone advice from the Office of the Federal Privacy Commissioner. The view is that section 6(1)(a)(i) is to be read disjunctively to mean 'to assess *or* record *or* maintain or improve the individual's health…'. Note, too, that NPP 10.3 (a)(iii) makes reference the collection of health information for 'the management, *funding* or monitoring of a health service'.

92 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector*, 8 November 2001, p viii.

The application of the Privacy Act to information already held is set out at Appendix A.

Collecting health information (NPP1 and NPP10): In effect, all the privacy principles are relevant to health information. Detailed analysis of that relevance is presented in the Federal Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector*. One point that document makes is that to understand how the new federal privacy regime affects the 'collection' of health information it is necessary to read NPP1 (collection) and NPP10 (sensitive information) together. The obligations created by these principles for a health service provider when collecting health information can be summarised as follows:[93]

- Under NPP10.1, personal health information can only be collected with consent, except in specified circumstances including, but not limited to, emergencies, as required by law, or in circumstances relating to legal or equitable claims.
- Under NPP10.2, a health service provider may also collect health information without consent, under special conditions. For example, when providing a health service where: the information is necessary to provide a health service to the individual, and the information is collected as required by law (other than the Privacy Act itself), or in accordance with the rules of a competent health or medical body.
- NPP 10 (3) sets out further grounds for any 'organisation' to collect health information without consent where collection is necessary for: (i) research relevant to public health or public safety; (ii) the compilation or analysis of statistics relevant to public health or public safety; or (iii) the management, funding or monitoring of a health service.[94] In each of these three cases, certain conditions apply, including that the research/statistical/or management purpose cannot be served without the collection of information relating to an identifiable individual, it is impracticable for the organisation to seek the individual's consent, and reasonable steps must be taken to de-identify the information before it is disclosed. Further the information must be collected in accordance with either the rules of professional confidentially relevant to the organisation, or in accordance with guidelines approved under section 95A of the Commonwealth Privacy Act.[95]
- NPP1.3 requires all organisations (not just health service providers) to take reasonable steps to ensure that individuals are aware of certain matters, including, but not limited to, who is collecting the information, the fact that the individual is able to gain access to the information and the purposes for which the information is collected.
- Under NPP1.1, only information necessary for the performance of the health service provider's functions or activities can be collected.
- Under NPP1.4, information is to be collected directly from the individual where this is

---

93 This is based on Office of the Federal Privacy Commissioner, *Guidelines on privacy in the private health sector*, 8 November 2001, p 1.

94 This category would only apply therefore to health service providers, but would include private health insurance companies.

95 For a comprehensive account of the implications for medical research see - R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health *The Sydney Law Review* 5.

reasonable and practicable.

Collecting family medical histories: NPP1.5 states that when private sector organisations generally collect personal information about third parties, they are obliged to take reasonable steps to ensure that the third party is made aware of his or her rights under NPP1.3. One consequence of this is to put in doubt the legality of a general practitioner, or other health service provider, collecting information about a patient's family medical history. This is because such a process involves the collection of identifiable personal information about a third party, the patient's father for instance. Typically, the information is gathered in a way which does not satisfy the requirement to take reasonable steps to make the third party aware of their access rights and other matters;[96] nor would the process typically satisfy those circumstances under the NPPs where the consent of family members is required before collection occurs.[97] To make the collection of family medical history subject to such requirements would clearly impose an intolerable burden on general practitioners and others.

To avoid this pitfall, the Federal Privacy Commissioner has issued a Temporary Public Interest Determination to ensure that the collection of family medical history by health service providers is not prevented by the Privacy Act. This applies in circumstances where: (a) the collection of the third party's information is necessary to the health service provider; (b) the information is collected to provide a health service directly to the individual; (c) the information is used to diagnose, treat or care for the individual; and (d) the third party is a member of the individual's family or household, or the third party's information is otherwise relevant to the individual's family medical history or social medical history.[98]

Use and disclosure of health information (NPP2): The relevant obligations for organisations, including health service providers, are as follows:

- Under NPP2.1(a), to only use or disclose personal information for the primary purpose for which it is collected, or for *directly* related secondary purposes if these fall within the reasonable expectations of the individual. An example suggested by the Federal Privacy Commissioner is where an individual agrees to see a specialist and the necessary information sharing between the general practitioner and the specialist occurs. Such a multi-disciplinary approach to health care is now the norm in Australia and, in these circumstances, consent would be not required for the general practitioner to share the necessary information with the specialist.[99]
- Under NPP2.1(b), to only use or disclose health information in other ways if the individual gives consent (whether express or implied), or if one of the exceptions to this principle applies. The exceptions include, but are not limited to, uses or disclosures required or authorised by law, those necessary to prevent or lessen a serious or imminent

96 These requirements are found under NPP1.5 read with NPP1.3.

97 Relevant is NPP10.1.

98 Temporary Public Interest Determination No 2001-1.

99 Office of the Federal Privacy Commissioner, n 93, p 14.

threat to someone's life, health or safety, or for research provided certain conditions are met.

As noted, NPP2.4 sets out the circumstances when a health service provider (but not other organisations) can disclose health information to a 'person responsible' for an individual who cannot give or communicate their consent.

Access and correction rights (NPP6): An organisation's obligations (including health service providers) include:

- Under NPP6.1, giving an individual access to their personal information if they ask for it, unless particular circumstances apply that permit the health service provider to deny access or to limit the extent to which access is given. These circumstances include where there is a serious threat to life or health, and where the request is frivolous or vexatious.'
- Withholding access as required by law, or for reasons connected with law enforcement purposes.
- Under NPP6.3, when access might otherwise be denied, considering whether providing access through an intermediary is possible.
- Under NPP6.4, where reasonable, correcting personal information at the request of the individual.

As to the frivolous or vexatious' ground for refusing access, the Federal Privacy Commissioner has commented that 'Usually, a request for access would not be frivolous or vexatious just because it is an irritation. Health service providers are encouraged to take a careful approach to this provision.'[100]

As noted, in its June 2000 report the House of Representatives Legal and Constitutional Affairs Committee expressed particular concern about these access provisions. It recommended that the access standards for health records as between the public and private sectors be harmonised on the basis of the ACT *Health Records (Privacy and Access) Act 1997*. This recommendation was not accepted by the Government.[101]

The Committee's views were founded on a lengthy analysis of the arguments for and against the access provisions under the Bill, ranging from the AMA's view that too much access was being granted, on one side, to the Public Interest Advocacy Centre's argument that the only exemptions that should apply are those that would 'interfere with the privacy of other people or where there is a risk of imminent harm', on the other.[102] As to the question of inconsistency with the public sector, the main contention was that the right of access under NPP6 falls short of that available in the public sector under Freedom of Information legislation. In particular, NPP6 was said to be subject to too many exemptions – 11 in total - whereas under FOI legislation the right of access for the public sector is only qualified in

100 Office of the Federal Privacy Commissioner, n 93, p 35.

101 House of Representatives Legal and Constitutional Affairs Committee, n 71, Chapter 7.

102 House of Representatives Legal and Constitutional Affairs Committee, n 71, p 79.

relation to: medical or psychiatric records concerning the applicant; and where, in the agency's opinion, disclosure may have an adverse effect on the applicant's physical or mental health. But even then the agency is directed to give access to a registered medical practitioner nominated by the applicant.

