SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **37**

SUBMITTER

Australian Medical Association

AUSTRALIAN MEDICAL ASSOCIATION
ABN 37 008 426 793

T | 61 2 6270 5400
F | 61 2 6270 5499
E | ama@ama.com.au
W | www.ama.com.au

42 Macquarie St Barton ACT 2600
PO Box 6090 Kingston ACT 2604

10/139

19 August 2010

Senate Finance and Public Administration Committee
PO Box 6100
Parliament House
CANBERRA ACT 2600

Dear Senate Finance and Public Administration Committee

Thank you for providing the Australian Medical Association (AMA) with the opportunity to comment on the draft Australian Privacy Principles. Privacy is paramount to good medical practice; therefore, the AMA supports privacy legislation that enhances good quality health care.

General comments on privacy

Doctors have a general ethical and legal duty to protect the privacy of their patients' personal information. The provision of good quality health care depends on patients fully disclosing their personal information to their doctor. Doctors base their professional judgement regarding a patient's medical management on the full and frank disclosure of the patient's personal information. Without full disclosure, the doctor's ability to confidently formulate an accurate diagnosis or treatment plan is seriously undermined. Patients may either not attend a doctor or may limit or falsify the personal information they provide to their doctor because of fears that their privacy may be breached, potentially resulting in serious consequences for the patient's health care. As such, patients must have the trust and confidence that their doctor will protect the privacy and confidentiality of their personal information, including their medical record.

The AMA recognises that a patient's right to privacy and confidentiality is not absolute and there may be exceptions in the public interest; for example, in the case of a medical emergency. The AMA believes, however, that where a doctor is compelled to disclose patients' personal information, this must overwhelmingly be proven to serve the public interest. The public benefit of such disclosure must outweigh the risk that patients may not seek medical attention or may modify their personal information they disclose to their doctor because of fears their privacy will be breached. Where relevant and practical, the AMA encourages doctors to ensure patients are made aware of such limits to confidentiality at the outset of a consultation. At all times, such disclosure should be to the minimum extent necessary to achieve the objective.

Specific Comments on draft Australian Privacy Principles

Australian Privacy Principles 3, 6, and 12 in relation to lessening or preventing a serious threat to an individual

In setting out exceptions to obtaining consent from an individual, we note that the threshold by which an entity or organisation may collect, use, disclose, or access personal information in relation to lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety, has changed in the draft APPs (APP 3 (3)(b)(i), APP6 (2)(c)(i), and APP12 (3)(a)).

The current NPPs, as well as the IPPs, state there must be a 'serious and imminent' threat in reference to an individual. According to the Office of the Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector (8 November 2001),* a 'serious and imminent threat' is described as follows:

> *A 'serious' threat must reflect significant danger, and could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. Alternatively, it could include the threat of infecting a person with a disease that may result in death or disability. A threat could also relate to an emergency, following an accident, when an individual's life or health would be in danger without timely decision and action.*
>
> *A threat is 'imminent' if it is about to occur. This test could also include a threat posed that may result in harm within a few days or weeks. It is much less likely to apply to situations where the risk may not eventuate for some months or longer.*

The removal of the word 'imminent' must not result in inappropriate breaches of patient privacy. It will be necessary to clarify what the change in terminology actually means (eg., how this differs from the current requirement) and provide revised guidance as to when it is appropriate for a doctor to disclose a patient's personal information in the absence of consent.

We note that the exception for 'a serious threat to public health or public safety' has been retained in the draft APPs and this is acceptable. In the Guidelines referred to above, a 'serious' threat to public health or public safety relates to:

> *Broader safety concerns affecting a number of people. This could include the potential spread of a communicable disease, harm caused by an environmental disaster or harm to a group of people due to a serious, but unspecified, threat.*

Definition of sensitive information

We note that in the draft APPs, health information is included as part of sensitive information; however, the draft APPs have removed the strong reference to health information currently contained in the NPPs. For example, section 10.2, 10.3, and 10.4 of 'NPP 10 Sensitive information' (see Appendix) deal specifically with the collection of health information; however, this is no longer included in the draft APPs. Whilst we are aware that there will be further consideration of health information by the committee, it's not clear why the focus on health information has been removed from the draft APPs themselves. We would seek

assurance that the protection of health information is not in any way compromised or lowered because of this.

Other issues

We acknowledge that the Government will introduce the new privacy laws in four stages. We strongly recommend that as these changes to privacy legislation are rolled out they also be accompanied by draft explanatory guidelines that the Office of the Federal Privacy Commissioner will provide e.g. Guidelines on Privacy in the Private Health Sector. This will help doctors and their staff understand, incrementally, what changes they might need to make to their privacy policy documents and processes within the practice, as a result of the new privacy laws. This will reduce the burden on practices to undertake a wholesale review of their privacy practices when the entire suite of new privacy laws are operational. Where relevant to health information, such guidelines should be developed in consultation with the medical profession.

Further, we ask that the Government consider the administrative burden on already busy medical practices in having to comply with privacy legislation, in its proposed changes to the privacy legislation. The changes must not create additional red tape for doctors and their practice staff.

Finally, many doctors work as salaried doctors in public hospitals and also have rights of private practice. Accordingly, they are required to be familiar with the nuances of, and comply with, state government as well as commonwealth privacy legislation. This can be quite burdensome for doctors. We strongly recommend consideration of a single, national privacy legislation that covers the Commonwealth, States and Territories.

Concluding remarks

As outlined above, the AMA supports privacy legislation that enhances good quality health care. Privacy legislation should support and facilitate doctors in meeting their duties to patients and enhance patient confidence and trust in the medical profession.

Sincerely

[Signed]

Dr Andrew Pesce
President

Appendix 1
Reference to 'health information' in NPP 10. Sensitive information

10. Sensitive information

10.1……..
10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:
(a) the information is necessary to provide a health service to the individual; and
(b) the information is collected:
(i) as required or authorised by or under law (other than this Act); or
(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.
10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:
(a) the collection is necessary for any of the following purposes:
(i) research relevant to public health or public safety;
(ii) the compilation or analysis of statistics relevant to public health or public safety;
(iii) the management, funding or monitoring of a health service; and
(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
(c) it is impracticable for the organisation to seek the individual's consent to the collection; and
(d) the information is collected:
(i) as required by law (other than this Act); or
(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.
10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.
10.5 In this clause:
non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.