'A National ID system to put health privacy at risk'

Submission to the Community Affairs Legislation Committee Inquiry into *Healthcare Identifiers Bill 2010* and *Healthcare Identifiers (Consequential Amendments) Bill 2010*

Graham Greenleaf
Professor of Law,
Co-Director, Cyberspace Law & Policy Centre
University of New South Wales

Background

The Cyberspace Law & Policy Centre at the University of New South Laws Faculty of Law is a research Centre which is involved in research concerning the public interest in networked transactions. I am a Professor in the Faculty of Law, and Co-Director of the Centre. I have over thirty years experience in privacy law and policy, and at various times have been a statutory member of the NSW Privacy Commissioner, adviser to the Federal Privacy Commissioner, adviser to the European Commission on privacy issues, co-founder of the Australian Privacy Foundation, founding Editor of *Privacy Law & Policy Reporter* (Sydney, 1993-2006), and currently Asia-Pacific Editor of *Privacy Laws & Business International Newsletter* (London, 2006-). I am the author of numerous articles and submissions on privacy issues, and co-editor of *Global Privacy Protection: The First Generation* (2008).

Annexures

Two draft documents are annexed to this submission and are referred to below:

(I) '34 PIA recommendations not adopted by NHTA' (G Greenleaf)

(II) 'Comparisons between the identification systems in the 'Healthcare Identifiers' (2009-10), 'Australia Card' (1986-87) and 'Access Card' (2006-07) proposals, from Bills and related sources' (G Greenleaf)

Another misleading Bill legislating surveillance by instalments

The fundamental problem with this Bill is that it is incomplete, covering only a small but central element of a much broader health identification and surveillance system which includes electronic health records.

When seen in its entirety (insofar as is possible from published documents), the proposed surveillance system shares a very large number of common elements with the discredited and rejected Australia Card (1986-97) and Access Card (2006-07) proposals put forward by governments from both major parties. This can be seen from the preliminary analysis in Annexure II.

The 'Access Card' Bill was very strongly criticised by the Senate Committee that examined it in 2007 for presenting to the Parliament a Bill which only covered a fragment of the overall legislative proposal.

The situation is the same here. The Victorian Privacy Commissioner in her submission politely explains the fundamental flaw in the Bill (emphasis added):

> 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 ehealth 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.

A more blunt way of stating this is that for the government to require the Parliament to consider this Bill in isolation is misleading to the Parliament. It is an unreasonable request, and the Bill should be rejected until the full package is presented to the Parliament.

The Privacy Impact Assessments (PIAs) commissioned by NEHTA were also adamant that this was a major issue. From Annexure I it can be seen that Clayton Utz (PIA Recommendation 1) considered that a 'new regime' of privacy laws was necessary *before* a universal health identifier was introduced. Recommendations 14 (Function expansion), Recommendation 15 (Controlling unintended uses and disclosures of UHI information) and Recommendation 19 (Retention and destruction of UHI information) reiterated the need for these matters to be covered in specific UHI enabling legislation. Mallesons also recommended that these matters be covered by 'robust, transparent and public mechanisms' (7.4.1), and ones that are not dependent on rule-making powers that fall short of this (7.4.2).

Submission 1: The Parliament should reject this Bill until the whole package of legislation for electronic health records is presented. The dangers of this Bill cannot be understood without that context.

Submission 2: The elements in this Bill and related documents that are similar to the previous rejected attempts to introduce compulsory national identification systems ('Australia Card' (1986-87) and 'Access Card' (2006-07)) are sufficiently numerous and striking as to justify intense scrutiny by the Senate.

Unjustified rejection of Privacy Impact Assessment recommendations

NEHTA obtained three Privacy Impact Assessments (PIAs) in the course of developing this legislation, from consultancy companies and law firms with considerably expertise in privacy and information systems available to them.

However, the bulk of the recommendations made by second (Clayton Utz) and third (Mallesons Stephen Jacques) PIAs have not been implemented by NEHTA (which referred many of them 'for government consideration') or in the Bill. They are set out in Annexure I, and referred to in specific contexts throughout this submission. However, the general issue remains that the government has not systematically stated why it has rejected each of the recommendations arising from the PIAs. The PIA process is not complete until the responsible implementing body explains why it accepts or rejects each recommendation.

Similarly, a major function of PIAs should be to give the Privacy Commissioner a detailed set of recommendations which should be considered by her Office (from its different public interest perspective), and on matters of major public importance such as this Bill the Privacy Commissioner should be required to state whether she supports or opposes each recommendation in a PIA.

Submission 3: The Senate should require the Department to explain which (if any) of the more than 30 PIA recommendations not implemented by NEHTA have been implemented by the Government in the Bill, and the reasons for rejecting the remainder. The Senate should also require the Privacy Commissioner to specify which of these PIA recommendations she supports, and her reasons for rejecting the others. This Bill should not proceed in the absence of that information.