Enforcement: The appropriate enforcement procedure depends on whether an approved Code is in place. If not, complaints are handled by the Federal Privacy Commissioner. If a Code is in place, complaints may be made to the health service provider concerned and, if not resolved, may be taken to the Privacy Commissioner or an independent adjudicator. Breaches of the NPPs can result in an order from the Commissioner to restrain an action, undertake an action, or to give monetary compensation. A decision to give an individual a remedy can be appealed in the Federal Magistrate's Court, and can be enforced through the Court if not complied with by the relevant health service provider.

Note that in some industries complaints can be handled by Code authorities, such as the Banking Industry Ombudsman. However, this arrangement is unlikely to apply in the highly diverse field of health service provision.

4.3 Comments:[103]

The Federal Privacy Act and its extension to the private sector has been the subject of widespread comment. One line of comment concerns the failure to comply with the European Directive on Data Protection. In submissions to the House of Representatives Standing Committee on legal and Constitutional Affairs the European Commission expressed the view that further safeguards will need to be introduced if the Australian privacy regime is to be regarded as 'adequate'. A significant inadequacy, in the Commission's opinion, is the application of NPP6 (access and correction rights) to only Australian citizens and permanent residents. As Brett McGuire and Anthony O'Hea explain, 'The European Commission's concern with this provision arises primarily due to the continuing growth of e-commerce which has made possible interference with the privacy rights of European citizens by Australian companies.'[104]

Criticism has also been directed against the range of exemptions available under the privacy regime. In general terms, this refers to the broad exemptions available to small business, as well as to the employee records exemption. The establishment of such 'privacy-free zones' prompted Professor Greenleaf to say that 'the political process has failed to deliver

---

103 ALRC, n 16, p 153. Summarised are the range of criticisms made against the Federal privacy regime. For example it is said that 'since organisations are free to develop their own codes, this may further contribute to a lack of consistency in how health information is treated – although the statutory scheme for approving codes may help prevent significant inconsistencies from arising'. It is also noted that 'it is unclear which health industry body will be responsible for the private sector health guidelines and whether doctors, hospitals and health funds will be subject to separate codes.

104 B McGuire and A O'Hea, 'Privacy in Australia – What Went Wrong?' (2001) 12 *Public Law Review* 246 at 247.

Australian citizens, consumers and businesses privacy legislation of world standard.'[105]

As noted, the 'small business' exemption does not apply to health service providers. The 'employee records' exemption does apply and therefore health information collected in this context is not subject to the NPPs. More generally, the exemptions expressly relating to health information have attracted considerable debate, particularly those relevant to the principle of 'access and correction'. The House of Representatives Legal and Constitutional Affairs Committee review was concerned that 'the range of exceptions may too broad' and that, as a result, different privacy standards would apply in the public and private health sectors. The Committee commented: 'As was pointed out by a number of witnesses, many patients will interact with both the public and private health sectors in the course of a single health event. It would seem unnecessarily complicated to grant different rights of access in relation to information held in the public and private sectors'. Its view was that these standards should be harmonised along the lines achieved in the ACT. It is precisely that harmonisation which is the subject of Victoria's *Health Records Act 2001* and, in NSW, of the Draft Health Records Bill.

For his part, the Federal Privacy Commissioner has acknowledged that complexities arise when health services 'are delivered through a mix of private and public sector providers across both private and public sector sites'. The Commissioner gives the example of where 'public and private hospitals are co-located', stating:

> Where a private health service provider works within a public hospital, it is generally the case that the medical record remains subject to management by the public sector hospital, and therefore comes under relevant Sate/Territory legislation –regardless of clinical entries in those records by public or private sector providers.
>
> However, if a private health service provider treats an individual in a public hospital, but retains records (including copies) in a private clinic or other place away from the public hospital, these records would be subject to the [Federal] Privacy Act.[106]

For some, such complexities add weight to the argument that health information is a special area in which private and public sector activities overlap to a point where, to avoid confusion, they need be governed by a single piece of legislation. The potential for confusion created by the concurrent operation of State and Commonwealth regimes must also be acknowledged. A further area of debate is the constitutional validity of State-based private sector privacy laws, with the Federal Privacy Commissioner seemingly adopting the view that the Commonwealth has intended to 'cover the field' in this area. The fact that Victoria has already enacted private sector health records legislation and that NSW intends to follow that lead in the immediate future suggests that there are alternative interpretations of this

105 G Greenleaf, n 70, p 126.

106 Office of the Federal Privacy Commissioner, n 90, pp iv-v.

constitutional question.

5. HEALTH RECORDS AND INFORMATION PRIVACY BILL 2001 (EXPOSURE DRAFT)

5.1 The Ministerial Advisory Committee

In its December 2000 report, *Panacea or Placebo? Linked Electronic Health Records and Improvements in Health Outcomes*, the NSW Ministerial Advisory Committee on Privacy and Health Information recommended 'That the system of linked electronic health records be governed by a separate and specific piece of State legislation entitled the Health Records and Information Privacy Act'. It further recommended that the proposed Act:

(a) apply to all health records, in whatever form kept, in both the public and the private sectors of health care and health care delivery in New South Wales;
(b) specify the purposes for which health records may be linked and transferred so that no linkage or transfer may take place without specific legislative authority;
(c) incorporate the Information Protection Principles as set out in Part 2 of the Privacy and Personal information Protection Act 1998 modified as and if required to meet the specific needs of the health sector;
(d) establish protocols and provide mechanisms whereby linked electronic health records (or parts thereof) can be transferred between authorised parties;
(e) provide for the right of inspection, access, copy, annotation and correction of any health record by any person who is the subject of such a record, except where exceptional circumstances (to be defined clearly in the legislation and which relate to the protection of the welfare of such a person) apply;
(f) vest in the Privacy Commissioner of New South Wales the powers to:
    - investigate and determine complaints made under the Act
    - initiate investigations and conduct enquiries and audits relevant to the conduct and administration of the Act
    - make reports and recommendations to the Minister and Parliament regarding the administration and operation of the Act.
(g) establish mechanisms for allowing complaints related to alleged breaches of privacy and other improper conduct to be made and determined
(h) impose significant penalties of both a civil and criminal nature for breaches of the Act;
(i) incorporate (either directly or by cross-reference) all existing privacy and confidentiality requirements present in various existing health-related statutes of New South Wales
(j) give specific recognition to particular problems related to the capacity of children to withhold information from their parent or guardian in particular circumstances.[107]

