Office of the Victorian Privacy Commissioner

Submission to the Senate Community Affairs Committee

on the

Healthcare Identifiers Bill 2010 & Healthcare Identifiers (Consequential Amendments) Bill 2010

5 March 2010

Office of the Victorian Privacy Commissioner (Privacy Victoria)
GPO Box 5057
10-16 Queen Street
Melbourne Victoria 3000
Australia
Phone: 1300-666-444
Fax: +61-3-8619-8700
Email: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

1. Introduction

Electronic health (or e-health) records are already a feature of the health system in the Australian public and private health sectors and their use is increasing. Their wider introduction appears inevitable. The primary challenge of this development is to maximise both the protection of individual privacy and positive health outcomes.

It is for this reason that I provide this submission on the Healthcare Identifiers Bill 2010 ("the Bill") & the Healthcare Identifiers (Consequential Amendments) Bill 2010, despite the fact that health information is not regulated by the *Information Privacy Act 2000 (Vic)*. The privacy implications of the creation of a national identifier are such as to necessitate comment.

One of the fundamental components to allow creation and linkage of e-health records is a universal, unique identifier for each individual patient. Without such an identifier, effective linkage will be virtually impossible. Likewise, the privacy risks involved in this identifier are largely, though not exclusively, related to the proposed use and disclosure of the identifier to link e-health records.

For this reason, the Bill, in which the arrangements around the healthcare identifiers are dealt with, without dealing with the broader privacy issues concerning e-health, is somewhat artificial and limited. To a large extent, the process guarantees "function creep", in that the specific e-health functions to which the identifier will be put and the way in which the e-health system will be operated and managed are not being defined at this stage [for example, clauses 14 and 21]. Rather the general areas of "provision of healthcare", "management, funding, monitoring or evaluation of healthcare" and "conduct of research" [Clause 24(1)] are included as constituting authorised use or disclosure. This makes it difficult to adequately assess whether the safeguards being instituted will ultimately be sufficient or effective.

2. The Healthcare Identifiers Service Operator

Clause 6 states:

> (1) The Chief Executive Officer of Medicare Australia is the ***service operator***.
>
> (2) However, if the regulations prescribe another person for the purpose of this subsection, that person is the ***service operator*** instead.

As previously submitted[1], there are a number of issues with Medicare Australia being the organisation that operates the Healthcare Identifiers Service (HIS).

In its 2004-2005 report on the integrity of Medicare Enrolment Data, the Australian National Audit Office (ANAO) found that the great majority of data contained in the Medicare enrolment database was sufficiently accurate, complete and up to date to support the efficient administration of Medicare and its functions at that time. Notwithstanding that, ANAO

[1] Privacy Victoria, Healthcare identifiers and privacy - discussion paper on proposals for legislative support: Submission to the Australian Health Ministers' Advisory Council, 14 August 2009

found that some data, particularly in fields containing various dates, was logically inconsistent or in error.[2]

The ANAO made six recommendations, addressing matters including:

- further data cleansing;
- resolving duplicate enrolments;
- checking the accuracy of some techniques employed during data migration;
- making better use of information from State Registrars of Births, Deaths and Marriages to update records of people who are deceased; and
- redeveloping a Technical Standards Report.

One of the major rationales for the previous government's proposed Access Card was the need to improve the integrity and accuracy of Medicare and Centrelink enrolment data, which under that scheme was to be achieved by the re-enrolment of the entire Australian population. However, the Medicare database is now to form the basis on which Individual Health Identifiers (IHIs) are to be issued. This raises concerns about data quality – one of the fundamental principles of privacy – before the system even commences.

Given that the introduction and maintenance of healthcare identifiers will be the basis for any future e-health developments, the ameliorative steps recommended by the ANAO should be taken before proceeding or the existing Medicare data should not be used.

Moreover, the location of the HIS within Medicare has the potential to lead to a perceived conflict of interest. While the stated intention is that the HIS will be a separate and new Medicare business, not linked to its funding or claims-for-payment functions, the fact that all of these functions will effectively be operated by the one organisation is likely to lead to a degree of public disquiet or concern about potential misuse.

In addition, the future re-allocation of the HIS to another entity should not be done by regulation. If there is a need to allocate this task to a body other than Medicare Australia, this should be done by amending the legislation itself, ensuring full parliamentary scrutiny of the process.

