Australian Medical Association Limited
ABN 37 008 426 793

42 Macquarie Street, Barton ACT 2600
PO Box 6090, Kingston ACT 2604
Telephone: (02) 6270 5400 Facsimile: (02) 6270 5499

Website: http://www.ama.com.au/

President: Dr William Glasson
Secretary General: Dr E Robyn Mason

THE AUSTRALIAN MEDICAL ASSOCIATION'S SUBMISSION

TO THE
LEGAL AND CONSTITUTIONAL'S
INQUIRY INTO THE *PRIVACY ACT 1988*

Submission prepared by:

Pamela Burton, BA; LLM, Legal Counsel
Dr Kate Stockhausen, Ph D, Senior Research Officer
On behalf of the Australian Medical Association Limited

22 February 2005

INDEX

1. OVERVIEW

The introduction of the *Privacy Act 1988,* particularly after the private sector amendments came into force and State and Territory privacy and health records legislation was enacted, has heightened corporate awareness of the individual's right to privacy.

However, it is clear that organisations in both the public and private sector have not always found it easy to apply the principles sensibly and effectively. For example, government bodies permitted by law to disclose certain sensitive information to health service providers, sometimes show little understanding of the limitations imposed on the private sector to lawfully collect it. The recent hiccups with the HIC's Prescription Shopping Information Service for use by doctors is an example of this, referred to further below.

An individual's personal information can be held across public and private sectors, and across the various Federal, State and Territory jurisdictions. There is a need for a comprehensive framework to ensure nationally consistent regulation of all health information whether held by the public or private sectors. At present some sensitive information is better protected or differently protected than other information depending on whether the organisation handling it is public or private, and on which State or Territory laws apply.

It is very difficult for medical practitioners and organisations that handle health information to comply with the public/private, Federal/State mishmash of regulation. This is being made more complex by emerging technologies.

Particularly problematic for health doctors is how to correctly store, transfer and dispose of health records in an environment of electronic record keeping. Complex software applications are needed to separate one patient's records from another. Patient records often include 'links' to information and resource materials, making it difficult to determine precisely what makes up 'the record'. Software applications often incorporate unsolicited 'pop-up' advertisements, for example on prescription choices, which, in the event that a doctor opts to prescribe the advertised product for the patient, raises the issue of whether the advertisement forms part of the record.

Potential risks to patient privacy arise in the collection, storage and transfer of patient information in an electronic environment in the absence of clear and consistent national standards. The recently introduced Smart Card that incorporates a consumer identification number without a clear statement of the use for the identification could threaten patient privacy. Concerns about privacy arise out of the emergence of biometric imaging data and microchip technology. The ability to undertake genetic testing of an individual has privacy implications for others. The use of new technologies has to be addressed in the privacy context.

The introduction of the *Privacy Amendment (Private Sector) Act 2000*, has particular implications for private medical practitioners.

The application of a 'one size fits all' privacy solution across all industries has posed difficulties for the health sector with its endless possibilities of complex medical/ethical situations that health service providers, and doctors in particular, face.

The legislative regime needs to be reviewed and amendments to the National Privacy Principles that apply to the private sector need to be made. The AMA's recommendations as to this are set out in this submission.

The 'mishmash' of uncoordinated health specific privacy legislation in most State and Territory jurisdictions and the generic Commonwealth *Privacy Act 1988* calls for a replacement set of nationally coordinated health specific privacy principles, or an overarching national health privacy code.

The AMA urges that privacy law be made uniform across the Australian jurisdictions for both the private and public sector, and that a health specific set of privacy rules be devised to enhance not hinder the public's health and well being.

Adequate resources need to be made available for the proper administration of national privacy laws.

2. THE OVERALL EFFECTIVENESS AND APPROPRIATENESS OF THE ACT AS A MEANS BY WHICH TO PROTECT THE PRIVACY OF AUSTRALIANS

(i) International comparisons

The AMA supports privacy rights being regulated by legislation. The common law is inadequate to guard the privacy of individuals. The AMA has not undertaken a study by way of international comparisons. However, we are aware that most western countries have statutory privacy regulation. We note the failure of the United States of America to join countries such as Canada, United Kingdom and Australia in mutual privacy obligations limits safe transborder data flow.

(ii) Capacity of the legislative regime to respond to emerging technologies

The developments in information and communication technology have made the community much more aware of privacy issues surrounding their health information and the potential for their privacy to be invaded. Issues of data linkage, particularly in the context of insurance and employment, are of increasing concern.

The community has reason to feel vulnerable to Government sanctioned data collection and linkage. For example, for many years, and throughout the development of different aspects of e-health in Australia, the Government has consistently 'sold' e-health as having an objective of improving health outcomes. Its focus on the access to electronic health information data for its own secondary, unrelated purposes, however, has at times overshadowed and undermined the credibility of its stated objective on health outcomes. Function creep and a low priority approach to the establishment of key building blocks in e-health to protect privacy has been a highlight of Government initiatives to date. Importantly, this impacts on confidence in and acceptability of electronic systems for both patients and providers.

Changes in information technology have had significant impact on the health sector. In particular, new technology permits access to a wide range of information that can contribute to improvements in the delivery of healthcare and health outcomes for patients. The ultimate development of a national electronic health record has the potential to provide the means to share an individual's health information for the purposes of their health care needs throughout their lifetime. Access to a reliable, historical record of an individuals' encounters with the health system throughout their lifetime can contribute to safety and quality in the delivery of health care, particularly as the patient moves in and out of different parts of the health system.

However, such systems also provide a source of data on individuals that has never before been available in a form that can be interrogated and linked so easily and so widely. This new environment, while creating the potential for significant positives in improving health care, has at the same time created significant potential risks to the privacy of individual health information and the independence of a medical practitioners' clinical decision making.

It is the AMA's view that the development in information and communications technology has created a significantly greater potential for privacy intrusion through data linking.

We now deal with some specific developments which are the subject of this Inquiry.

