Australian Government

Department of Health and Ageing

Ms Kelly Paxman
Acting Committee Secretary
Legal and Constitutional References Committee
Australian Senate
Parliament House
Canberra ACT 2600

Dear Ms Paxman,

SENATE INQUIRY INTO THE *PRIVACY ACT 1988* (Cth)

I am writing to provide you with a copy of the Australian Government Department of Health and Ageing's submission for inclusion in the Senate Legal and Constitutional References Committee's report on the Inquiry into the *Privacy Act 1988* (Cth) (see attached).

The submission addresses each of the issues raised in the Terms of Reference available on the Committee's website at www.aph.gov.au/senate_legal.

To assist the Committee in the compilation of the Inquiry a copy of the Department's submission together with a copy of this letter will be forwarded by e-mail to **legcon.sen@aph.gov.au**. I have no objections to the submission being published on the Senate Committee's website under the name of 'The Australian Government Department of Health and Ageing'.

In the interim, should you or any member of the Senate Committee require any further information, please contact Mr Paul Fitzgerald, Assistant Secretary, Health Information Policy Branch on (02) 6289 5744 or 0412 178 957.

Yours sincerely

Philip Davies
Deputy Secretary

March 2005

MDP 84 GPO Box 9848 Canberra ACT 2601
Telephone: (02) 6289 8400 Facsimile: (02) 6285 1994

Australian Government

Department of Health and Ageing

SUBMISSION TO THE AUSTRALIAN SENATE

LEGAL AND CONSTITUTIONAL REFERENCES COMMITTEE

INQUIRY INTO THE PRIVACY ACT 1988 (Cth)

Australian Government Department of Health and Ageing

February 2005

For further enquiries regarding this submission, please contact:

Assistant Secretary
Health Information Policy Branch
Information and Communications Division
GPO Box 9848
CANBERRA ACT 2601

Tel: (02) 6289 5744
Fax: (02) 6289 8295

TABLE OF CONTENTS

Executive Summary

On 9 December 2004, the Senate referred the *Privacy Act 1988* (Cth) to the Legal and Constitutional References Committee, for inquiry and report by 30 June 2005.

This submission by the Australian Government Department of Health and Ageing (including input from the Therapeutic Goods Administration) is provided in response to the Inquiry's Terms of Reference, namely.

(a) the overall effectiveness and appropriateness of the *Privacy Act 1988* as a means by which to protect the privacy of Australians, with particular reference to:

  (i) international comparisons;

  (ii) the capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy, including:

    (A) 'Smart Card' technology and the potential for this to be used to establish a national identification regime;

    (B) biometric imaging data;

    (C) genetic testing and the potential disclosure and discriminatory use of such information, and

    (D) microchips which can be implanted in human beings (for example, as recently authorised by the United States Food and Drug Administration); and

  (iii) any legislative changes that may help to provide more comprehensive protection or improve the current regime in any way;

(b) the effectiveness of the *Privacy Amendment (Private Sector) Act 2000* in extending the privacy scheme to the private sector, and any changes which may enhance its effectiveness; and

(c) the resourcing of the Office of the Federal Privacy Commissioner and whether current levels of funding and the powers available to the Federal Privacy Commissioner enable her to properly fulfil her mandate.

While, in the absence of an issues paper, the extent or direction of the Senate's interests in the range, detail and complexity of health issues under the Terms of Reference for this Inquiry is unclear, general comments regarding the application of the Privacy Act to Australia's extremely complex health care system and health service provision have been made.

In particular, the submission highlights the need within the health sector to strengthen Australia's existing privacy regime through the introduction of a nationally consistent health privacy code. The Department supports the introduction of the proposed National Health Privacy Code – a joint Commonwealth, State and Territory initiative in line with what has been agreed at the Australian Health Ministers' Advisory Council and Australian Health Ministers' Conference - as a means of providing strong and effective regulation for the handling of health information in both the public and private sectors.

The Department would also be supportive of amendments to the Privacy Act that:

- further clarified for both researchers and consumers how personal health information may be used for secondary purposes – there is evidence that the coexistence of the NHRMC Guidelines under section 95 and section 95A of the Privacy Act is creating some confusion for these two groups and compromising the research and health care that could otherwise improve outcomes for both individuals and public health;

- allowed for penalties for breaches of privacy given the highly sensitive nature of personal health information;

- ensured there were consistent complaints mechanisms for breaches of privacy across jurisdictions and the public and private sectors;

- allowed for the collection of an individual's family history under the National Privacy Principles; and

- allowed for deceased persons who have been dead for 30 years or less to come within the scope of the Act, as proposed in the National Health Privacy Code.