5.2 Draft Health Records Bill 2001

Responding to this recommendation an exposure draft of a Health Records Privacy Bill was released by the NSW Health Minister in December 2001. According to an explanatory guide

---

[107] Ministerial Advisory Committee on Privacy and Health Information, n 32, p 25.

on the Draft Health Records Bill, [108] one of its founding principles is to 'build on what has already been achieved at the State and federal level, rather than duplicate it'. The Draft Bill, it was said, 'has been designed to maintain consistency with the Commonwealth National Privacy Principles, so that action undertaken in order to ensure an agency, organisation or individual is ready to comply with the Commonwealth Principles will ensure compliance with the principles established under this Bill'. The explanatory guide continued:

> The aim of the Health Records and Information Privacy Bill is to provide a single state-based scheme for the management of health privacy obligations, imposing the same set of Privacy Principles on information holders in both the public and private sector. The Bill will also provide a readily accessible complaints process and recognise the special issues which arise in the handling of health information. Similar legislative approaches have already been adopted in both the ACT and Victoria.[109]

In terms of the rationale behind the Bill, it was said that the Ministerial Advisory Committee 'considered that a strong regulatory regime protecting health information and applying irrespective of the format in which the information is kept, was essential to address community concerns about the privacy risks associated with electronic records'.[110]

5.3 The Draft Bill in summary

In what is a familiar arrangement for privacy legislation, the 15 Health Privacy Principles (HPPs) are set out in a Schedule to the Bill. Briefly, the HPPs cover:

- collection (HPP 1-4)
- retention and security (HPP 5)
- access and alteration (HPP 6-8)
- accuracy (HPP 9)
- use and disclosure (HPP 10-11)
- identifiers (HPP 12)
- anonymity (HPP 13)
- transborder data flows (HPP 14)
- linkage of health records (HPP 15).

Of these, HPP 15 is the most obvious departure from the familiar list of privacy principles, designed as it is to meet particular concerns in the health field. In effect, HPP 15 prevents the creation of linked electronic health records without the *express* consent of the individual to whom the information relates. Certain exceptions apply, including where an organisation creates a health records linkage system to which only related bodies corporate of the

---

108 In this section of the paper the Health Records and Information Privacy Bill 2001 is referred to as either the Draft Health Records Bill or the Draft Bill.

109 *Guide to the Health Records and Information Privacy Exposure Draft Bill*, p 2.

110 *Guide to the Health Records and Information Privacy Exposure Draft Bill*, p 1.

organisation have access and which is for the benefit of [sic] individual.'[111] In certain other respects the proposed arrangements for the public and private sectors vary, but the common thread is that the HPPs apply across the board.

The Draft Bill is in 10 Parts setting out the operation of the proposed HPPs. In summary, Part 1 is introductory in that it sets out the Bill's purposes and objects, and deals with definitional issues. Part 2 then defines how the proposed Act is to be applied, in terms of its coverage of private and public sector organisations, and the retrospective or prospective application of various HPPs. Part 3 makes special provision for the application of the HPPs to public sector agencies, and provides that complaints against public sector agencies will be dealt under the *Privacy and Personal Information Protection Act 1998* (NSW). Part 4 deals specifically with the private sector, in particular setting out the arrangements for the retention of health information and access to it in more detail than is found under the HPPs. Part 5 deals with the making of health privacy codes; Part 6 with the making of complaints, but only against private sector persons. The functions and powers of the NSW Privacy Commissioner are found under Part 7, while Part 8 is headed 'Miscellaneous' and includes various proposed offence provisions.

Note that the following discussion is based on the Exposure Draft version of the Draft Health Records Bill, as released for public comment in December 2001.

5.4 Coverage

The Draft Health Records Bill applies to 'every organisation that is a health service provider or that collects, holds or uses health information.'[112] The word 'organisation' in this context means a public sector agency or a private sector person. In other words, the Draft Bill covers any organisation, private or public sector, dealing in health information, be it a health service provider or not.

Reflecting section 6C of the Federal Privacy Act, the term 'private sector person' is defined in the Draft Bill to include any of the following that is not a public sector agency: a natural person; a body corporate; a partnership; a trust or any other unincorporated association or body. Also consistent with the Federal Act, 'small business operators' are excluded from this definition, but not if they are health service providers. This means that all health information held by private sector health service providers is covered under the proposed NSW legislation; on the other hand, health information held by a small business operator who is not health service provider is excluded.

A further point of contrast to make with the Federal Act is that the NSW Draft Bill is silent on the question of employees' records. As noted, these are exempted entirely from the Federal privacy scheme. At this stage, it seems that the NSW proposal would cover health information in employee records held by private sector employers, but not if the employer qualified for exemption as a small business operator (that is, as a non-health service

111 Draft Health Records Bill 2001, Schedule 1, HPP 15 (3) (c).

112 Draft Health Records Bill 2001, clause 11 (1).

provider).[113] To illustrate by way of some examples.

First, consistent with the Federal regime, a general medical practice, with an annual turnover of less than $3,000,000, would be subject to the proposed State based HPPs. So, too, at this stage (and this is where the NSW scheme deviates from the position federally) would any health information records collected in the general practice's capacity as an employer.

The same would apply to a private nursing home with an annual turnover of less (or more) than $3,000,000.

Secondly, in contrast to the position under the Federal Privacy Act, a private health insurance company would not qualify as a 'health service provider' under the NSW Draft Bill. This is because a very different approach is taken to defining 'health service' under the Draft Bill. However, in the likely event that the private health insurance company has an annual turnover of more than $3,000,000 (and would not therefore qualify for the 'small business operator' exemption), it would be covered under the proposed NSW scheme as a private sector organisation 'that collects, holds or uses health information.' As a result, the health information held by a private health insurance company would be subject to the HPPs (as it would be subject to the NPPs). Further, (and here the NSW scheme diverges from its federal counterpart) any health information the company held on its employees' records would similarly be subject to the HPPs.

The same would apply for a private hospital in NSW. Under the Draft Health Records Bill it is clearly a 'health service provider' and all the health information it holds, be it in relation to its patients, or to health information records collected in its capacity as an employer, would be subject to the HPPs.

Thirdly, health information held on the employee records of a small business operator which is not a health service provider – a local garage employing 2 or 3 mechanics, for example, with an annual turnover of less than $3,000,000 – would be exempt from the NSW regime. This is consistent with the position under the Federal Act.

Further comparison can be made with the Victorian *Health Records Act 2001* which does not make any exemption for 'small business operators.' In that situation, the HPPs apply across the board to health information held by all private sector organisations – with annual turnovers of more or less than $3,000,000. Moreover, the HPPs apply across the board to health information held by employers in the form of employee records.

5.5 Health service and health service providers

Both terms are defined in the Draft Bill. Health service provider' is defined as any public sector agency or private sector person that provides a health service, unless exempted by regulation.

---

113 It may be that, owing to concerns about consistency with the Federal regime, this is one area where the NSW proposals may be revised before a Bill is introduced into Parliament.