(A) Smart Card

The incorporation of a consumer identification number (CIN) embedded in a chip on the recently introduced Medicare Smart Card gives rise to growing concerns at the extent to which the Government could, for example, potentially link MBS and PBS and other data. As to this, the AMA has put a separate submission to the Office of the Federal Privacy Commissioner's Review of MBS and PBS Privacy Guidelines. In its submission the AMA urges that it is of great importance that the law, and the MBS and PBS Privacy Guidelines, continue to stringently protect the function separation of the two data bases as a means of protection against data linkage.

Further, the issuing of the Smart Card incorporating a CIN before the primary purpose, or any other purposes, for the CIN are defined for the use of the information to be collected from it, shows disregard at the Federal level for privacy protocol.

The Government announced the implementation of the Smart Card initiative, including functionality for a CIN without any consultation with the wider community. A stated purpose is fundamental to providing privacy protection related to the uses of such a number.

The implementation of any functionality for the Smart Card, particularly using the CIN, will have very significant ramifications for threats to privacy, particularly if requirements related to the functional separation of the PBS and MBS data are relaxed.

(B) Biometric imaging data

The AMA makes no special submission on biometric imaging data at this stage. However, the comments we make above about a Medicare Smart Card Consumer Identification Number, will apply if biometric imaging data is developed to incorporate a CIN that potentially link various data sets.

Malcolm Crompton states[1]:

> *Use of biometrics for identification has the potential to be more privacy invasive in cases where it involves the identifying organisation holding large amounts of information about individuals that it may or may not need, or that the individual may or may not know about.*

(C) Genetic testing

The Australian Law Reform Commission and the Australian Health Ethics Committee completed a joint inquiry into the Protection of Human Genetic Information and produced a comprehensive report entitled *Essentially Yours. The Protection of Human Genetic Information in Australia* (Report 96, March 2003). This addresses the issue of genetic information and health privacy law.

[1] "Biometrics and Privacy: The end of the world as we know it or the white knight of privacy?" Australian Journal of Forensic Sciences, 36:49-58, 2004

The report has not been responded to adequately by either the Attorney-General or the Commonwealth Department of Health and Ageing.

Genetic information is unique in that it is both personal as well as familial in nature. This means that although one's genetic information can reveal information regarding their own (past, present, and future) health, it can also reveal information that may be relevant to the health of their genetic relatives.

Although the AMA does not recommend at this time that it is more efficient to create specific genetic privacy legislation or that existing legislation could be amended to adequately incorporate and cover genetic information, it is imperative that a nationally consistent approach to the protection of genetic information, including genetic samples, be undertaken.

(D) Microchip implants

The AMA makes no special submission at this stage on the handling of information contained in microchip implants, other than to restate concerns raised above under the heads of "Smart Card" and "Biometric imaging data".

(iii) Legislative changes required to improve the regime

The AMA confines its comments and recommendations for changes to the general legislative privacy regime to the impact of the privacy legislation on the health sector and its patients. In the following section of this submission we outline the changes we see are required to the private sector provisions of the *Privacy Act* in the context of the provision of health services.

The AMA has long-urged that overarching health privacy legislation is vital to adequately and appropriately protect patient privacy. The development of the Australian Health Ministers' Advisory Council's (AHMAC's) National Health Privacy Code is an attempt to meet this need.

However, there is a need for changes to the legislative regime or as a minimum some amendments to the Act before the National Health Privacy Code (NHPC) is issued.

While the AMA is in favour of a single set of privacy principles for the health sector, we urge that the National Privacy Principles that apply to the private sector be amended before the NHPC is issued, so that the NHPC reflects any changes made to the legislation and incorporates privacy principles that work effectively in the health context.

Secondly, the Federal Privacy Commissioner, her Office and the community have been left in the dark about how such a Code (being health specific and covering Federal and State jurisdictions) constitutionally will fit into the current Federal privacy legislative scheme.

The relationship between the privacy legislation under review and the NHPC being developed by the AHMAC needs to be clarified. The status of the NHPC needs to be clear and agreed to.

3. THE EFFECTIVENESS OF THE *PRIVACY AMENDMENT (PRIVATE SECTOR) Act 2000*

The following submissions focuses on the application of the Commonwealth *Privacy Act 1988* as it applies to the private health sector.

The AMA submits that some amendments to the NPPs are required to enable these generic principles to be applied to the health sector in a manner that does not impede good ethical and clinical practice.

Good privacy practice should enhance and not hinder best clinical practice and optimal patient care. The paramount concern of doctors is the health care and well being of their patients.

(i) Current problems with the NPPs

(A) The concept of 'primary purpose'

The NPPs should allow collection of information to accommodate the aim of a doctor to provide proactive, preventative and holistic health care. This approach provides the doctors with the opportunity of explaining to patients how the information collected will be handled, and for the patients to indicate any special restrictions on the use of the information.

The NPPs currently restrict doctors from providing a continuum of care and holistic care by requiring a myriad of implied or specific consents from time to time. This is a product of a strict definition of the 'primary purpose' for which patient information is collected. That is, the current NPPs when applied to the health sector don't allow for the patient expectation that their doctor will take a whole person approach to their health care. The concept of 'primary purpose' in NPP 2 for the use and disclosure of personal information means that patient information is only collected for the single purpose of that episode of care.

The AMA submits that the concept of 'primary purpose' when applied in the context of health care should accommodate the meaning of 'the health care and well being of the patient', unless another meaning is specifically agreed to between the doctor and the patient.

The AMA argues that the doctor's professional and legal obligations do not permit the single 'primary purpose' of collection to be construed narrowly as being the purpose of diagnosis and treatment of a single presenting condition. This interferes with the delivery of holistic health care.

Difficulties have been demonstrated

The flaw in applying generic privacy principles to the doctor/patient relationship is well illustrated by the fact that the NPPs prevent doctors from taking family histories without the consent of the family members.