Introduction

'Health' information is defined under section 6 of the Privacy Act as an:

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, or intended donation, by the individual of his or her body parts, organs or body substances.

Under the same section it is also defined as a specific type of personal information - 'sensitive information about an individual'.

As such, personal health information must be afforded the highest privacy protection available. However, deciphering who has the right to access health information about an individual and what they are allowed to know under Australia's current privacy regime can be challenging.

A. Overall effectiveness and appropriateness of the Privacy Act 1988

Complexity of the health privacy landscape

One of the main issues for health care providers, health care consumers and data custodians (record keepers) in the management of privacy in the health sector is the complex interconnecting web of privacy protections in place.

The existing privacy regime has several levels:

- at one level, there are the common law confidentiality duties involved in the provider-patient relationship, as well as ethical and professional obligations (i.e. codes or practice and professional service charters) relating to these issues;

- at the federal level, Commonwealth and ACT government agencies must not only comply with the 11 Information Privacy Principles set out at section 14 of the Privacy Act but also other laws that govern the disclosure of information about a person obtained in course of duties as set out in their own specific legislation. Officers working in the health portfolio must consider the Information Privacy Principles in conjunction with, for example, the secrecy provisions of relevant health legislation, in particular section 130 of the *Health Insurance Act 1973* (Cth) and section 135A of the *National Health Act 1953* (Cth) and section 86-2 of the *Aged Care Act 1997*; and

- at the State/Territory level, most governments also have their own arrangements in place. For example, Victoria has legislation in place the *Health Records Act 2001* which aims to cover both the public and private sectors in that State and which is substantially similar to the National Privacy Principles provisions of the Privacy Act. NSW too, has similar legislation in place the *Health Records and Information Records Privacy Act 2002*.

Due to this myriad of arrangements in place, complexities arise when services are delivered through a mix of private and public sector providers across both private and public sector sites and between jurisdictions.

For this reason, the Department supports the introduction of uniform, nationally consistent rules for the handling of all health information – National Health Privacy Principles as outlined in the proposed National Health Privacy Code. At the request of Health Ministers, the National Health Privacy Working Group was set up in 2000 to oversee the development of a national framework for health privacy. The proposed Code is the result of this framework that aims to:

- safeguard the health privacy and dignity of all individuals;

- achieve national consistency in health privacy protection - across jurisdictions and between the public and private sectors; and

- take into account changes in the way personal health information is handled as a result of technological change.

Further comment on the Code is made at p14 of this submission.

i) International comparisons

Unlike Australia, some overseas countries have already adopted uniform, nationally consistent principles for privacy protection across jurisdictions. The most obvious example is the member states of the European Union whose Council of Ministers agreed to formally adopt the *European Union (EU) Directive on Data Protection* on 25 July 1995. The European Union Directive seeks to protect harmonise privacy protection across member states and trading partners (such as Australia, US and Canada) by:

- establishing legal principles for privacy protection to be enacted in all member states; and

- prohibiting the transfer of personal information from an EU country to any country which does not have adequate privacy laws in place.

It remains unclear at this stage, whether the Directive will affect the transfer of personal health information between Australian and European countries with regard to personal health information.

The Department has, however, had ongoing exposure to privacy policy issues connected with the international exchange of data and information most recently connected to the agreement between the Government of New Zealand and the

Government of Australia for the establishment of a joint scheme for the regulation of therapeutic products.

In December 2003 Australia and New Zealand signed a Treaty to adopt a joint scheme for the regulation of therapeutic products, to be administered by a single Agency (the Agency) in both countries. The Therapeutic Goods Administration is currently working with the New Zealand Medicines and Medical Devices Safety Authority (Medsafe) on legislation to implement this joint regulatory scheme.

The Treaty provides that the Agency is to remain no less accountable to the individuals and governments of both countries than similar agencies of either country. In the privacy context, this means that Australians and New Zealanders will be able to complain of a breach of privacy by the Agency under the Privacy Act of their own country. Therefore the Agency will need to comply with the requirements of both Privacy Acts.

