SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **26**

SUBMITTER

Office of the Health Services Commissioner

HEALTH SERVICES COMMISSIONER

Level 30, 570 Bourke St
Melbourne VIC 3000 Australia
Telephone: 8601 5222 (administration)
Telephone: 8601 5200 (complaints)
Toll Free: 1800 136 066
Facsimile: 8601 5219
TTY: 1300 550 275
DX: 210182
Email: hsc@dhs.vic.gov.au
www.health.vic.gov.au/hsc/

SUBMISSION BY THE HEALTH SERVICES COMMISSIONER, VICTORIA, TO THE SENATE FINANCE AND PUBLIC ADMINISTRATION COMMITTEE'S EXPOSURE DRAFT OF AUSTRALIAN PRIVACY AMENDMENT LEGISLATION – AUSTRALIAN PRIVACY PRINCIPLES

DATE: 10 August 2010

Introduction

Thank you for the opportunity to comment on the Exposure Draft of the Australian Privacy Amendment Legislation which contains the new Australian Privacy Principles (APP), which will form part of a new Privacy Act.

The Health Services Commissioner (HSC) is an independent statutory authority whose purpose includes to promote and protect health privacy in Victoria. The HSC administers the *Health Records Act 2001* (Vic) and is responsible for the protection of individuals' personal health information that is handled by Victorian Government agencies, health service providers and private sector organisations in Victoria.

As the jurisdiction of HSC is confined to health privacy, this submission will address only those matters in the Exposure Draft that are relevant for health. I note there will be further exposure drafts of the re-written *Privacy Act* referred to the Committee about specific privacy protections relating to health, which will provide the opportunity for further submissions.

APP 1 - Open and transparent management of personal information

APP 1(2) requires entities to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and will enable the entity to deal with enquiries or complaints from individuals about the entity's compliance with the APPs. APP 1(4)

sets out what a privacy policy must contain, and of significance is the requirement that it contain information about how an individual may complain about an interference with their privacy, and whether the entity is likely to disclose information to overseas recipients. The provisions in APP 1 go further than the existing provisions in the *Privacy Act 1988* (Cth) and the equivalent provisions in the *Health Records Act,* and these changes are supported.

APP 2 - Anonymity and pseudonymity

This principle is consistent with the equivalent provision in the *Health Records Act* (Health Privacy Principle 8) and is supported.

APP 3 - Collection of solicited personal information

This principle is generally consistent with the equivalent provision in the *Health Records Act* (Health Privacy Principle 1) and is supported.

APP 4 - Receiving unsolicited personal information

This proposed principle is difficult to apply in a health setting, as the usual situation in which a health service provider receives unsolicited information is when a relative or friend of their client contacts them to provide information. It will not be easy to determine whether or not the entity could have collected the information under APP 3 if the entity had solicited the information. Therefore further consideration needs to be given to how this principle should apply in the case of health privacy. Health Privacy Principle 1.7(d) deals with this issue in the context of information given in confidence, and the Committee should examine Health Privacy Principle 1.7(d).

APP 5 - Notification of the collection of personal information

The matters an individual needs to be informed about when an entity collects personal information are broad, and more far reaching than the equivalent provisions in the *Health Records Act*, and this principle is supported. In particular, pursuant to APP 5(2)(h) and (i), the entity must take reasonable steps to notify the individual of how the individual may complain about an interference in their privacy, and whether the entity is likely to disclose the personal information to overseas recipients. The inclusion of these matters is welcome.

APP 6 - Use or disclosure of personal information

This principle is consistent with the equivalent provision in the *Health Records Act* (Health Privacy Principle 2) and is supported. The more stringent requirement for sensitive information (which includes health) in APP 6(2)(a) is supported. APP 6(2)(c) deals with use or disclosure in the absence of consent where the entity reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to life, health or safety. APP 6(2)(c)(ii) requires it must be unreasonable or impracticable to obtain the affected individual's consent to the use or disclosure. In a health setting, such a use or disclosure is likely to involve a client suffering from psychiatric illness, and such a requirement may place an additional limit on the ability of the entity to use or disclose the personal information. Consideration needs to be given as to whether such a provision is appropriate when dealing with health privacy.

The inclusion of APP 6(2)(i), where use or disclosure is permitted if the information is reasonably necessary for the purpose of a confidential alternative dispute resolution process, is welcome.

APP 7 - Direct marketing

HSC makes no comment in relation to APP 7, as it is not relevant in a health care setting.

APP 8 - Cross border disclosure of personal information

HSC has concerns about the content of this principle. The protection afforded by APP 8(1) does not apply if the overseas recipient is subject to a local law or binding scheme that provides the same privacy protections, and there are mechanisms the affected individual can access to take action to enforce that protection. HSC considers this problematic, as an individual in Australia would need to take action in the overseas jurisdiction to seek redress in the case of an interference in their privacy, and this is not reasonable. Health information is sometimes sent overseas by health insurers, and there are instances of medical imaging organisations sending images overseas for interpretation. The affected individuals should be afforded the same level of privacy protection as other Australians and they should be able to seek remedies within Australia.

Further, APP 8(2)(b) provides that the protection afforded by APP 8(1) does not apply if the entity obtains the consent of the individual to overseas disclosure, after having been given information to that effect. This is of concern, as a detailed privacy notice at the end of a document which includes information about disclosure to overseas recipients, is not likely to be read by many individuals. In the case of health, the commercial imperative to send information overseas does not apply compared to other sectors, therefore stringent requirements are needed in relation to sending health information overseas.