It became necessary for a Public Interest Determination (PID) to be issued. This PID provides for a compliance exemption and permits doctors to collect family and social histories. This PID needs to be made indefinite by incorporating the exemption in the NPPs.

In more recent times the Federal Government's initiative in establishing the HIC's Prescription Shopping Information Service was temporarily thwarted by the inability of doctors to collect such information without the consent of their patients.

A PID has been issued to permit such collection without the consent of patients. Interestingly, the PID does not exempt doctors from informing their patients that they are collecting this information from the HIC. Such notification is not required under the NPPs where that notification poses a 'serious threat to the life or health of any individual'. However, in the usual case, that is where the doctor fears that harm might occur, for example, that the patient might walk out and go to another doctor, the threshold test to dispense with notification is not met. The PID does not deal with this situation, although the HIC clearly intends doctors to access the Service when they have any suspicions about their patient's prescription request. This matter needs to be addressed.

Solutions

These problems would not arise if the holistic concept of 'primary purpose' for collecting information is accepted, and if exemptions to compliance were permitted by substituting the words 'possible harm to' for the words 'pose a serious threat to the life or health of an individual".

The AMA's detailed submission on this aspect of the NPPs is contained at **Attachment A**.

(B) Access to personal information

The AMA supports a person's right to access information held about them. However, patients' rights to access their information should take into account the potential for interference with the therapeutic relationship and patient harm. Again amendments are required so that the inappropriate threshold of posing 'a serious threat to the life or health of any individual' is lowered so that patient information can be withheld where access could cause patient harm or interfere with a treatment protocol.

The provision for patient access to their health records should incorporate exemptions where that access could cause patient harm short of posing a 'serious threat to the life or health of an individual" required by NPP.

There are occasions where access to clinical notes can cause harm to the patient or interfere with the therapeutic relationship. This poses a serious problem for doctors such as GPs and psychiatrists in particular, in the proper provision of mental health care. Further, NPP 6 fails to protect the doctor's private or preliminary views in the thinking processes required for full medical assessments, accurate diagnosis and the formulation of treatment programs, and patient access to these private notes exposes patients to less than optimal health care.

The AMA's detailed submission on this aspect of the NPPs is contained at **Attachment B**.

(C) Incorporating current PID exemptions into the legislation

The Public Interest Determinations relating to family and social histories, and to doctors collecting information from HIC's Prescription Shopping Information Service should be made indefinite by incorporating the exemptions into the legislation.

It has been recognised that doctors are required to take family and social histories from patients without necessarily obtaining the consent of the family member or other third party. A Public Interest Determination (PID) has been made accordingly. The AMA urges that the PID be incorporated into legislation, as the PID operates for a finite period of time only.

In the absence of making the PID indefinite or incorporating its intent into the legislation, patient health will be put at risk. Where doctors fail to take comprehensive medical histories, they are exposed to litigation if a failure to diagnose results from an inadequate medical, family or social history.

Doctors understand that such family history information will often be biased, limited, and of uncertain quality. However, the histories can often provide helpful indications that may be important to the health care of the patient being assessed.

In the mental health area, the collection of such information is also used to elucidate the nature of perceived family relationships between the patient and their family. The way in which the family history is told, and the emotional emphasis in the family history narrative, is important in understanding the patient in a holistic fashion. It is well understood by mental health professionals that such family history narrative will often have perceptual bias which is particular to the patient being assessed, and reveals more about the patient's attitudes and emotional make-up than information about the family members mentioned. Leaving aside the impracticalities of obtaining third-party consent, should the family member's consent be required, or should the family member access and correct the information, the value of the collected information would be lost.

The Government's explanation of the benefits of the HIC Prescription Shopping Information Service speaks for itself. The PID exemption, suitably extended to exempt doctors from notifying their patients, is necessary to permit doctors to lawfully collect that information and should also be incorporated into the legislation.

(D) Security of electronic records

National standards for the secure storage and transmission of electronic health information are required. This may require further resources to be allocated to the Office of the Federal Privacy Commissioner in order to give attention to the way of best monitoring and enforcing the provisions for security of electronic health records.

The AMA has consistently restated the need for significant patient safeguards in relation to consent in the setting of electronic health records. The push to make profits in GPs' practices bought by corporate interests raises the risk of inappropriate 'data-mining' of personal data for commercial purposes. Governments are sometimes inattentive about such issues and there is a

potential for data linking between government departments and agencies. The potential insecurity of information held on-line and the speed with which it can be disseminated are causes for concern.

The AMA makes three points in particular about electronic health records:

Firstly, there is an absence of national standards for the secure storage and transmission of health information in an electronic environment.[2] This is a matter than can only be addressed at the Federal level.

Secondly, stronger provisions and greater resources at the Federal level are required to properly address the security of electronic health records, and to prevent corporate misconduct for the on selling of health data. For example, questions arise about whether so-called de-identified material is genuinely de-identified, and how easily can it be re-identified.

Thirdly, the AMA is concerned that the Federal Privacy Commissioner is not represented on a range of key national electronic health initiative forums including those related to the National Electronic Health Transition Authority, the Australian Health Information Council and HealthConnect. The protection of privacy in an electronic environment is critical to the progress of such initiatives and covers a wide range of issues. The expertise of the OFPC should be available to all stakeholders through these forums.

Technology is not the barrier to the implementation of electronic health records. Policy issues around privacy have proven to be the most challenging. A failure to resolve these issues to the satisfaction of the medical profession and their patients represent a potential barrier to progress.

The key issues for the medical profession are:

- the capacity to adequately protect the privacy of their patients' health information; and

- that the procedures, processes and technical security requirements associated with protecting patient privacy in an electronic environment does not impinge on limited practice resources, particularly time/human resources, in an environment of workforce shortages and increasing patient demand.