The development of the privacy arrangements for the new Agency has not brought to light any gaps or deficiencies in the Australian *Privacy Act 1988*, but the Committee may still wish to compare it with the New Zealand *Privacy Act 1993*. Although the two Privacy Acts take substantially the same approach to the protection of personal information by government agencies, the two sets of Information Privacy Principles are worded differently and impose different levels of protection of information in certain circumstances.

For this reason, the Agency will put in place administrative arrangements that will ensure it provides the highest level of protection afforded to personal information by either the Australian or New Zealand Privacy Act and, where only one of those Acts imposes a particular requirement, the Agency also complies with that requirement.

Any moves towards making the Australian and New Zealand Information Privacy Principles more consistent would make it easier for the Agency (and indeed any future trans-Tasman Agency with the same approach to accountability) to determine the privacy requirements with which it must comply.

ii) New and emerging technologies

Having ready access to relevant health information is the cornerstone of good clinical care. However, existing paper-based records and legacy systems have meant that information is often kept locked away within organisational boundaries, leading to gaps in information flow across the health sector. Emerging information and communication technologies, such as electronic health record systems, offer new ways for accessing information silos allowing with consumer consent, the electronic exchange of clinical and provider information between health care providers.[1]

Technological change and the growing use of information and communications technologies to better manage health service information will have the most wide-ranging impact in reforming health service provision and improving the quality of care for consumers.

Such technologies can provide powerful tools in the health sector for increased collection, storage, transfer and analysis of personal information, thereby overcoming current gaps in information flow and improving overall quality and safety. At the same time, given the highly sensitive nature of personal health information, there need to be robust privacy measures in place both to ensure that personal privacy is not compromised and to enable the benefits to be fully realised for both individuals and the wider community.

To this end, Australian, State and Territory governments are investing in a number of e-health initiatives at the national level aimed at harnessing the potential of information and communications technologies to build a more effective and efficient health care system. At the same time, work is underway to ensure that all such initiatives are underpinned by appropriate privacy and security infrastructure.

To fully harness the benefits of new information technologies in the heath care sector, it is critical that the means are in place to ensure that the electronic exchange of clinical information is accurately and securely matched to the right individual. Failure to do so could result in clinical decision making being compromised.

[1] Health*Connect* Interim Research Report – Volume 1 Overview and Findings, p1

In this context, there has been growing recognition that a unique patient identifier is needed across the health sector as a key building block for the national e-health agenda. At the same time, it is also clear that, given the sensitivity of personal health information, any such initiative requires robust safeguards in place, particularly in terms of preventing function creep. At a minimum, providers and consumers will want to see measures in place that:

- restrict the use of health identification systems to the health sector;

- define permitted functions, with transparent processes in place to guard against function creep; and

- impose penalties for misuse of identifiers.

Major national initiatives relevant to the Senate Inquiry – and which are discussed in more detail below – include:

- the implementation of Health*Connect*, Australia's national health information network;

- the development of a Medicare smartcard as a secure means for identifying participants in Health*Connect*;

- work underway to investigate options for a national health identifier as a key building block for all e-health initiatives; and

- the development of a proposed National Health Privacy Code as the national set of rules for the handling of personal health information across the public and private sectors.

Health*Connect*

Health*Connect* is Australia's national health information network for the safe electronic collection, storage and exchange of clinical information among health care providers, subject to consumer consent.

It is a cooperative venture between the nine Australian, state and territory governments. Following three years research and development, including trialling in 3 jurisdictions, the Australian Government has committed $128m over four years to implement Health*Connect* nationally.

Whole of state implementation activities have commenced in South Australia and Tasmania, with regional expansion also underway in the Katherine region of Northern Territory. Additional Health*Connect* trials are also being established in Queensland and NSW.

It is recognised for Health*Connect* to be regarded by interested stakeholders as 'privacy enhancing' is dependent on:

- how the concept of privacy is promoted, addressed and built into the design process;

- how open, transparent and accountable related business processes are; and

- the extent to which consumers have a choice on how their health information is used.

For this reason, privacy protection is an integral component of Health*Connect*.[2]

Participation in Health*Connect* is voluntary for both consumers and providers and participants can also choose to withdraw at any time. Building on existing Commonwealth, State and Territory privacy legislation and the proposed National Health Privacy Code, strict privacy rules and protocols will be in place to ensure that

[2] http://www.abc.net.au/health/regions/cguides/healthpriv.htm

the individuals' records are only accessed on a 'need to know' basis – and only by provider organisations authorised by the consumer.