Risk of extra-Parliamentary privatisation of national health ID system

The 'service operator' who runs the healthcare identifiers system can be changed at any time *by regulations* from Medicare to any other person (s6), including by a private sector operator. The Minister can give directions to the service operator (s32).

It is quite clear that a change of operator should never occur by regulations, but only 'by amending the legislation itself, ensuring full parliamentary scrutiny of the process' as the Victorian Privacy Commissioner submits.

Submission 4: No legislation should ever allow a national identification system to be operated by the private sector. A fortiori, no legislation should allow such a step to occur without the full scrutiny of the legislative process.

That the government is proposing that the control of the future health records of all Australians could be privatised at all, let alone without full Parliamentary scrutiny, is likely to greatly upset many Australians. It is the type of 'try on' that was found all through the Access Card legislation, and is now being trotted out again in the hope that no one will notice.

Healthcare providers must inform individuals of their IHI

Although Medicare is required to provide, on request, a healthcare recipient with their IHI and other information included in its records as the system operator, this base level right of access is all that would be provided by the Privacy Act in any event. A healthcare provider may disclose an IHI to the healthcare recipient (cl 23), but is not obliged to do so (although various privacy Acts may operate depending on the type of healthcare provider).

Even though an IHI may be allocated to a person without their knowledge, there is no obligation on either Medicare or the healthcare provider involved to pro-actively provide IHI details to a person when it is allocated. There should be, because otherwise many individuals will not know a number has been allocated to them until something goes wrong with the system.

Submission 5: When an IHI is allocated, the Bill should provide that either Medicare or the healthcare provider involved pro-actively provide IHI details to a person when it is allocated.

A compulsory ID number

The allocation of the healthcare identifier is compulsory, the service operator is 'not required to consider whether … a healthcare recipient agrees' (cl 9(4)). The general compulsory

nature of the whole regime established by the Bill is summed up by the Victorian Privacy Commissioner:

> 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 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 policy aspects and implications of the destruction of the patient/person controlled system is then summarised by the Commissioner as follows:

> 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.

Once again, use of an identifier will become 'pseudo-voluntary'.

The PIAs stressed the importance of the use of the IHI remaining voluntary (as distinct from the allocation of IHIs).

Submission 6: The Bill should provide and guarantee that the use of an IHI is not a condition of obtaining healthcare, and that it is an offence to make it a de facto condition of obtaining healthcare. There are provisions in the Access Card Bill which attempt something similar.

The legislation does not even provide a right of appeal against decisions concerning assignment of healthcare identifiers, it leaves this to yet-to-be-seen regulations (s9(5)). It is obvious that fundamental liberties such as rights of appeal should be guaranteed in the Bill itself, not left to bureaucratic whim.

Submission 7: Cl 9(5) should be deleted and replaced with a right of appeal.

Protection of anonymous health care needed

The Clayton Utz PIA recommended individuals having the choice whether to activate an IHI, and that activating an IHI should never be a pre-requisite for obtaining healthcare

(Recommendations 3 and 6). Many of the other recommended controls regarded by Clayton Utz as essential have also been rendered nugatory by the government's change to a compulsory model (Recommendations 10, 11, 12, 13). Mallesons' PIA recommendations 7.8.1-7.8.4 also included detailed recommendations for maintaining anonymity and pseudonymity in provision of health services.

The submission by the Queensland Office of the Information Commissioner, after examining how it is impossible for individuals to prevent their IHI being used in relation to the obtaining of healthcare, concludes that it is necessary to provide a right to individuals to consent to the use of an IHI, and limited circumstances where this can be overridden.

Submission 8: As submitted by the Queensland Office of the Information Commissioner, healthcare providers should seek an individual's consent (which could be a standing consent, but revocable) to retrieve and to use their IHI, except where the lack of the IHI would make the provision of the healthcare service impractical.

Inevitable function creep, with inadequate attempts to control it

The right of any healthcare provider to use the IHI for a very wide range of purposes (cl 24), and to use it as a key identifier in their own record systems (cl 25) will ensure that it will be utilised, and regarded as compulsory, in the record systems of tens of thousands of organisations throughout Australia.

Although cl 27(1) (in combination with NPP 7) should seriously restrict its use outside this already wide ambit, there are holes in that prohibition. Any other law, State, Territory or Federal, can allow any other uses or disclosures of the IHI (cl 26(2)(b)). The Clayton Utz PIA Recommendation 15 did not recommend any such exception, and nor does the Mallesons PIA.

Submission 9: Cl 26(2)(b)) should be deleted to prevent function creep, particularly at State and Territory level.