In this context the OFPC can provide the necessary expertise to contribute to policy development around key issues including, the development and use of a national patient identifier, consent processes in an electronic environment, the purpose and uses of data collected by electronic means in health settings, data linkage, and importantly, a nationally consistent approach to privacy protection in an electronic environment. Key issues relating to whether systems or underlying fundamentals, such as the national patient identifier, should be opt-in or opt-out and proposals that an electronic health record 'enabler', the national health identifier, replace the functions of the Medicare number, are currently under discussion. Decisions in this regard will have significant implications for both doctors and patients. It is our view that the Federal Privacy Commissioner must participate in this debate.

[2] The NSW *Health Records and Information Privacy Act 2002* Act, for example, requires express consent by an individual before their health information is included in electronic health records. It also expands the definition of 'personal information' to deal specifically with personal genetic information.

The Federal Government has suggested that the *Privacy Act* will be amended to 'fit' with the proposed design of specific electronic systems. The electronic system design should not drive the privacy regime. Privacy of personal health information in an electronic environment must be developed and incorporated during design stages of electronic systems. The presence of the OFPC in these key forums will contribute to confidence of stakeholders that privacy has been a key element addressed throughout system and related policy development.

(E) Exemption of the Media

Amendments to the *Privacy Act* are also necessary to protect patient privacy from exposure to the media. The current media exemption to compliance with the private sector provisions of the Act should be reviewed.

The AMA recognises that freedom of speech and the right of the media to publish information must be protected. However, totally exempting the media from privacy law seriously undermines the protection given to individual privacy by the Act. It has been forcibly put to the AMA that the medical profession should not be treated any differently under privacy law to any other profession, notwithstanding that the application of some aspects of the generic privacy law conflicts with good clinical practice. Yet, a total exemption applies to the profession of journalism.

Mental health service providers are particularly aware of the impact on their patients of the media not being bound by the privacy laws. The media can report mental health matters and take photographs in a way that is stigmatising and invades patients' privacy. Information is too readily obtained from the police, who have a legitimate and lawful reason to collect it.

The reporting of admission of a person to a psychiatric hospital and of their treatment for an identified psychiatric illness, for example, not only invades the privacy of the person concerned but also that of other patients in the hospital. The media invasion of a particular facility in Sydney severely disrupted the delivery of clinical care and resulted in other patients avoiding admission because they were concerned about the risk of being photographed by reporters covering the story.[3]

The present situation puts public curiosity ahead of an individual's right to privacy. The media has not proved responsible in the regulation of their own conduct in this respect, particularly when reporting on the mental health of particular individuals that is often revealed in sensationalised media stories.

We seek that the exemption be removed, and that the media be subject to privacy law when dealing with personal health information of individuals, subject to appropriate exemptions to ensure that the public interest is properly served.

(F) Exemption of political organisations

The AMA also strongly urges that the exemption of political organisations from compliance with the Act in certain circumstances, be tightened.

[3] As reported by Dr Bill Pring, Chair, Mental Health Privacy Coalition, 18 February 2004

The *Privacy Act* exempts political organisations in wide circumstances from its ambit. Political organisations can breach a patient's confidentiality when that organisation determines it is in the public interest. This needs to be reviewed.

In their push to win voter support politicians can and do invade the privacy of individuals. The abuse of their leadership role in this respect devalues the importance of privacy law.

This abuse can occur outside the protection of parliamentary privilege. For example, a Federal Senator who is an anti-abortion campaigner gained access to a woman's medical records against her wishes. The woman had been a patient of the Royal Women's Hospital in Victoria where she had a termination of a 32 week-old foetus on health grounds. The Victorian Coroner's court had ruled it had no jurisdiction to inquire into the death of the foetus. The Senator sent the records to the Victorian Medical Board requesting an investigation into the conduct of the doctor who carried out the procedure. The patient was still receiving psychiatric treatment. She objected to her medical records being used and disclosed in this way. The distress caused to her could only exacerbate her poor state of health.

(G) Medical Research

The AMA is concerned about the narrow view taken under the NPPs of when consent for use of clinical data can be dispensed with, in the interests of medical research.

Research should be permitted under strict protocols where it is in the public interest, rather than patient data only being permitted to be used for medical 'Research relevant to public health or public safety'.

'Public health and public safety' should not be construed as referring only to such matters as 'communicable diseases' and 'polluted waterways'. Research that might improve the health of any one or more individual is relevant to public health.

A recent media report referred to cancer researchers complaining that they could not gain access to vital government-held information for studies into cancer and the workplace because of fears that releasing the data will breach the privacy law. Dr Richie Gun, a researcher at Adelaide University, is reported to have stated that the law was harming public health and he called for its overhaul. It also reported that Professor David Hill, of the National Health and Medical Research Council, said the privacy law had hampered attempts to build a road trauma registry as well as other health research.

A broadening of the narrow application of the exemption of research is required to reflect public interest requirements.

All appropriately approved medical research should be regarded as relevant to 'public health or public safety'. The exemption in NPP 10.3 to the requirement to obtain consent when it is 'impracticable' to do so should include when it is not viable (that is, so inconvenient or unprofitable that the research would be hindered).

All medical research is approved by a properly constituted ethics committee which follows guidelines developed by the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council of Australia. AHEC's *National Statement on Ethical Conduct in Research Involving Humans* is referred to the Minister for approval under the Council's enabling Act. It is then published by the Council and issued as Public Policy. It deals with matters of privacy as well as the range of other ethical matters relating to research. The Statement, amended from time to time, is drafted after a wide consultation process takes place in accordance with the Act. It is the key document under which all medical research takes place.

It is impractical (because of inconvenience and cost) to get consent from the thousands of patients for statistical purposes, and cruel when usually the consent needs to be obtained often just after the patient has received devastating news of their condition.

The narrow view taken of what is valid medical research for the purposes of consent requirements under the NPPs interferes significantly with the medical training protocols of private hospitals, which are today, often teaching hospitals.

(ii) Children's privacy

Having listed recommended changes above, the AMA strongly urges that the approach of the NPPs to children's privacy be retained, and not whittled away by provision for parents to access their under16 year old children's Medicare records.