Smart card technology

Medicare smartcard

The Australian Government is investigating the role smartcards may have in ensuring accurate and safe identification of people participating in clinical e-health schemes such as Health*Connect*, which link and share information about an individual currently held in different parts of the health sector e.g. hospitals, general practice, laboratories, etc.

A new Medicare smartcard is being introduced in Tasmania in conjunction with the implementation of Health*Connect* in that state. The new smartcard was launched by the Minister for Health and Ageing on 28 July 2004.

In addition to supporting current uses of the Medicare card for payment of Medicare eligible services, the smartcard will hold a consumer identifier for Health*Connect*. The smartcard is voluntary. As well as having the functions of the current Medicare card, the smartcard is being tested as an access "key" for Health*Connect*-held information, ensuring individuals' records are matched to the correct person at all times. It will also enable consumers to authorise participating health care providers to access their Health*Connect* records.

The smartcard, which has the look and feel of the current Medicare card, contains a computer chip that will contain consumer information such as a Health*Connect* consumer identifier and basic demographic and possibly other patient information, if required. It will also enable consumers to establish or change their consent settings for Health*Connect*. There is no intention to store a consumer's complete health record on the card.

The use of the Medicare smartcard is governed by existing privacy protections for both Commonwealth agencies and private sector organisations, including the

Information Privacy Principles and the National Privacy Principles contained in the Privacy Act.

As required under NPP7 of the Privacy Act, contractual obligations will be used to limit collection, use and disclosure by private sector organisations of the Health*Connect* consumer identifier contained in the smartcard. Collection, adoption, use and disclosure of the Medicare number by private sector organisations will continue to be subject to NPP7.

There is no intention to widen the use of the Medicare smartcard or the Health*Connect* identifier beyond the health sector.

National health identifier

Health Ministers at their 29 July 2004 meeting, agreed in principle to develop a national health identifier. Work is now underway through the National E-Health Transition Authority (NEHTA) to investigate the business case and technical specifications for a national health identifier. The use of such an identifier would be limited to the health sector and will be underpinned by robust privacy arrangements, including possible legislation to prevent function creep.

Proposed National Health Privacy Code

The private sector provisions in the Privacy Act have made substantial progress in creating a culture of privacy across the private health care sector, including the need to balance the consumer's needs for privacy with the public's interest in having access to data for research and other secondary uses to benefit both individuals and their communities.

While the Privacy Act provides a platform for building a national privacy framework, the emergence of state privacy and health records legislation alongside the private sector provisions has created an increasingly complex set of arrangements and onus on private sector health professionals in understanding what their obligations are under the various regimes. This is likewise confusing for consumers who are unsure

which legislation applies under what circumstances. For example, how they can access their own health record and what charges they should pay.
The end result is a patchwork of public and private sector legislation, common law and codes of conduct governing the handling of health information privacy in Australia which in turn creates major problems for the future of e-health initiatives such as Health*Connect*. As a national network, Health*Connect* needs to have the same privacy rules in force across the private and public health sectors, and across all jurisdictions. This is particularly an issue in the health environment where individuals continually move between the private and public sectors and where providers will routinely deliver health care services in both sectors.

Under Health*Connect*, summary health information will potentially follow the consumer wherever and however they encounter health services. Information recorded in Health*Connect* will be then be downloaded, subject to the individual's consent, into the health service provider's electronic system. While Health*Connect* can make its own national policy rules, it will be of critical importance that robust privacy arrangements are in place to protect the information once it resides in providers' systems – and that these arrangements can be consistently applied wherever the information resides.

The co-existence of Commonwealth, state and territory health information privacy legislation has also created a significant burden on private sector health care services in understanding and meeting respective obligations, as well as confusion for health consumers affected by dual legislative instruments.

The existing inconsistency in privacy makes specific national projects such as Health*Connect* difficult to implement, as there is confusion about which principles apply and under what conditions.

This concern is shared by all Health Ministers as demonstrated by their commitment to the National Health Privacy Working Group charged with developing a national framework for the privacy of health information and the proposed National Health Privacy Code to underpin Health*Connect* and other e-health initiatives. Likewise, Departmental consultations with a number of stakeholders has revealed that there is

strong support for health specific privacy legislation - for example, the consultations relating to the proposed National Health Privacy Code and other consultations relating to Health*Connect*.