Health service' is defined in a different way to any of the other Australian legislative models. The relevant Federal, Victorian and ACT legislation all take a broad functional approach to defining 'health service' in terms of 'activities' that, for instance, assess or maintain an individual's health, or diagnose or treat an individual's illness. Federally, it is left to the guidelines published by the Privacy Commissioner to stipulate which services do and do not fit this expansive criteria.

The NSW Draft Bill, on the other hand, is more certain and task specific in that it lists particular medical services, whether provided as public or private services. These include: medical, hospital and nursing services; dental services; mental health services; health education services; services provided by podiatrists, chiropractors and others; services provided by dietitians, masseurs and others; and services provided in other alternative health care fields.

From this approach it is at least clear that private health insurance companies are not health service providers. As discussed in an earlier section of this paper, it seems they would be health service providers under the Federal Privacy Act. The position in Victoria, on the other hand, would appear to be that private health insurers are excluded from its definition of 'health service' which, unlike its Federal counterpart, does not make reference to the 'recording' of health information. All of which begs the question as to whether the NSW/Victoria or the Federal approach it to be preferred.

5.6 Health information

The Draft Bill first defines 'personal information' in a way that is consistent with the NSW *Privacy and Personal Information Protection Act 1998*. It then defines 'health information' as a sub-set of 'personal information' that is 'information or an opinion' about a person's physical or mental health and information collected about organ donation and genetic information. It also includes information about a 'health service' provided (or to be provided) to a person.

One variation from the Federal and Victorian models can be noted. Thus, the Federal Act refers to information about '*the health or a disability*' of an individual. The Victorian Act goes a step further and refers to the '*physical, mental or psychological health…or a disability*' of an individual. Whereas the preferred formulation in the Draft Bill is '*the physical or mental health*' of an individual. Thus, the NSW draft makes no mention of disability. Is the omission significant? Arguably not, for any information about a relevant disability would almost certainly fall under the rubric of 'physical or mental health'.[114] That conclusion is supported by the definition of 'disability' under the *Anti-Discrimination Act 1977* (NSW).

5.7 Consent

Unlike the Federal Privacy Act, as well as the Victorian and ACT health records statutes,

[114] Note that section 31 (4) of the FOI Act also uses the phrase 'physical or mental health'.

the Draft Bill does not define the word 'consent'. In all these statutes it is made clear that *express or implied consent*'. The same would be the case under the Draft Bill, some provisions of which makes direct reference to 'express consent' where this is appropriate. The question is whether, for the sake of clarity, consent should be defined to include implied or express consent?

5.8 Children and capacity

Consistent with the other legislative privacy regimes currently in operation in NSW and other the Australian jurisdictions, children are not precluded from taking advantage of the rights established under the Draft Bill. They may do an act authorised, permitted or required by the Draft Bill, but only if they are capable of understanding the nature and effect of the act, or of communicating their intention with respect to the act. Stated negatively, as it is in the Draft Bill, if a child (even with assistance) is incapable of such understanding or communication, *'by reason of age, injury, illness, physical or mental impairment'*, then they cannot act on their own behalf, only by means of an authorised representative. The fact that a child, a word defined to mean an individual under 18, may have the required capacity becomes clear when it is said in clause 7 (3) that, when a child 'is capable of doing that act', an authorised representative may only act on a child's behalf on the child's express authorisation.

What this appears to mean is that the factor of 'age' will prevent a child from making a complaint or accessing its medical records unless, that is, it can be shown that the child has the requisite understanding and powers to communicate its intentions. The issue of the minor's capacity will be, if Lord Scarman's comments in case are a reliable guide, a 'question of fact' and will 'not be determined by reference to any judicially fixed age limit'.[115] *Gillick's* case is a good illustration of the how sensitive an issue this can be. That case involved the right of parents to consent to the medical treatment of a child, in particular the giving of contraceptive advice to a girl under 16 years of age. Among other things, it was decided that a girl under 16 has the legal capacity to consent to medical examination and treatment, including contraceptive treatment, if she has sufficient maturity and intelligence to understand the nature and implications of the proposed treatment. By extension, a 15 year old girl might also want to prevent her parents from gaining access to her medical records, or to instigate a complaint against a general practitioner who, without her consent, discloses her health information to her parents. Such 'acts' are not precluded under the formulation adopted by the Draft Bill.[116]

The formulation in the Draft Bill is based on section 85 (3) of the Victorian statute, although there the provision is limited to 'giving consent, making the request or exercising the right

---

115 *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] 1 AC 112 at 188.

116 Note that section 49 of the *Minors Property and Contracts Act 1970* (NSW) deals with the power of under-16s to consent to medical treatment. It protects doctors and dentists from civil claims for assault provided: if the patient is under 16 a consent has been given by his/her parent or guardian; if the patient is aged 14 he or she has given prior consent. Implicit in these arrangements is the understanding that, at the age of 16, a young person has the same right to consent to medical treatment as an adult.

of access'. The making of complaints is covered separately under section 47 where it is stated unequivocally that a complaint may be made 'by a child', or on its behalf.[117] This positive formulation has the virtue of clarity and may be thought a preferable approach from a children's rights standpoint. However, it may be thought overly simplistic. The child's right is stated without qualification as to age or capacity. Questions as to the internal consistency of the Victorian scheme might also be posed, where a child might be found not to have the capacity to make a request for access, but to enjoy an unqualified power to complain when the request is refused.

Another model, at least as regards a child's right of access to medical records, is found in the ACT's health records legislation. This is stated in positive (if not exactly plain) language, so that a person under 18 has a right to information if they are of sufficient age and mental and emotional maturity to understand the nature of the health service provided and to give consent.[118]

In any event, complex and sensitive issues are at stake here. Under the Draft Bill the question of fact as to capacity must, presumably, be answered in the first instance by whoever is charged with the duty of giving access to the child's medical records. The decision may fall initially, therefore, to a general practitioner, but afterwards to the Privacy Commissioner if a complaint is lodged by the child. Acting as the complaints gatekeeper, the Commissioner would be the ultimate arbiter as far as this issue is concerned.

5.9 Retrospective operation of the HPPs

With certain exceptions the HPPs would apply to all health information collected by an organisation before or after the commencement of Schedule 1. The exceptions are as follows:

- HPP 1-4 (collection)
- HPP 13 (anonymity)

In both cases only information collected after the HPPs are in force would be covered. This is consistent with the position federally in relation to the equivalent NPP 1 (collection) and NPP 8 (anonymity).

The situation in respect to HPP 7 (access) and HPP 8 (amendment) is more complex. In certain specified areas the HPPs are to apply to information collected before the commencement of Schedule 1. These specified areas are defined broadly to include such matters as: an individual's medical history; the results of medical investigations about an individual; and a diagnosis of an individual's illness. This can be contrasted with the more

---

117 To this the provision adds: 'A child who is capable of understanding the general nature and effect of choosing a person to make a complaint on his or her behalf may do so if he or she is otherwise incapable of exercising powers'.