Children's privacy is a central part of the review of NPP 2 on use and disclosure, specifically NPP2.4, that deals with disclosure of information to a person who is responsible for the individual.

The AMA is particularly concerned that the Australian Government is developing legislation to give parents access on request to all information held by HIC concerning their children aged less than 16 years. The Government believes that, in the ordinary course of events, parents should have a right to access information about their children, especially when it relates to their children's health and welfare. It states that the parents' right of access to their children's Medicare records should apply irrespective of whether children have their own Medicare Card.

The adverse consequences of this legislative proposal may outweigh the benefits. In circumstances where the parent wishes to access their child's records without the consent of the child, there is a risk that legislating to grant access to such records may adversely affect the relationship between the young patient and his or her doctor. It could discourage some young people in need of help and advice from attending their doctor or being candid in the consultation.

In order to make a proper clinical diagnosis and recommend appropriate treatment, a doctor must receive honest and complete information from the patient. For example, if a young person feels that his/her records are not confidential, he/she may refrain from informing the doctor that they are sexually active, smoke, use alcohol, etc. The doctor is then making a clinical diagnosis and treatment recommendation based on incomplete information.

Compared with the rest of the community, young people often experience difficulty in accessing health services. No further barriers should be placed on this.

The AMA believes that if parents have concerns regarding health services that their children are accessing, then they should discuss this with their children.

We believe that, where possible and developmentally appropriate, doctors should afford young people the same respect, rights and responsibilities as older patients.

If a young person is able to make autonomous decisions regarding medical treatment, and wishes that treatment to remain confidential, then their doctor must respect and maintain that confidentiality.

(iii) The need for harmonisation of Australia's privacy laws

The AMA urges a nationally coordinated or unified national privacy and health records legislation. The 'mish-mash' of privacy and health specific privacy legislation is confusing to both doctors and their patients.

In particular, clarification of the status of the NHPC, its content, and where it fits into the various jurisdictions' legal frameworks is required. The OFPC should play a leading role in guiding the direction of the NHPC initiative.

4. RESOURCING THE OFFICE OF THE FEDERAL PRIVACY COMMISSIONER

The AMA is of the view that the OFPC should be better resourced to carry out the functions of the Office under the Act. In the AMA's view further resources are required than are presently at the disposal of the Privacy Commissioner for administration and enforcement of the Act generally.

The AMA's belief is that the OFPC has insufficient resources to investigate and take action in respect of privacy breaches in a timely manner, particularly in relation to the problems associated with the on-selling of electronically held personal information.

Advances in technology will inevitably outstrip the electronic security capability, and the OFPC has neither the powers nor the resources to properly deal with this.

This is made worse by the current exemption of media and political organisations which bodies' activities often cause unacceptable infringements of privacy in a technological environment where personal information can be accessed quickly and easily.

The AMA notes the way in which the OFPC has approached its task of administering the *Privacy Act* as it applies to the private health sector in two particular respects.

First, its 'light' touch approach recognises that the medical profession itself considers that good privacy forms part of good clinical practice. The 'light' touch allows doctors to continue their commitment to patient privacy as an essential component of good clinical practice rather than viewing privacy as simply something to which doctors must comply to avoid legal consequences.

Second, the OFPC has worked cooperatively with the AMA in sharing information about difficulties doctors have encountered with the Act, taking part in the AMA's privacy education programs, and in being available to clarify privacy issues. The OFPC has recognised and attempted to address both perceived and real difficulties posed by the legislation. An example of this is the obtaining of Public Interest Determinations when it has been required.

The work of the OFPC has occurred despite the severe lack of resources provided to it to investigate and rectify privacy complaints, carry out educative campaigns, take action on its own initiative, and be proactive in the administration of the Act.

The AMA would be happy to elaborate on these submissions further, if required, and answer any questions.

The Australian Medical Association
AMA House
42 Macquarie Street
BARTON ACT 2600

Ph: (02) 62705400

22 February 2005

ATTACHMENT A

The concept of 'primary purpose'

The concept of 'primary purpose' when applied in the context of health care should accommodate the meaning 'the health care and well being of the patient', unless another meaning is specifically agreed to between the doctor and the patient.

Good privacy practice forms part of good clinical practice and complements doctors' duty of confidentiality. However, some doctors report that they experience difficulty in incorporating into their privacy policy the legislative obligations imposed by the NPPs without compromising best clinical practice. This arises largely because of the generic nature of the NPPs which are not health specific, but rather are designed to apply to all industries in the private sector.

1. The 'primary purpose' of collecting health information

NPP 2 incorporates the concept of the sole 'primary purpose' for the collection of personal information.[4] The information collected for the 'primary purpose', or a secondary purpose directly related to the 'primary purpose' of collection, can be used or disclosed for that purpose without further specific consent being obtained from the individual.

What constitutes that 'primary purpose' in the health care context is a critical matter that underlies the whole privacy scheme.

The AMA submits that in the health care context the 'primary purpose' of collecting personal information is to provide for the person's health care and general well being, unless a more limited purpose is clearly envisaged or agreed to by the patient and doctor.

Doctors generally understand 'health' to refer to the physical health of the entire body, not just certain 'bits and pieces' (eg. limbs, organs). 'Well being' refers to one's welfare or mental, emotional, and even spiritual 'health' (and is thus intrinsically linked with one's physical 'health'). 'Health care' is thus comprised of *both* health and well-being. It is holistic.

The care of a patient's health and well being is not achieved by episodic care. The process is not static, nor can it be temporally defined. One's past health and well being impacts on one's current health and well being which in turn influences one's future health and well being. Health care is an on-going process that spans from conception through to death. Most valuable health care interventions are opportunistic. That is they are unrelated to the primary reason for the patient attending the doctor.