In the absence of a consistent set of national rules, the challenge for Health*Connect* implementation is to develop a single set of clear policies and procedures which complies with all relevant obligations and has universal application to all entities (whether public or private sector) and individuals in all Australian States and Territories.

Biometric imaging data

This Department has no plans to introduce an initiative that would permit the collection of biometric information. [3]

Designed essentially for identification and authentication purposes, proponents of the technology argue that biometrics allow the individual far greater control over access to computer systems and restricted sites when compared with user names and passwords – as they verify and authenticate biological traits that cannot be easily forged or passed onto other users. Looked at from this perspective, it would seem biometrics do have the potential to benefit the individual and could have privacy enhancing capabilities. However, it is equally clear that potential privacy risks posed by such technologies will only be prevented, if from the outset, privacy requirements are considered and addressed, prior to their implementation.[4]

It would appear however, that the Privacy Act would not be a limiting factor[5] if there was an identified need, as evidenced by a speech given by the former Federal Privacy Commissioner, Mr Malcolm Crompton in March 2002 entitled: *Biometrics and Privacy – The End of the World as we know it or the White Knight of Privacy?* The speech notes the range of claims made about the biometrics and privacy (from 'big

---

[3] Biometrics has been defined as 'the biological identification of a person, which includes characteristics of structure and of action such as iris and retinal patterns, hand geometry, fingerprints, voice responses to challenges and the dynamics of hand-written signatures.' Source: http://www.answers.com/biometrics&r=67

[4] Malcolm Crompton, the then Federal Privacy Commissioner, *Biometrics and Privacy – The End of the World as We Know it or the White Knight of Privacy*, Source: www.privacy.gov.au/news/speeches/sp80notes, p

[5] This statement is not intended to be a legal view and further legal advice should be sought.

brother' to 'white knight of privacy') and identifies and explores impacts on individual privacy through the collection and use of biometrics.

In his speech, Mr Crompton states that is '*nothing inherent in a biometric that would make it sensitive information under the Privacy Act.*'[6] Notwithstanding this, where biometric information is converted to an algorithm which accompanies personal information it is likely to be covered by the Privacy Act. If biometric imaging results in data that is not personal information then the current Privacy Act is unlikely to apply. If this is the case, some other regime to protect people in relation to the use of that data does need to be considered.

Genetic testing

The use of human genetic samples and information was the topic of a federal inquiry led jointly by the Australian Law Reform Commission (ALRC) and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council (NHMRC).[7] In summary, the ALRC and AHEC were asked to inquire into and report on whether, and to what extent, a regulatory framework is required to:

- protect the privacy of human genetic samples and information;
- provide protection from inappropriate discriminatory use of human genetic samples and information; and
- reflect the balance of ethical considerations relevant to the collection and uses of human genetic samples and information in Australia.[8]

As a result, privacy issues related to the handling and protection of human genetic samples and information have been well documented in:

- the Inquiry's Issues Paper 26 entitled *Protection of Human Genetic Information;*

[6] Crompton (March 2002), op.cit., p10

[7] Refer: Attorney-General and Minister for Health and Aged Care, 'Gene Technology', *Joint News Release*, 9 August 2000 and Attorney-General and Minister for Health and Aged Care, 'Genetic Privacy', *Joint News Release*, 7 February 2001.

[8] ALRC 96 *Essentially Yours: The Protection of Human Genetic Information in Australia*, March 2003 refer http://www.austlii.edu.au/au/other/alrc/publications/reports/96/1_Introduction.doc.html#fn1

- the Inquiry's Discussion Paper 66 entitled *Protection of Human Genetic Information*;
- the written submissions provided to assist Inquiry members advance advice on policy-making processes on this issue; and
- the final report ALRC 96 entitled *Essentially Yours: The Protection of Human Genetic Information in Australia*, tabled in federal Parliament in May 2003.[9]

In relation to the general question of privacy of genetic information, which would include the results of genetic testing, the Department indicated in its responses to the Discussion Paper that:

> The Department is of the view that human genetic information is part of a broader *continuum* of health and personal information. As with other forms of information, genetic information has predictive capacity for certain diseases and can provide information about related individuals. However, there is much more work to be done on the linkages between and relative impact of, environmental factors and genetics.