3. Assignment, use and disclosure of healthcare identifiers

The Bill authorises the HIS to assign [Clause 9] and disclose [Clause 17] health care identifiers. Likewise, the Bill authorises healthcare providers to use and disclose personal information in order to obtain a healthcare identifier from the HIS [Clause 16] and to use and

[2] See ANAO, *Integrity of Medicare Enrolment Data*, Report No. 24, 2004/2005, January 2005, available at www.anao.gov.au

disclose a healthcare identifier for specified purposes [Clause 24]. These processes require neither the consent of the individual, nor notice to the individual to whom the identifier relates [Clause 9(4)].

The National Health and Hospitals Reform Commission (NHHRC) recommended that a person-controlled electronic health record should be available for each Australian, with the capacity for individuals to choose which healthcare providers and carers would have access to their person-controlled health records.

At a number of public forums (Melbourne, 29 July 2009; Canberra, 20 November 2009) and in the document issued by the Australian Health Ministers' Conference (AHMC) to accompany the Exposure Draft of the Bill[3], it has been stated that individual healthcare identifiers (IHIs) "will not be a requirement for accessing healthcare in Australia".

Given the Bill establishes mechanisms for the automatic and universal assignment and the use and disclosure of IHIs in a way which is outside of the control of the individual – not even requiring notice to the individual that an identifier has been assigned – it is difficult to accept this statement. It would appear that any healthcare provider in possession of the individual's Medicare number, name, date of birth and sex (i.e. effectively any healthcare provider that the individual has ever consulted) will be able to obtain the individual's IHI from the HIS and apply it to the individual's health records. In addition, use or disclosure of the IHI will then be authorised without either the consent of or notice to the individual, provided it is for the purposes specified in the Bill. This does not appear to be consistent with a "patient (or person)-controlled" system, nor with avoiding the use of an IHI identifier becoming a de facto condition of obtaining healthcare.

I recognise that it may not be practically possible to institute an effective system that is truly "person-controlled" and that does not require the use of an identifier in order to obtain healthcare (at least where the individual also wishes to obtain a Medicare benefit in relation to that healthcare service). If that is indeed the case, the rhetoric concerning the "voluntary" nature of e-health, the fact that e-health records will be "person-controlled" and the notion that use of an IHI will not be required in order to obtain publicly funded health care should be abandoned.

4. Interaction with existing privacy laws

The Bill creates a number of offences for unauthorised use or disclosure of IHIs [Clause 26]. I strongly support the inclusion of these provisions, given the sensitive nature of the information to which the IHIs will be linked and the fact that, once an e-health system is introduced, the identifier will in effect be a "key" to an individual's entire e-health records.

In addition, the Bill contains a number of provisions concerning the operation of existing privacy laws in relation to IHIs. I acknowledge that steps have been taken to ensure that privacy protections will apply to IHIs across all Australian jurisdictions, in both the private and public sectors.

[3] AHMC, *Building the foundation for an e-health future... ...update on legislative proposals for healthcare identifiers,* November 2009, para 5.2, p.13;

The HIS will be an "agency" within the meaning of the *Privacy Act 1988* (Cth) [Schedule 2, Part 1 of the Health Identifiers (Consequential Amendments) Bill] regardless of whether or not it continues to be Medicare Australia. An act or practice that constitutes an offence under the Bill will also constitute an "interference with the privacy of an individual" for the purposes of section 13 of the Privacy Act [Clause 29(1)]. This will mean that the Australian Privacy Commissioner will have jurisdiction to accept complaints under Part V of the Privacy Act, even where the interference with privacy is committed by a State or Territory authority [Clause 29(2)]. However, where there is existing State or Territory privacy legislation, this legislation will continue to have effect to the extent that it is capable of operating concurrently with the Bill [Clause 37].

This will mean that, in effect, both State or Territory privacy authorities and the Australian Privacy Commissioner will have jurisdiction over breaches of the Bill by State and Territory authorities, unless a declaration is made by the (federal) Minister that relevant provisions of the Bill do not apply to a State [Clauses 37(5) and (6)].

It would appear to me that, where there is existing State or Territory privacy legislation, it is preferable that this continue to apply to State and Territory authorities to the exclusion of the Privacy Act. However, where there is no existing State or Territory legislation, the Commonwealth law should apply, so as to provide privacy protection in that jurisdiction.

A situation in which two separate regulators have jurisdiction, depending on which of them the individual happens to complain to, may create unnecessary confusion and allow "forum shopping" on the part of complainants. The provisions should be redrafted to reduce the reliance on Ministerial declarations and make it clearer that, where there is existing State or Territory legislation, this should apply.

HELEN VERSEY
Victorian Privacy Commissioner