The reference in NPP 2 to the 'primary purpose' of doctors collecting health information about patients should, in the health care context, be for 'the health care

[4] NPP2.1 states, as it applies to sensitive information, that an organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless the secondary purpose is directly related to the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose. Subject to other exemptions, consent is otherwise required.

and well being of the patient'. This permits a workable application of the NPPs generally so far as they deal with issues of consent for collection, use and disclosure of information, the 'secondary purposes' for which further consent is or is not required for use and disclosure of that information, and the requirements about the timing of the destruction of medical records. Only then will the application of the NPPs work to enhance, not hinder good clinical practice.

2. The construction adopted

However, this is not the approach taken by the OFPC to date, and indeed, the AMA understands that the OFPC has legal advice that NPP2 is not open to such a construction.

The way in which the NPPs have been applied is to assume that the collection of personal information by a doctor is for the purpose only of investigating, diagnosing, advising and treating a particular health issue, that is, the doctor is able only to use that information for the purpose of that episode of care.

This causes insurmountable problems to the efficient, effective and safe delivery of health care services, requiring a myriad of consents, and causing undue cost and delay as well as the risk to patient health. The AMA has provided examples of the problems this approach to the application of the NPPs gives rise to in its *Submissions on Draft Health Privacy Guidelines,* August 2001, accessible on the AMA's website at *ama.com.au/web.nsf/doc/WEEN-66586H/$file/draft_hpg.pdf.*

The AMA previously argued that the terms of NPP2 are open to a construction that supports the primary purpose being sufficiently broad as to permit a holistic and preventative approach to the health care of a patient. The AMA argued then, that the NPPs, with appropriate adjustment to the *Guidelines on Privacy in the Private Health Sector,* November 2001, could be incorporated into doctors' privacy policies accordingly.

The OFPC has determined that the default position is that the 'primary purpose' is restricted to the episode of care about which the patient attends, and that patients must otherwise specifically agree to the use of their information for other purposes, or for a holistic approach to their health care. The OFPC argues that this is intended to protect patients from disclosure of information, say their HIV or pregnancy status, to others in the treating team when not directly relevant to the particular episode of care.

In answer to this concern, the AMA has pointed out that it is, and will always remain, a patient's right to restrict the use of their information by discussion and agreement with their doctor. No one can force a patient to provide particular information, and the AMA's *Code of Ethics* specifically informs doctors to respect this right.

Given the OFPC's view that the NPPs envisage a narrow view of the 'primary purpose' and they are not open to a broader construction when applied to the collection of health information by treating doctors, these submissions will assume, therefore, the correctness of that assumption.

The AMA also accepts that NPP 10.2(b)(ii) that permits collection of health information 'where it is necessary to provide a health service to the individual' in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, provides no relief. Codes of ethics that might form such a body of rules are not 'binding' as

they do not have the force of law. In any event, even if 'binding' was amended to substitute the word 'guide', unless the concept of 'primary purpose' is given a broader meaning, restraints remain on the information collected being used and disclosed to achieve holistic care.

The narrow view of 'primary purpose' is compounded by an unrealistic threshold test provided for in NPP 2.1(e)(i). It states that before patient information can be disclosed to another person without the patient's consent it must be shown that there is 'a serious and imminent threat' to an individual's life, health or safety. The exemption does not accommodate cases where the disclosure is necessary to avoid possible or future harm to a patient, and which disclosure is not for the 'primary purpose' for which the information was originally collected.

3. The consequences

The flawed drafting of NPP 2 arises from a fundamental misconception of the role of doctors and a failure of the legislatures to accommodate the 'doctor-patient' relationship, which is founded on the principle of confidentiality.

The narrow construction of the 'primary purpose', in turn, limits what falls within secondary purposes that are 'directly related' to the primary purpose. It substantially widens the ambit of what falls within the concept of 'secondary purposes' for which specific consent is required before material is used or disclosed for attending to different aspects of a person's health care. The use and disclosure of health information for the purposes of ongoing health care is, thus inappropriately obstructed.

The need for management of some problems might not be appreciated by either the doctor or patient at the initial encounter. They may become apparent, say after a patient is sent to hospital for an unrelated problem, and the assessment, diagnosis and continued management of the problems require the use of the original information collected. The management of a patient's health cannot be dissected into the management of various conditions.

If 'primary purpose' is purely encounter related, where the patient is indisposed, the consent of a relative must be obtained before a patient's information is disclosed for the purpose of the ongoing health care. This erodes confidentiality. It might entail, for example, the doctor revealing the HIV or pregnancy status of the patient, contrary to the policy intent of the privacy principles. This breach of confidentiality strikes at the heart of the patient privacy that the privacy legislation sets out to protect and undermines the confidential nature of the doctor-patient relationship.

Worse, the consenting relative, parent or guardian has the power of veto over the use and disclosure of the information, despite the health care needs of the patient, unless there is a 'serious and imminent' threat to the life, health or safety of the patient. Thus, the mentally able, awake and alert, adult English speaking patient will be entitled to receive appropriate health advice and treatment promptly. Not so the mentally disabled, or a child with a non-English speaking parent or the unconscious.

The doctor who has the confidence of his or her patient and is privy to all their personal information, might be better placed to make decisions for the patient than another person to whom detailed information needs to be given to ensure the consent is fully informed.

A danger of the restrictive approach to the use of health information is that it serves to increase the vulnerability of those less assertive patients who depend upon their doctor to take care of their health in a holistic manner.

If the patient (or their guardian) finds the consent expectations too strenuous or impractical and chooses not to be tracked down every time consent is needed, then their health care suffers. If the doctor does not follow through in the interests of the patient's health care, they may be in breach of their duty of care, and be exposed to a medical suit for damages.