The Government is currently considering the Final Report of the ALRC/AHEC Inquiry and is likely to provide a whole of government response.

With respect to the discriminatory use of the information, the purpose of the current Act is to protect the privacy of information and not to prevent its discriminatory use. There is a range of legislation in force to cover discriminatory use of information.

The Privacy Act appears to protect the privacy of genetic information and ensure that the information could not be used for purposes other than those consented to, or otherwise defined by the Act.

Clause 2.1(e) of the National Privacy Principles states that an organisation can disclose personal information about an individual to another person where:

> *the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:*
>
> *(i) a serious and imminent threat to an individual's life, health or safety; or*

[9] Refer to ALRC site at: http://www.alrc.gov.au/inquiries/title/alrc96/index.htm.

(ii) a serious threat to public health or public safety; or

To ensure that the predictive nature[10] of genetic information is provided for, the Committee might consider recommending a provision similar to Clause 2.2 (i) of the proposed National Health Privacy Code that states (subject to certain conditions) personal information may be disclosed to another person where:

in the case of genetic information of an individual which is or could be predictive at any time of the health of another individual–

(i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to that other individual's life or health

This would allow for information to be disclosed where the threat is serious but not imminent.

Microchips for human use

On 16 October 2004, an article entitled: *Implantable Chips in Humans get the Nod* appeared in the Sydney Morning Herald reporting that the US Food and Drug Administration (FDA)[11] 'has given permission for humans to receive implantable electronic tags for computerised medical information'.[12]

Neither the Department nor the Therapeutic Goods Administration (TGA) is considering introducing a microchip for human use here in Australia, either at this present time or in the foreseeable future.

If a microchip is implanted in a person solely to enable the transmission of personal health information about that person to a third party, then it may not fall within the meaning of "therapeutic goods" as defined in section 3 of the Therapeutic Goods Act

---

[10] Predictive testing offered to asymptomatic individuals with a family history of a genetic disorder and a potential risk of eventually developing the disorder. Source: http://ghr.nlm.nih.gov/ghr/glossary/predictivetesting Predictive testing may be used for example, for cancers or neurological disorders that have genetic or familial associations.

[11] The FDA is an agency within the US Department of Health and Human Services.

[12] Refer http://smh.com.au/articles/2004/10/14/1097607372385.html?oneclick=true

1989 (the TG Act) as that definition hinges on the meaning of 'therapeutic use', also set out in section 3. In addition, it may not meet the definition of medical device in the TG Act (s 41BD). All these definitions centre, in part, on whether the particular item is for the diagnosis, prevention, monitoring, treatment or alleviation of disease.

If the particular microchip is not a therapeutic good (therapeutic goods include medical devices) then it would not be subject to regulation of its safety quality and efficacy under the TG Act.

However, it is emphasised that this conclusion is subject to being provided with further information about the precise nature and uses for a microchip, particularly the particular 'medical applications' it is used for. In some cases, it may well be that microchips can be characterised as being for the diagnosis, prevention, monitoring treatment or alleviation of disease.

iii) Changes that may help to provide more comprehensive privacy protection

Legislative changes

Research

The private sector provisions provide a good balance between protecting individual health information privacy while at the same time recognising that there are important public and individual benefits to be gained through secondary uses of personal health information for research.

Notwithstanding the benefits, the coexistence of National Health and Medical Research Council (NHMRC)[13] Guidelines under Section 95 and Section 95A of the

[13] The functions of the NHMRC come from the statutory obligations conferred by the *National Health and Medical Research Council Act 1992*. The Act sets down four statutory obligations on the directions taken by NHMRC. These obligations are to:

- raise the standard of individual and public health throughout Australia;
- foster the development of consistent health standards between the various States and Territories;
- foster medical research and training and public health research and training throughout Australia; and
- foster consideration of ethical issues relating to health.