118 *Health Records (Privacy and Access) Act 1997* (ACT), section 10 (6) read with the definition of 'young person'.

restrictive position federally where, under NPP6, access and correction rights only apply to information held before 21 December 2001where: (a) it has been used or disclosed since the commencement of the Federal regime; and (b) providing access would not pose an unreasonable administrative burden or expense on the health service provider.

Do questions of constitutional inconsistency arise potentially in this context? Does the Federal law give a private health service provider the power to refuse access to medical records in circumstances where the Draft Bill would require access to be provided? Even if constitutional inconsistency is not an issue, complexity may be, for the two regimes would appear to require health administrators to comply with different standards.

As to the obligations of health administrators in a practical sense, the operation of the retrospectivity rule under the Draft Bill is modified by proposed section 30 (4) which provides that, where access is sought for health information collected prior to commencement, a private sector organisation can satisfy the requirement for access by providing a summary of the information in question.

5.10 Relationship with the Privacy and Personal Information Protection Act 1998

Basically the relationship is twofold. First, the Draft Bill excludes health information from the definition of 'personal information' under the *Privacy and Personal Information Protection Act 1998* [**the NSW Privacy Act**]. In this way, the protection of health privacy is made the exclusive concern of the Draft Health Records Bill. Secondly, the complaints mechanism established under Part 5 of the NSW Privacy Act remains in operation for public sector health service providers.

5.11 Public sector agencies

This application of the existing privacy complaints regime to public sector agencies is established under Part 3 of the Draft Bill which is headed, 'Special provisions for public sector agencies'. In effect, breaches of the HPPs or any relevant code of practice by a public sector agency are to be dealt with in the same way as any breach of an IPP under the NSW Privacy Act. The full requirements for internal review apply therefore, as do the avenues of appeal to the Administrative Decisions Tribunal.

It is also the case that the FOI Act would not affected by the Draft Bill. Indeed, any rights of access and correction under the FOI regime are to apply as if they were part of the proposed Health Records and Information Privacy Act. These arrangements mirror the relationship between the FOI Act and the NSW Privacy Act.

A general point to make is that there is considerable overlap between the State privacy and FOI legislation, particularly where access and correction rights are concerned. It is also the case that conflict can arise between the two schemes, notably where an FOI request includes a document that contains the personal information of someone other than the applicant (a third party). This potential for conflict is modified by the inclusion in the FOI legislation of an exemption for Documents affecting personal affairs'which provides: 'A document is an exempt document if it contains matter the disclosure of which would involve the

unreasonable disclosure of information concerning the personal affairs of any person (whether living or deceased)'.[119] However, the term 'personal affairs' is not defined, which raises the question whether it is to be interpreted in a way that is consistent with the phrase 'personal information' under the State privacy legislation. Also, the prohibition is only against 'unreasonable disclosure', which leaves unresolved the question of when information concerning personal affairs would be released to a third party.

5.12 Private sector organisations – special provisions

As well as conforming to the HPPs, additional requirements are proposed for private sector persons (organisations) under Part 4 of the Draft Bill. These are set out as follows: retention of health information (Division 2); access to health information (Division 3); and amendment of health information (Division 4).

Retention of health information: These requirements are in addition to HPP5 which provides, among other things, that health information should not be kept for longer than is necessary, is protected by reasonable security safeguards and is to be disposed of in a secure way.

As to the additional requirements, some apply to all private organisations, others only to health service providers. As noted, private health insurance companies are not health service providers under the Draft Bill. A provision applying only to health service providers is proposed section 24 which deals with the 'retention of health information'. The proposal mirrors clause 41 of the *Private Hospitals Regulation 1996* in requiring health information to be retained for 7 years (in the case of adults) and 25 years (in the case of children). Conversely, proposed section 27 applies only to non-health service providers who are required to destroy or de-identify health information when it is no longer needed for the purpose for which it was collected.

Also, special provision is made for medical practitioners who comply with regulations under the *Medical Practice Act 1992*.

Access to health information: These requirements are in addition to HPP7 which establishes a right of access to health information. The added requirements set out in detail: how a request is to be made (in writing, for example);[120] how and when a response is to be made (a request for access must be responded to within 45 days);[121] the form in which access is to take (by giving the individual a copy of the health information);[122] the power of

---

119 *Freedom of Information Act 1989* (NSW), Schedule 1, clause 6(1). For an analysis of the questions of consistency which arise see – G Griffith, n 56, pp 26-27; A Rath, *Freedom of Information and Open Government*, NSW Parliamentary Library Research Service, Background Paper No3/2000, pp 18-20.

120 Draft Health Records Bill, proposed section 28.

121 Draft Health Records Bill, proposed section 29.

122 Draft Health Records Bill, proposed section 30.

an organisation to require evidence of identity;[123] and for the making of alternative arrangements with the consent of the individual concerned.[124]

Also set out are the situations in which access need not be granted.[125] Consistent with other Australian privacy regimes, various 'law enforcement' and 'legal proceedings' exemptions would apply. So, too, would an exemption against an 'unreasonable repeated request' where information has already been given, or where the request has been refused and there are no reasonable grounds for making the request again. This is a more specific and probably an improved formulation of the 'frivolous or vexatious' exemption under NPP6.1 of the Federal privacy regime. Other grounds of exemption include where the information is subject to 'confidentiality' (a term which is separately defined under the provision), or where providing access would reveal the organisation's intentions 'in relation to negotiations, other than about the provision of a health service, with the individual in such a way as to expose the private sector person unreasonably to disadvantage.

As in the case of NPP6.1 under the Federal regime, access can also be refused on the ground that it would pose a 'serious threat to the life or health of the individual or any other person.' Alternative arrangements may be made for the provision of access, by reference to a registered medical practitioner.[126] This is similar to the arrangements in place under section 31 (4) of the FOI legislation for public sector agencies, in which case reference is made to the information having an 'adverse effect' on the applicant's physical or mental health. Note that, at present, under the Private Hospitals Regulation 1996 access may be refused to either a patient or to his or her 'representative' – where access is judged to be 'prejudicial to the patient's physical or mental health' - but that the refusal can be appealed to the Director General of the NSW Department of Health.[127]

Amendment of health information: These requirements are in addition to HPP8 which provides that: (a) at the request of an individual, health information must be amended to ensure it is accurate and up to date; and (b) if the request for amendment is refused, then the an individual may further request that a statement of the amendment sought be attached to the information in question.