The standard of care required for a doctor to discharge their duty of care is that reasonably expected of the ordinary skilled person exercising and professing to have a special skill. In exercising the duty of care owed to a patient, a doctor is expected to regard the patient's interests as paramount. The doctor-patient relationship is based on trust and the doctor must respect confidentiality and the patient's need for health privacy. Doctors are ethically obliged to always act in their patient's best interests. However, a patient's health is put at risk and a doctor is exposed to a suit for damages for negligence if he or she, in giving supremacy to privacy obligations over considerations of patient health, fails to pursue all reasonable avenues available to assess, diagnose and treat a patient for any condition about which a doctor might become aware.

For example, an obese patient attending for a cut finger might be provided with advice from the doctor on how to prevent a heart attack in later years. A 32 year old patient is not likely to attend their doctor in order to ask how to prevent heart attack when 80 years of age. A further example of a doctor being expected to use patient information for a purpose beyond the 'primary purpose' in the discharge of his or her duty of care is to follow up medication compliance where non-compliance is suspected.

Often is the case where a doctor, whose skills and training are limited to a particular field, wishes to report a medical observation about a patient to the patient's GP without raising the matter first with the patient. The exemption to disclosure does not apply, as it is not 'a serious and imminent threat' to the patient's life, health or safety.

For example, an ophthalmologist might observe signs of depression in a patient being seen for eye problems. Not being comfortable raising the matter with the patient, which might provoke an expectation in the patient that expertise is at hand, the ophthalmologist exercising appropriate clinical judgment, chooses to mention the matter to the referring General Practitioner (GP). The ophthalmologist is not a trained counsellor and by mentioning the matter to the patient might find him or herself having to discuss the options and provide advice. Further, mentioning the matter can impinge on the doctor-patient relationship already developed.

By way of further example, a GP on seeing a record of a service or results of a service, might suspect, find or diagnose a condition not related to the reason for the encounter (e.g. a blood borne disease discovered from a blood test for another purpose). The GP may need to explore this aspect of the patient's health with others, or authorise further testing of the blood sample without the opportunity of discussing the issue with the patient, who might be indisposed. To obtain the consent of a relative to disclose information in order to carry out a further test, say for HIV/AIDS, would constitute a serious breach of patient confidentiality.

The way in which the NPPs are cast assumes that an individual consults a doctor about only one condition. That is rarely the case. Patients often present with more than one discrete medical condition. Perhaps on presenting with a cut finger (a condition) there is also a request for a Pap smear. The Pap smear can't even be characterised as 'directly related' to the primary purpose of collecting health information for the purpose of attending a cut finger. The current law on the handling of health information requires a separation out of the episodes of care in the course of one consultation.

Where a patient does attend a doctor for a discrete episode of care, on seeing the patient, the doctor might not regard the attendance in the same light. The GP in particular who takes a holistic and preventative approach to medicine might need to ensure that the simple 'cut finger' is not caused by 'blackouts' (epilepsy), or that it was not a result of violence in the home, or from self harm from an episode of depression, for example.

The appropriate exchange of information between treating doctors is necessary if they are all to stay in the same health care loop in respect of the patient. The narrow definition of 'primary purpose' threatens the GP's role as the coordinator of the management of the patient's health. GPs need to receive information back from consultants to whom they have referred a patient, and consultants need to obtain additional information from GPs, and enter into discussion about various aspects of a patient's health care, not only the condition for which the patient was referred.

Reports from doctors indicate that some hospitals, now aware of the privacy obligations, are prohibiting doctors from forwarding a discharge form to the GP without the patient's specific consent. This is a clear case where the patient should be required to 'opt out' and state they do not wish this to occur, in order that the expectations of patients generally and the management of their health care is not compromised. Good clinical practice requires the treating medical team to be privy to all relevant medical history and information about the patient.

Under the current law it is a breach of privacy for a hospital specialist to speak about a patient's case with another specialist on a collegiate basis, or to speak to another member of a treating team about other aspects of their patient's health. That is, implied consent cannot be assumed in these situations. In the interests of quality care it is submitted that a patient who wishes to restrict the sharing of their health information to a treating team, or restrict the information to be available to members of a treating team, should make the specific request so that the patient can be warned of the possible health consequences of the restriction.

Not all medical encounters are face-to-face. Compliance by those doctors who do not necessarily see their patients is often difficult. It can discourage pre-emptive investigations. In particular, pathologists, and those radiologists and anaesthetists who do not necessarily see their patients at the time of collecting and using their personal information face these dilemmas. The use and disclosure of health information in order to investigate a suspected health condition is not always 'directly related' to the primary purpose of a presenting condition, nor might the unrelated health condition be reasonably contemplated by a lay patient.

By way of example, a GP might arrange a blood sample to be taken for a discrete purpose, such as to test for hormone levels, or say, infection. The laboratory telephones to inform the GP that the test indicates an abnormality in cell count

unrelated to the condition being tested. The GP provides the laboratory with a further history for the purpose of carrying out other tests on the blood sample. This is a breach of the NPPs, in the absence of obtaining the patient's consent. Obtaining consent will result in delay and incur further costs, and could unduly and unnecessarily alarm the patient.

There are other implications to the narrow definition of the 'primary purpose'. NPP 4.2 requires records to be destroyed or permanently de-identified if no longer needed for any purpose for which the information may be used or disclosed under the NPPs. Such an application of NPP 4.2 would be contrary to some State legislation and inconsistent with best practice guidelines and some professional codes of conduct.

The example of the patient attending a GP for a cut finger is apt. As soon as no longer reasonably required, NPP 4.2 requires the records to be destroyed. Yet the history of the cut finger might later, but not foreseeably, be relevant to diagnosis of epilepsy, domestic violence, or other conditions.

To comply with their professional, ethical and legal duties individual doctors are required to widely define their purpose of collecting information and have their patient understand and agree to this, in order to 'bundle' the required consents to accommodate the necessary use and disclosure of the information in the interests of the patient's health care. Whether doctors are sufficiently aware of or should be expected to be aware of the intricacies of the privacy law to properly meet the 'bundled' consent requirements is another issue. Otherwise, doctors are currently required to obtain specific consent of their patients before they refer to or use medical histories and other information they hold for the purpose of future episodes of care, which substantially interferes with the continuum of health care.