As the Victorian Privacy Commissioner adds,

> 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.

This was addressed specifically be Mallesons, who recommended imposing tight limits on uses Medicare could make of the IHI.

Submission 10: The Mallesons PIA recommendations 7.5.3 and 7.6.2 limiting the use Medicare can make of IHI should be included in the Bill.

Unrestricted data matching to create the health identifier database

Any 'data source' is authorised to disclose 'identifying information … of a healthcare recipient' to Medicare in order to create this database (cl 12(1)). Any anyone whatsoever can be declared by regulations to be a 'data source' (cl 12(2)).

So Medicare can have regulations authorising it to obtain personal information from any organisation in Australia, and every such organisation will have legislative protection against what would otherwise be breaches of the Privacy Act. This is one of the most massive legislated authorisations of Privacy Act breaches since the Data Matching legislation.

Submission 11: Any authorisation of data matching schemes to enable Medicare to build this database should be specifically included, by named organisation, in legislation.

No controls over data matching accesses to the health identifier database

Mallesons PIA Recommendation 7.14.1 is for 'a specific legislative restriction on law enforcement and security agencies being generally able to access information held for the purposes of the HI Service'.

The Bill completely fails to deliver this, because cl 15(2)(b) allows disclosures by the Service Operator for 'a purpose that is authorised under another law'. As with the Access Card Bill, the huge array of current demand powers can be used to require Medicare to hand over information from the health identifier database.

Submission 12: The Department, and the Privacy Commissioner should be required by the Senate to identify all current situations where disclosures under because cl 15(2)(b) may be authorised under another law.

Submission 13: As Mallesons PIA recommended, there should be a specific legislative restriction on law enforcement and security agencies being generally able to access health identifier information.

Healthcare providers should be required to report data breaches

Mallesons correctly recommended that data breaches should be notified (to the Privacy Commissioner and to data subjects as appropriate). This should be part of the privacy protections involved in this legislation, in advance of more general legislation recommended by the ALRC.

Submission 14: As in Mallesons PIA Recommendation 7.18.2, the legislation should require Healthcare Providers to comply with a statutory breach reporting regime. This provision could be repealed when more comprehensive data breach notification laws are enacted.

Summary of Submissions

Submission 1: The Parliament should reject this Bill until the whole package of legislation for electronic health records is presented. The dangers of this Bill cannot be understood without that context.

Submission 2: The elements in this Bill and related documents that are similar to the previous rejected attempts to introduce compulsory national identification systems ('Australia Card' (1986-87) and 'Access Card' (2006-07)) are sufficiently numerous and striking as to justify intense scrutiny by the Senate.

Submission 3: The Senate should require the Department to explain which (if any) of the more than 30 PIA recommendations not implemented by NEHTA have been implemented by

the Government in the Bill, and the reasons for rejecting the remainder. The Senate should also require the Privacy Commissioner to specify which of these PIA recommendations she supports, and her reasons for rejecting the others. This Bill should not proceed in the absence of that information.

Submission 4: No legislation should ever allow a national identification system to be operated by the private sector. A fortiori, no legislation should allow such a step to occur without the full scrutiny of the legislative process.

Submission 5: When an IHI is allocated, the Bill should provide that either Medicare or the healthcare provider involved to pro-actively provide IHI details to a person when it is allocated.

Submission 6: The Bill should provide and guarantee that the use of an IHI is not a condition of obtaining healthcare, and that it is an offence to make it a de facto condition of obtaining healthcare. There are provisions in the Access Card Bill which attempt something similar.

Submission 7: Cl 9(5) should be deleted and replaced with a right of appeal.

Submission 8: As submitted by the Queensland Office of the Information Commissioner, healthcare providers should seek an individual's consent (which could be a standing consent, but revocable) to retrieve and to use their IHI, except where the lack of the IHI would make the provision of the healthcare service impractical.

Submission 9: Cl 26(2)(b)) should be deleted to prevent function creep, particularly at State and Territory level.

Submission 10: The Mallesons PIA recommendations 7.5.3 and 7.6.2 limiting the use Medicare can make of IHI should be included in the Bill.

Submission 11: Any authorisation of data matching schemes to enable Medicare to build this database should be specifically included, by named organisation, in legislation.

Submission 12: The Department, and the Privacy Commissioner, should be required by the Senate to identify all current situations where disclosures under because cl 15(2)(b) may be authorised under another law.

Submission 13: As Mallesons PIA recommended, there should be a specific legislative restriction on law enforcement and security agencies being generally able to access health identifier information.

Submission 14: As in Mallesons PIA Recommendation 7.18.2, the legislation should require Healthcare Providers to comply with a statutory breach reporting regime. This provision could be repealed when more comprehensive data breach notification laws are enacted.