The additional requirements set out the manner in which a request for amendment is to be made (in writing and specifying the way in which the information is claimed to be inaccurate), as well as time limit for responding to a request (45 days)[128] and the grounds for refusing a request (basically if an organisation is satisfied that the information is accurate

123 Draft Health Records Bill, proposed section 33.

124 Draft Health Records Bill, proposed section 34.

125 Draft Health Records Bill, proposed section 31.

126 Draft Health Records Bill, proposed section 32.

127 Private Hospitals Regulation 1996, clauses 43 and 44.

128 Draft Health Records Bill, proposed section 35.

accurate and up to date, or if it is satisfied that 'the application contains matter that is incorrect or misleading in a material respect').[129]

Further requirements relate to the applicant's notation that may be added to a record where a request for amendment has been refused. For example, conditions are placed on the private sector organisation when it discloses the relevant health information to any other organisation (including public sector agencies): a statement must be given saying, first, that the individual to whom the information relates claims it is inaccurate or out of date and, secondly, setting out particulars of what is said in the notation.[130]

5.13 Private sector organisations - complaints

As noted, complaints in relation to public sector agencies may be dealt with under the mechanisms provided by Part 5 of the NSW Privacy Act,[131] notably the requirement to conduct an internal review. This means that the mechanisms in Part 6 of the Draft Bill would apply only to the private sector.

Proposed under the Draft Bill is a scheme where complaints are received,[132] assessed[133] and dealt with by the NSW Privacy Commissioner who may: seek to resolve the complaint by conciliation; make further investigations and report on the complaint; or determine that the complaint has been resolved.[134] Where the NSW Privacy Commissioner has reported on a complaint, the outcome can be appealed to the Administrative Decisions Tribunal which has a range of actions open to it, including ordering the respondent organisation to pay compensatory damages of up to $40,000 (the same maximum as operates for the public sector under the NSW Privacy Act).[135]

Two comments can be made. One is that, while the internal review strategy may be appropriate for public sector agencies with all the bureaucratic resources at their disposal, it would not seem appropriate for the private sector where very different resource implications may apply. Secondly, with similar considerations in mind, it may be that different maximum levels of compensatory damages should apply to the public and private sector, especially perhaps to health service providers who would qualify as small business operators.

---

129 Draft Health Records Bill, proposed section 36.

130 Draft Health Records Bill, proposed section 37.

131 But note that an alternative mechanism, based on conciliation by the NSW Privacy Commissioner, can also be pursued under that Act.

132 Draft Health Records Bill, proposed section 44.

133 Draft Health Records Bill, proposed sections 45 and 46.

134 Draft Health Records Bill, proposed section 47.

135 Draft Health Records Bill, proposed section 59 (1)(a); *Privacy and personal Information Protection Act 1998* (NSW), section 55 (2)(a).

5.14 The NSW Privacy Commissioner – codes, guidelines and referrals

The Privacy Commissioner is central to the enforcement and operation of the proposed scheme. One example is that the Commissioner must be consulted about the making of any code of practice before it is submitted to the Minister for approval. This arrangement is equivalent to that operating under the NSW Privacy Act. In both cases it is the Minister, not the Privacy Commissioner, who has the power to veto a code which modifies the application of either a HPP or IPP (Information Privacy Principle).[136] Similarly, under the Draft Bill it is the Privacy Commissioner who issues any relevant guidelines, but he or she does so with the Minister's approval.[137]

Among the powers granted to the Privacy Commissioner in the Draft Bill is to refer, in appropriate cases, complaints to other bodies, notably the Health Care Complaints Commission and, to avoid jurisdictional controversies, the Commonwealth Privacy Commissioner.

A point of comparison to make with the position in Victoria is that there the newly established Privacy Commissioner's Office does not handle health information complaints. Instead, these are to be dealt with by the Health Services Commissioner.

5.15 The HPPs and NPPs compared

HPPs 1-4 (collection): These constitute a reformulation of NPP 1 (collection). The difference is that under the HPPs the various facets of the collection process are separated out, making it easier to identify how the principles are to operate in practice.

Comparison with the Federal scheme is complicated by the fact that NPP1 must be read alongside NPP 10 (sensitive information). While NPP 1 does require an organisation to make an individual aware of certain access rights and other matters, it does not state expressly that personal information must be collected with the individual's consent. On the other hand, NPP10 does state expressly that 'sensitive information,' including health information, must be collected with the individual's consent. However, various exceptions apply, some operating only in respect to health service providers, others more generally to 'organisations' that collect health information for research or statistical purposes. One

136 The issue is discussed in G Griffith, n 56, pp 29-30. A Legislative Council amendment to the Privacy and Personal Information Protection Bill 1998 granted the Privacy Commissioner the power to ensure that a code could only exempt a public sector agency from compliance with an IPP 'if the Privacy Commissioner is satisfied that the public interest in allowing the exemption outweighs the public interest in the agency complying with the principle'. The effect of this would have been to place the privacy Commissioner, not the Attorney General, in a position where he/she could veto a code of practice. In the parliamentary debates this was said to be consistent with the position in other privacy regimes, including New Zealand, Hong Kong and the UK. The amendment was opposed by the Government and its view prevailed.

137 Draft Health Records Bill, proposed section 70 (4)(e).

exception is where collection without consent is necessary for *'the management, funding or monitoring of a health service'*. Certain conditions apply, but basically this appears to offer a broad area of exception from the 'consent' requirement to hospital and other health managers, as well as to such funding bodies as private health insurance companies.

HPPs 1-4 do not make consent a condition of collecting health information. Like NPP 1 it sets out instead various matters an individual is to be made aware of 'at or before the time' the information is collected, or if that is not practicable, 'as soon as possible after that time'. The exceptions to these requirements are then set out in HPP 4.3. Included is an exception where 'the organisation is lawfully authorised or required not to comply with it'. This would incorporate any rights and privileges of an organisation under the Federal Privacy Act and could therefore be said to cover any problems of direct consistency that might arise between the State and Federal regimes, but only, it should be said, to the extent that the State regime sets higher privacy standards than its Federal counterpart.

But note in this respect that the higher standard of 'consent' is established federally under NPP 10.1. Is it a problem in this context that the Draft Bill does not mirror that requirement? Does the potential for 'direct inconsistency' with the Federal Privacy Act, as that term was explained earlier in this paper, arise here? Federally, an organisation could be required to obtain consent, while at the State level it would be sufficient to make the individual aware of the matters set out in HPP 4.3.

HPP 5 (retention and security): This is basically a more detailed formulation of NPP 4 (Data security) which establishes the requirement to protect personal information in broad terms.

HPP 6 (information about health information held by organisations): Again, this is a more detailed formulation of the principle of 'openness' established in NPP 5.

HPP 7 and 8 (access and correction): These correspond to NPP 6 (access and correction), only in this instance the detail of the proposed NSW scheme is set out in Part 4 of the Draft Bill, 'Additional health privacy principles for private sector'. These were discussed in an earlier section of this paper.

HPP 9 (accuracy): This is a re-statement of NPP 3 (Data quality) which establishes an organisation's duty to take reasonable steps to ensure the accuracy of the data it holds.