4. In summary

The narrow view of the 'primary purpose':

- places onerous restrictions on the collection, use, and disclosure of patient information by treating doctors, obstructing the management of a patient's health;
- interferes with the clinical and ethical judgment of doctors, whose duty it is to always act in the patient's best interests;
- undermines the primacy of the doctor-patient relationship (eg. by eroding the confidentiality imperative);
- could lead to a doctor breaching their duty of care to their patient, and expose them to a suit for damages;
- impedes the ability of treating doctors to consult with each other on clinically relevant information;
- poses particular obstacles for those doctors who do not necessarily attend their patients;
- could cause the premature destruction of medical records no longer required for a particular episode of care, that might be required later for other medical conditions.

The AMA submits that this is unwarranted, unworkable, costly and can result in privacy principles posing obstacles to good clinical and ethical practice. Studies

support this submission.[5] The experience of doctors since 2001 as reported to the AMA proves this to be the case.

5. The solution

- That NPP 2 be amended to recognise that the 'primary purpose' of collection of health information by doctors is the 'health care and well being' of the patient;
- That NPP2(e) be amended to include 'or in the case of a patient, harm to that patient';
- The NPPs and the Guidelines be designed to reflect that the paramount concern of doctors is the health and well being of their patient.

[5] Australian Institute of Health and Welfare (AIHW) studies. Support can be found for the need to widen the meaning of 'primary purpose' in the context of the collection of health information by health providers in the joint report of the University of Sydney and the AIHW of the national BEACH (Bettering the Evaluation and Care of Health) survey of general practice activity.
The report "General Practice Activity in Australia 1999-2000', at xiv found that General Practitioners (GPs) could record up to four problems at each patient encounter.
At 2.5 (p.7) of the report is a diagrammatical BEACH relational database illustrating that reasons for encounters have only an indirect relationship with problems managed.

ATTACHMENT B

Access to personal information

The provision for patient access to their health records should incorporate exemptions where that access could cause patient harm short of posing a 'serious threat to the life or health of any individual'.

1. Access rights and potential harm

The AMA supports a person's right to access information held about them. However, in the health care context, there are occasions where that access can cause harm to the patient or interfere with the therapeutic relationship. The relevant exclusion in NPP 6.1(b) requires that it 'would pose a serious threat to the life or health of any individual'. This is too high a threshold to overcome the harm that might occur to a doctor-patient relationship or the patient.

Mere risk of harm or the disruption of the therapeutic relationship is not sufficient to meet the exemption in NPP 6.1(b). This poses a serious problem for doctors such as GPs and psychiatrists in particular, in the proper provision of mental health care.

2. Protection of doctors' private and preliminary thoughts

NPP 6 fails to protect the doctor's private or preliminary views in the thinking processes required for full medical assessments, accurate diagnosis and the formulation of treatment programs. Patient access to these private notes exposes patients to less than optimal health care.

Assessment, diagnosis and treatment involves the doctor's clinical judgment and often his or her thinking is assisted by *aides memoire* and consideration of differential diagnosis which should be private until the doctor commits to a professional opinion and management plan.

For example, a doctor at the hospital emergency department, faced with a patient admitted with abdominal pain with no organic cause, might make a differential diagnosis of narcotic use for the benefit of the next doctor on duty. It is not in the interests of the patient to know that this diagnosis was considered or initially suspected. If the patient is able to access this note (and may thus take offence at such a differential diagnosis), it is likely that the doctor will not record it.

The problem for doctors and patients occurs particularly where mental health issues are concerned, and the recording of the doctor's preliminary or tentative thoughts as consultations proceed and histories unravel. These are not expected to be correct while the diagnostic and treatment protocols are being worked through and access to the professional's thoughts can be damaging to the relationship and treatment program, and the health of the patient.

Psychiatrists take down facts as described. It might include hearsay but it is nevertheless important for the therapist to note it as told. Whether the information is truthful or not might indicate something in itself.

As part of the therapeutic process, psychologists and psychiatrists are trained to record their own reactions to their patients, and dynamic aspects of the doctor-

patient relationship. The psychiatrist might note, for example, their own adverse or positive reaction to the patient, as the therapy is interactive.

It is not appropriate, nor in the interests of the therapeutic process, that the patient have access to such notes. The therapist will not show the notes to the patient. While patient access might not be life threatening it can disrupt the treatment.

Further, the requirement in NPP 6.7 that the reason for withholding access to the information must be given to the patient may cause the very harm the health care provider seeks to prevent.

3. Carers' need to know

The access provisions together with restrictions on access to patient information fail to take sufficient account of the patient's carer's need to know information about the patient. Not only is a carer required to provide an appropriate environment for the patient being cared for, but may need to know what medication the patient is required to take, the patient's condition on discharge from hospital, what problems they may encounter, and details of follow up appointments. Disclosure of this information to the carer is necessary for the patient's ongoing care, whether or not the patient consents.

4. Privacy of vulnerable patients

Children, no matter how young, the mentally disabled and the unconscious patient, have a right to confidentiality, and privacy requirements should not over-ride this.

Difficulties can arise from a parent or step-parent having access to young children's clinical notes in which a doctor has included suspicions in the course of an examination or consultation. For example, a doctor at an emergency department of a hospital is unlikely to make a note of a suspicion that a young patient is being abused by the patient's parent, guardian, or relative of the guardian, so long as that parent or guardian is at liberty to obtain the notes. The next doctor on duty will not have the benefit of the surmise.

5. Abuse by lawyers and insurance companies

It is clear from reports to the AMA that patients' rights to access are often abused by legal advisors and insurance companies who persuade their clients that they require the whole of their health records from their treating doctors. This 'back door' method of obtaining information for medico-legal or insurance purposes instead of following court or other appropriate protocols is an unintended consequence of NPP 6. We submit that it needs to be addressed.