APP 9 - Adoption, use or disclosure of government related identifiers

The restriction on adopting government related identifiers contained in APP 9(1) applies to organisations and does not appear to apply to public sector agencies. This is of concern, as health services such as public hospitals should be subject to the same limitation. The purpose of this principle is to limit data matching unless it is provided for in another law or in regulations, in line with the need for stringent privacy requirements for such activities.

At the end of APP 9(1) is a note which states "An act or practice of an agency may be treated as an act or practice of an organisation". HSC is uncertain whether this is an attempt to have public sector agencies bound by APP 9(1). If that is the case, it needs to be explicit.

APP 10 - Quality of personal information

This principle is consistent with the equivalent provision in the *Health Records Act* (Health Privacy Principle 3) and is supported.

APP 11 - Security of personal information

APP 11(1) is consistent with the equivalent provision in the *Health Records Act* (Health Privacy Principle 4.1) and is supported.

APP 11(2) states if an entity no longer needs the personal information of an individual and provided the entity is not required by an Australian law or an order of a court or Tribunal to retain the information, the entity must take reasonable steps to destroy or de-identify the information. Such a principle is not appropriate in the case of a health service provider, where minimum retention periods are necessary. In a health setting, there may be a lapse of time in people re-presenting for treatment, or there may be medical conditions that are slow to progress. Individuals may only discover many years later that the health treatment they received was below standard, and they or their health professional may require access to old medical records. A minimum retention period of at least seven years (as provided for in Health Privacy Principle 4.2) is therefore necessary.

At the moment, private sector health providers in Victoria, for example, are bound by HPP 4.2, which prevents them from destroying health information unless it is more than seven years after the last occasion on which a health service was provided. Therefore while the *Privacy Act* does

not have minimum retention periods, the operation of a state law in the form of the *Health Records Act* operates to regulate the minimum retention period. If the state health privacy laws are no longer to operate alongside the *Privacy Act,* as recommended by the Australian Law Reform Commission in its Report 108 "For Your Information", then this will need to be addressed in the *Privacy Act*. See below under the heading "Further Matters" for additional comment on this issue.

APP 12 - Access to personal information

APP 12(1) and most of 12(3) are consistent with the equivalent provisions in the *Health Records Act* (Health Privacy Principle 6.1) and for the most part are supported. In the case of APP 12(3)(c), it provides an organisation is not required to give an individual access to their personal information to the extent the request for access is "frivolous or vexatious". This exception is not appropriate in the case of personal health information, as a person has a right to access their health information, even if the contents are brief. An individual does not require a reason to access their health information, and such an exception is likely to lead to organisations refusing access without good reason. If the organisation has a legitimate reason for refusing access, the situation will be covered by one of the other exception grounds set out in APP 12(3).

In relation to APP 12(4) which has the heading "Dealing with requests for access", an organisation must respond to an access request within a reasonable time. In the case of health information, HSC believes a fixed period is preferable, to enable certainty for individuals. Reasonable time may differ depending on whether an organisation is large or small, and if a person wishes to complain that their access request has not been responded to, a person will not know how much time they should wait before lodging a complaint. A fixed time period removes this uncertainty. In the *Health Records Act*, an organisation is required to respond within 45 days, therefore they are allowed more time than the 30 days required of agencies under APP 12(4)(a)(i).

Further, APP 12(4)(b) states an entity must give access to the information in the manner requested by the individual "if it is reasonable and practicable to do so". In the case of access to one's personal health information, HSC considers such an exception should not apply. Most people seek access in the form of a copy. If such an exception applied, an organisation may seek to argue that it is not reasonable or practicable to do so, because of the volume or complexity of the information. The entity may suggest the person should inspect their records instead, which adds to the cost of access, as the staff member's supervision time would need to be included. Such an outcome would be unsatisfactory and contrary to the principle of patient autonomy that applies in a health setting.

The remainder of APP 12, which deals with the use of an intermediary, charging for access and giving reasons for refusal, are largely consistent with the equivalent provisions in the *Health Records Act* (found in Health Privacy Principle 6) and are supported.

APP 13 - Correction of personal information

APP 13 is consistent with the equivalent provisions in the *Health Records Act* (Health Privacy Principles 6.5 to 6.10) and is supported.

Other matters

At page 19 of the Companion Guide, it states "Section 3 of the existing *Privacy Act* preserves the effect of any State or Territory law that makes provision about interferences with privacy, if it is capable of operating concurrently with the existing *Privacy Act*. The Government does not intend to change its policy in this regard, so an equivalent provision to this effect will be included in the new *Privacy Act*". This suggests the Government has not accepted Recommendations 3-1 and 3-2 of the Australian Law Reform Commission's Report 108. HSC welcomes the Government's position.

HSC opposed the proposal to exclude state and territory health privacy laws to the extent they applied to private sector organisations, as HSC considers the interests of consumers and organisations can best be served by having state and federal regulators working co-operatively. HSC sees no difficulty in both Federal and State legislation having coverage of health privacy in the private sector, as the laws are largely consistent, and state based regulators are able to better deal with and respond to local concerns and issues.

HSC looks forward to the release of further exposure drafts of the re-written *Privacy Act* by the Committee about specific privacy protections relating to health.

Beth Wilson
Health Services Commissioner