HPPs 10 and 11 (limits on use and disclosure of health information): Federally 'use and disclosure' are covered under NPP 2. However, for its operation in respect to health information it must be read alongside NPP 10 (sensitive information). Under NPP2.1(a), the rule is that sensitive information (including health) cannot be used or disclosed for anything but the primary purpose for which it was collected, or for *directly* related secondary purposes if these fall within the reasonable expectations of the individual. By way of an exception to this rule, health information can be used or disclosed in other ways if the individual gives consent (whether express or implied), or if an exception applies under NPP 2.1(d). The exceptions include, but are not limited to, uses or disclosures required or authorised by law, those necessary to prevent or lessen a serious or imminent threat to

someone's life, health or safety, or for research provided certain conditions are met.

To a large extent HPPs 10 and 11 cover the same ground as their Federal counterparts. One difference between the HPPs and the NPPs is that the former are in more detail. A second is that the HPPs are probably easier to understand, if only because their intended application to health information does not have to be disentangled from a scheme covering personal information generally.

Consistent with NPP 2.1, HPPs 10 and 11 stipulate that health information is not to be used or disclosed for a purpose (a secondary purpose) other than the purpose (the primary purpose) for which it was collected unless, for example, the individual has consented to such use, or the secondary purpose is 'directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose'. Take, for instance, the collection of a blood sample from a baby at birth for the purpose of testing for a particular illness or disease. The mother's consent might be attained for its use or disclosure for another purpose, otherwise the 'direct purpose' test would have to be satisfied.

In fact, 'consent' and 'direct relation' are just 2 of 12 grounds under which health information can be 'used' for a purpose other than the primary purpose for which it was collected. As in the Federal scheme, 'research' is one ground of exception; 'law enforcement' another.

Areas where the Draft Bill deviates from the Federal scheme are as follows:

- Certain conditions apply, but both HPP 10 and HPP 11 make an exception for information used or disclosed for the secondary purpose of the 'Management of health services'. This relates to 'the funding, management, planning or evaluation of health services'. Is it on this basis that a private hospital would be permitted to disclose health information to a funding organisation, such a private health insurance company? It begs the question, is individual consent required for this to occur under the Federal scheme?[138]
- Again, subject to certain conditions, both HPP 10 and 11 make an exception for information used or disclosed for the secondary purpose of 'Training' (of an organisation's employees). This clearly contradicts the Federal scheme, with the Federal Privacy Commissioner's Guidelines stating that the use of information for training and education will 'usually require the individual's consent'.[139]
- Unique to HPP 11 is that health information may be disclosed to an immediate family member of the individual for 'compassionate reasons'. This is broader than the provision in NPP 2.4 for the disclosure of information 'to a person who is responsible for the

138 Office of the Federal Privacy Commissioner, n 90, p 17. It is clear the use of health information for fundraising activities by a private hospital is prohibited under the Federal regime.

139 Office of the Federal Privacy Commissioner, n 90, p 16.

Again these deviations may amount to differences, not direct inconsistencies, for constitutional purposes. As noted, NPP 2.1(g) makes an exception for health information where 'the use or disclosure is required or authorised by or under law'. 'Law' in this context would include State legislation and, from this, the argument has been put that State legislation would remain valid in so far as it *extended* the categories of disclosure permitted by the NPPs.'[140] This appears to be what is at issue under HPPs 10 and 11.

HPP 12 (identifiers): This is consistent with NPP 7 (identifiers), the key purpose of which is to prevent private sector organisations from adopting the identity numbers used by government agencies. Under the Draft Bill such an adoption may occur with the consent of the individual concerned. One might ask whether the more stringent requirement of obtaining the 'express' consent of the individual would be appropriate in this circumstance? At issue here is not consistency with the Federal Act, but the general question of the appropriate standard to be set in these circumstances so that individuals are clear about where consent has and has not been given.

HPP 13 (anonymity): This is in the same terms as NPP 8 (anonymity).

HPP 14 (transborder data flows): This mirrors NPP 9 (transborder data flows) except of course it is concerned with data flows outside NSW.

HPP 15 (linkage of health records): As noted this is unique to the Draft Bill and clearly picks up on one of the major policy reasons behind its formulation, namely, the development of linked electronic health records. HPP 15 prevents the creation of linked electronic health records without the *express* consent of the individual to whom the information relates. Certain exceptions apply, including where an organisation creates a health records linkage system 'to which only related bodies corporate of the organisation have access and which is for the benefit of [sic] individual'.

The above requirement for 'express consent' goes beyond what is required under the Federal regime, but again any problem of constitutional inconsistency is resolved by the inclusion of a clause stating that an organisation is not required to comply with the provision if 'lawfully authorised or required not to comply'. This would incorporate any rights and privileges of an organisation under the Federal Privacy Act.

5.16 Comments

There are sure to be differing perspectives on the Draft Health Records Bill. From one standpoint, it could be seen as yet another level of duplication and complexity in an area which is already busy with regulation. One area of complexity is the retrospective operation of the access and amendment rights, in relation to which health service administrators would be required to comply with different standards for State and Federal privacy purposes. Other issues include the potential costs to business and the possible confusions for consumers

140 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *The Sydney Law Review* 5 at 35.

faced with overlapping laws and separate complaints mechanisms. It could be argued that the prospect under the Draft Bill is of a multiplicity of laws, codes, guidelines and complaints mechanisms, making consistency as hard to achieve as intelligibility.

From another perspective, it could be said that the Draft Health Records Bill, like its Victorian counterpart, demonstrates the value of bringing public and private health sector privacy regulation under a single piece of legislation. As noted, this was a particularly contentious issue for the Federal private sector privacy law. The claim was made that, owing to the unique inter-relationship between the public and private sectors in the health field, that this is one area where such a dedicated industry-wide approach is required. That was the view taken by the House of Representatives Legal and Constitutional Affairs Committee. It might be argued that the difficulty involved in disentangling the operation of the provisions relating to health information from the remainder of the Federal privacy laws only serves to confirm that view. That is not to say that the House of Representatives Committee recommended the passing of distinct health privacy laws at the State level. On that point, however, it is the case that the provision of health service is largely a State responsibility and State involvement, legislatively and otherwise, could be said to be as desirable as it is inevitable. At any rate, it is clear that any single, industry wide legislative scheme must involve the States in some way.

On behalf of the Draft Bill, the contention can be made that it is a clear, yet detailed, formulation of the issues at stake in the health privacy debate. These might be counted notable virtues in themselves in such a complex area of the law. If not perfect, the Draft Bill is an example of the advantages produced by federalism in that, from a drafting standpoint, it allows a jurisdiction to learn from, and improve on, the legislative models already developed nationally, or in other States or Territories. If there is little realistic chance of the Draft Bill being used as a template for legislation in all the Australian jurisdictions, it might at least be a template for the National health Privacy Code which the Health Information Privacy Working Group is formulating at present. Instead, then of acting as a force for complexity, the Draft Bill might be seen as an agent working for a consistency of approach across the Australian jurisdictions.