The Council comprises nominees of Commonwealth, State and Territory health authorities, professional and scientific colleges and associations, unions, universities, business, consumer groups, welfare organisations, conservation groups and the Aboriginal and Torres Strait Islander Commission. More information about the NHMRC is available at http://www7.health.gov.au/nhmrc/aboutus/index.htm

Privacy Act 1988 has created some confusion both for researchers and consumers. Since December 2001, a range of NHMRC stakeholders have expressed concern that implementation and/or interpretation of Commonwealth and State privacy legislation is compromising research and health care that would otherwise improve outcomes for both individuals and public health. It has been suggested that this is an unintended effect of the privacy legislation and, more particularly, the private sector amendments to the Privacy Act.[14]

Penalties

Given the highly sensitive nature of personal health information, and the potential for personal and social harm that can arise from misuse of such information, there is strong support among consumer and provider groups for penalties for breaches of privacy. This has been borne out in the consultations carried out in relation to Health*Connect* and Medi*Connect*, as well as those concerning the proposed National Health Privacy Code.

Collection of family history

The collection of an individual's family history is an essential part of clinical care, as has been recognised by the Public Interest Determination made by the former Federal Privacy Commissioner, Malcolm Crompton. The Department recommends that this capacity be included in the NPPs.

Deceased persons

The Act only applies to living persons. The Department supports inclusion of deceased persons who have been dead for 30 years or less within the scope of the Act, as proposed in the National Health Privacy Code.

Other changes

Sub-contractor provisions

The provisions requiring Commonwealth sub-contractors to abide by the Information Privacy Principles and the National Privacy Principles is complex and confusing for sub-contractors – as borne out by the Department's experiences in the Medi*Connect*

[14] Campbell Research and Consulting. *The Impact of Privacy Legislation on NHMRC Stakeholders* July 2004.

Field Test whereby doctors and pharmacists were contracted to the Commonwealth. In addition to their existing privacy obligations under the Act, providers were required to comply with the Information Privacy Principles in respect of all personal information collected, used, disclosed or stored as part of the Medi*Connect* Field Test, to the extent that any existing obligations under the National Privacy Principles were inconsistent with the Information Privacy Principles, these were excluded during the conduct of the Medi*Connect* Field Test.

In the view of the Department, it would be much simpler and practicable to require private sector sub-contractors to abide by the National Privacy Principles.

Complaints

Privacy complaints mechanisms are inconsistent across jurisdictions, resulting in confusion for the health consumer. For example, under current processes, for a complaint against a private sector organisation, the consumer can make a complaint to the Federal Privacy Commissioner or, in the case of Victoria and NSW, to a State Privacy Commissioner. For a complaint against a public health sector organisation, the person can complain to a State/Territory health care complaints commissioner or a State/Territory privacy commissioner where one exists in that jurisdiction. As evidenced by the Health*Connect* trials and planned whole of state implementations, this results in somewhat unwieldy arrangements for all participants as well as those responsible for managing day-to-day operations.

Accordingly, the Department would prefer to see a more consumer-friendly approach for dealing with privacy complaints. One possibility could be for the OFPC to develop Memoranda of Understanding (MOUs) with health care complaints commissioners, within jurisdictions to enable more complaints to be dealt with locally.

B. Effectiveness of the *Privacy Amendment (Private Sector) Act 2000* in extending the privacy scheme to the privacy sector

With regard to the overall effectiveness and appropriateness of the Privacy Act, the Committee's work might usefully be informed by the Federal Privacy

Commissioner's recent review of the operation of the private sector provisions contained in the *Privacy Amendment (Private Sector) Act 2000* due to be provided to the Attorney-General of Australia, the Hon Philip Ruddock end March 2005 and to which the Department provided a submission (at Attachment A). The Privacy Commissioner was asked to consider the degree to which the private sector provisions met their objectives.

C. Resourcing of the OFPC

The Department has a portfolio-wide Memorandum of Understanding (MOU) with the Office of the Federal Privacy Commissioner (OFPC).

The MOU covering the period 1 July 2003 – 30 June 2005 has a total value of $736,726 (including GST). It provides funding support for two equivalent full-time staff within the OFPC to undertake research, analysis and provide advice on a range of activities relating to health information privacy. Projects that the OFPC is currently actively involved in advising on privacy arrangements are:

- Health*Connect*;
- Medicare Smartcard;
- review of 135aa guidelines; and
- proposed National Health Privacy Code.

The MOU is not meant to cover other OFPC core health privacy activities such as complaint handling, compliance, monitoring and education.

Parties to the 2003 – 2005 MOU include:

- Health Insurance Commission (an annual contribution of $124,875); and
- the Department's Health Information Policy Branch and National eHealth Systems Branch (both within Information and Communications Division).