## General comments on privacy

Society values the medical profession's highly specialised knowledge, skills, and dedication to the primacy of patients' health needs as serving a unique and vital role in the health care system. Patients entrust themselves to doctors for their medical care - they trust doctors to be competent in their work, to practise with the highest ethical standards, and to advocate for their patients' health needs.

Patients also trust doctors to protect their personal information. Doctors require a patient's full and frank disclosure of their personal information in order to make an accurate assessment of the patient's health care needs. Without full disclosure, the doctor's ability to confidently formulate an accurate diagnosis or treatment plan is seriously undermined. In providing a full and frank disclosure of their personal information, the patient trusts the doctor to keep that information confidential. The integrity of the confidentiality of the patient's personal information is essential to developing, enhancing, and underpinning the therapeutic relationship. This confidentiality secures the necessary trust and openness that characterises the ongoing communication between doctors and their patients to optimise care.

Should that trust be eroded, 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.

The AMA affirms, therefore, that any changes to privacy legislation promote the trust and confidentiality of the doctor-patient relationship.

## Specific Comments on the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*

The AMA affirms the principle that patients have a right to know what information is held about them, a right to access it, and to have some control over its use and disclosure.

A patient's right to privacy and confidentiality, however, is not absolute and there may be exceptions in the public interest. In such exceptions, disclosure of a patient's personal information without their consent may be permitted such as in a medical emergency or where permitted or required by law.

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.

In the AMA's previous submission on the draft Australian Privacy Principles (APPs) released for comment in 2010, we raised concerns that the draft APPs reduced the threshold by which an entity or organisation may collect, use, disclose, or access personal information (without consent) in relation to lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety. The threshold was reduced from a 'serious and imminent' threat to a 'serious' threat in reference to an individual. We note that this change has been retained in the draft Bill. Under Permitted General Situations (pages 17 and 18), item 1 refers to the following condition

*(b) the entity reasonably believes the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.*

As we highlighted previously, the current National Privacy Principles (NPPs), as well as the Information Privacy Principles (IPPs), state there must be a 'serious and imminent' threat in reference to an individual. According to the Office of the Federal 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.*

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 guidance must be provided to health care providers, as well as the general community, as to when it is appropriate for a health care provider to collect, use, or disclose a patient's personal information in the absence of their consent.

Retention of 'a serious threat to public health or public safety' is acceptable and reflects current privacy legislation.

**Reference to health information**

In our previous submission on the draft APPs, we raised concerns that the draft APPs had removed the strong reference to health information currently contained in the NPPs. We are reassured to see in the Bill that the APPs now contain a comprehensive section (16B)

addressing 'Permitted health situations in relation to the collection, use or disclosure of health information.' We strongly urge that this emphasis on health information be retained in any changes to privacy legislation.

**Other issues**

We urge the Government to consider the administrative burden placed on medical practices when complying with any changes to privacy legislation. Any changes to the legislation should be accompanied by draft explanatory guidelines to help doctors and other health care providers understand their obligations under a new privacy regime. Where specifically relevant to the privacy of health information, any guidelines should be developed in conjunction with the medical profession.

A community awareness campaign should also accompany any changes to privacy legislation in relation to health information so that patients, carers, and others understand their rights and obligations under the new privacy law.

**Concluding remarks**

Privacy legislation should enhance good quality health care by supporting doctors in meeting their duties to patients and enhancing patient confidence and trust in the medical profession and wider health care system.