Whatever one may think of that prospect, the issue of constitutional consistency is of pressing interest for the Draft Bill. The matter has been raised at many points in this paper. It has been suggested that, despite contrary indications expressed by the Federal Privacy Commissioner, that the 'covering the field' test of inconsistency may not apply in this context. As to questions of 'direct inconsistency', these are highly technical in nature and any attempt to second guess what a court might decide in a particular case would be something of a victory for temerity over prudence. That said, the obvious area of potential direct inconsistency as between the Draft Bill and the Federal Privacy Act relates to employee records. These are exempt from the Federal scheme, but would be covered under the Draft Bill, at least to the extent that health information is collected on such records. The potential for inconsistency may be very real in this context and, for this reason, this is one area where it is understood that the Draft Bill may be amended before it is introduced into Parliament.

It is in the nature of exposure drafts that they are likely to be altered, if only for fine tuning. When the Federal *Privacy Amendment (Private Sector) Act 2000* was being debated and

reported upon, considerable attention was paid to the many exceptions it included. The same was true of the NSW Privacy Act. As to how broadly or narrowly exemptions should be drawn in the field of health information, privacy advocates, on one side, and governmental officials, on the other, are unlikely to agree. Whether amendments are made in this respect, significant or otherwise, to the Draft Bill remains to be seen.

6. CONCLUSION

Much of the foregoing discussion has revolved around the complexities involved in establishing concurrent State and Federal health privacy regimes. It is the case that concurrent Federal and State regimes already operate in certain areas, apparently with reasonable success, one area being anti-discrimination legislation, another trade practices or fair trading laws. The question is whether this is the most appropriate model for health privacy.

Participants in the health privacy debate are sure to hold contrasting perspectives on this and other issues raised in this paper. Without claiming to definitively answer the many questions at stake, an objective observer might want to place the following propositions at the centre of that debate. One, that privacy legislation is of the utmost importance in a world where the electronic linkage of data is certain to result in the centralisation and accessibility of personal information. Two, that the case for adequate health information privacy legislation is especially strong. Three, that in respect to health information a particularly good argument can be made on behalf of a dedicated piece of legislation providing industry wide regulation, covering the public and private sectors. Four, that the same privacy standards should apply to both sectors. Five, that the same standards should apply in all Australian jurisdictions. Six, that the leading role played by the States in the provision of health services makes their involvement in any ‘national’ schema essential. Seven, that consideration should be given to the development of a consistent approach either by means of template legislation, or through a National Code of Health Information Practice. Eight, that the content of any health privacy law or code must be set out in clear and accessible terms, so that administrators and patients alike will be able to understand their rights and obligations. Nine, that consideration be given to a consolidation of the law relating to medical research and privacy. Ten, that the effectiveness of any schema will depend to a large extent on the operation of a properly resourced complaints and enforcement mechanisms.

APPENDIX A
Office of the Federal Privacy Commission Information Sheet 10 – 2001 Application to the Privacy Acts to Information Already Held

INFORMATION SHEET 10 - 2001 Application to the Privacy Act to Information Already Held

When the new private sector amendments to the *Privacy Act 1988* (Cth) (the Privacy Act) come into force on 21 December 2001, not all the National Privacy Principles (NPPs) will apply to information that private sector organisations have already collected. Section 16C of the Privacy Act sets out which NPPs will apply regardless of when the information was collected, and which NPPs will only apply to information collected after the private sector amendments commence.

Starting date of private sector provisions

The private sector provisions will take effect for different organisations at different times. This table explains when the provisions are due to take effect.

Type of organisation	**Start date**
Organisations with an annual turnover of more than $3 million. Health service providers regardless of turnover. Organisations with an annual turnover of $3 million or less that opt in to coverage.	21 December 2001
Organisations with a turnover of $3 million or less • that trade in personal information • are Commonwealth government contractors. (See *Information Sheet 12 – 2001 Coverage of and Exemptions from the Private Sector Provisions* for more detail.)	21 December 2002
Other small businesses with a turnover of $3 million or less.	The Privacy Act does not apply.

When each NPP applies

Only some of the NPPs apply to personal information that an organisation has already collected at the time the private sector provisions come into effect. The table below sets out, for those organisations covered by the Privacy Act, whether the NPP applies to information already collected and when each NPP will apply.

NPP	**Topic**	**What information the NPP applies to**
NPP 1	Collection	Only applies to information collected after 21 December 2001 (or for small businesses (not health services) applies to information collected after 21 December 2002).
NPP 2	Use and disclosure	Only applies to information collected after 21 December 2001 (or for small businesses

ISBN 1-877079-31-6

		(not health services) applies to information collected after 21 December 2002).
NPP 3	Data quality and collection	As it applies to collection it only applies to information collected after 21 December 2001 (or for small businesses (not health services) applies to information collected after 21 December 2002).
NPP 3	Data quality on use and disclosure	As it applies to use and disclosure it applies regardless of when it was collected (for small business (not health services), delay in application until 21 December 2002, then applies regardless of when collected).
NPP 4	Data security	Applies regardless of when information was collected (for small business (not health services), delay in application until 21 December 2002, then applies regardless of when collected).
NPP 5	Privacy policies and openness	Applies regardless of when information was collected (for small business (not health services), delay in application until 21 December 2002, then applies regardless of when collected).
NPP 6	Access and correction	If information already held is not used or disclosed it only applies to information collected after 21 December 2001. But if information already held is used or disclosed after commencement then rights of access and correction apply unless: • there is an unreasonable administrative burden; or • it will cause the organisation unreasonable expense (or for small businesses (not health services), applies to information collected after 21 December 2002, with no exception).
NPP 7	Commonwealth Government identifiers	Applies regardless of when information collected (for small business (not health services), delay in application until 21 December 2002, then applies regardless of when

ISBN 1-877079-31-6

		collected).
NPP 8	Anonymity	Only applies to information collected after 21 December 2001 (for small businesses, only applies to transactions entered into with an organisation after 21 December 2002).
NPP 9	Transborder data flow	Applies regardless of when information collected (for small business, delay in application until 21 December 2002, then applies regardless of when collected).
NPP 10	Collection of sensitive information	Only applies to information collected after 21 December 2001 (or for small businesses (not health services), applies to information collected after 21 December 2002).

About Information Sheets

Information sheets are advisory only and are not legally binding. (The NPPs in Schedule 3 of the *Privacy Act 1988* (Cth) (the Privacy Act) do legally bind organisations.)

Information sheets are based on the Office's understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and good practice or compliance tips. They are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation.

Nothing in an information sheet limits the Federal Privacy Commissioner's freedom to investigate complaints under the Privacy Act or to apply the NPPs in the way that seems most appropriate to the facts of the case being dealt with.

Organisations may also wish to consult the Commissioner's guidelines and other information sheets.

Office of the Federal Privacy Commissioner

www.privacy.gov.au

Privacy Hotline 1300 363 992 (local call charge)

December 2001 Office of the Federal Privacy Commissioner

ISBN 1-877079-31-6