



## Privacy Blueprint – Unique Healthcare Identifiers

Version 1.0 – 18 December 2006

**Australian  
Privacy  
Foundation**

post: GPO Box 1196  
Sydney NSW 2001  
email: [mail@privacy.org.au](mailto:mail@privacy.org.au)  
web: [www.privacy.org.au](http://www.privacy.org.au)

**Submission to the National E-Health Transition  
Authority (NeHTA)**

**March 2007**

### **The Australian Privacy Foundation**

The Australian Privacy Foundation (APF) is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about the organisation, see [www.privacy.org.au](http://www.privacy.org.au)

We note that the Foundation has not been able to devote as much time to the review of the Blueprint and the preparation of this submission as it would have liked, due to severe resource constraints. The last three months has seen a unprecedented number of important inquiries and reviews to which we have been asked to make submissions, often at very short notice – in contrast to your relatively generous consultation period. While noting these constraints, we acknowledge that NeHTA's previous stages of consultation have given us an opportunity for input to the development of the Framework

### **General Comments**

The Australian Privacy Foundation welcomes the approach to privacy issues taken in relation to this project. In particular, we welcome the extensive consultation to date, the six 'privacy tenets' and the proactive commitment to common privacy principles described in Section 3.1. We commend the approach that recognises that it is not yet known whether the proposed UHI organisation will be a public, private or hybrid organisation and therefore to which privacy jurisdiction it will be subject.

### **Specific Comments**

Comments below relate to selected sections of the document, with particular regard to the specific questions raised in section 4.

While we are primarily concerned with the IHI, as it affects the privacy of patients and citizens, there are also important privacy considerations relating to the proposed HPIs. While there will be significant public accountability interests to balance against the privacy interests of health professionals, they should not automatically lose all rights to privacy.

#### **Section 2.1.1**

We note the risks identified by NeHTA in respect the current arrangements for identifying individuals within the health care system. The Blueprint mentions, for example, the risk of medical results being inadvertently sent to the wrong doctor and/or about the wrong individual where names are similar. The

UHI is intended to prevent such problems from occurring. It is important to note that while a UHI can provide a more accurate way of identifying each individual, the possibility for errors can still arise. For example, human and technical errors will still occur with a UHI system, and sufficient protection needs to be in place to minimise any risks to privacy should such errors occur. There are many examples of systems based on unique identifiers where individuals are sent the wrong material, or contacted in error – sometimes on a more significant scale than occurs with paper-based errors. So while a UHI system should in principle reduce instances of mistaken identity, it is important to bear in mind that such a system is still open to significant errors, and steps taken to protect the data should reflect this reality.

### Section 2.3.1

This section states that “Medicare Australia would be required to undertake appropriate consent and notification processes before the IHI can be created, disclosed and used by the UHI organisation”. However, in a later discussion in Section 4.1, Question 1 mentions that “Medicare Australia would not be able to create any identifiers until individuals provided express consent”. There appears to be some ambiguity here as to who will be creating and issuing the IHI – will it be the UHI Organisation or Medicare? If Medicare will be doing so, will they then retain a record of the identifiers on their system?

From a privacy perspective such a process contains inherent risks to the integrity of the UHI system. Two approaches could be considered to avoid this situation. The preferable approach would be for Medicare to pass on information about individuals who provide consent, and have the UHI Organisation issue the UHI. Or alternatively, if Medicare were to issue the UHI, details of that UHI and the person attached to it should be deleted as soon as the information has been passed on to the UHI Organisations.

The UHI must in no way be linked to any other unique identifiers related to the individual. This point is particularly crucial in the context of the proposed ‘so-called’ Access Card. Our concerns about this National Identity Card project are detailed on our website at [www.privacy.org.au](http://www.privacy.org.au). The government has to date failed to explain how the ‘Access Card’ will relate to Medicare administration. Until such time as the government is prepared to explain this relationship, we submit that any Access Card number or registration must not be linked, or be able to be linked in any way, to a person’s IHI.

Legislation should be enacted to ensure that the IHI is not the same as the Access Card number, and is in no way linked or be able to be linked to the Access Card number or any other existing or new unique identification number.

The public confidence and trust essential for the success of a UHI system will be destroyed if there is any suspicion that it will be used for administrative or enforcement purposes as opposed to health care.

### Section 2.3.5 - Use and Disclosure

The Blueprint states “IHI and HPI data held in the records will be disclosed primarily to providers and provider organisations for use in the course of delivering healthcare to individuals”. The circumstances in which information is disclosed needs to be made more explicit. It should only be disclosed to providers in two circumstances: Firstly, when searching against someone’s details (such as name, DOB and address if necessary) to find what an individual’s UHI number is for the purposes of then using that UHI to attach to a health record. Secondly, when searching against a person’s UHI number to confirm personal details about the person (that is, to confirm details already supplied by the person). The UHI data should not be able to be accessed simply to find out other details about the person that have not already been volunteered by the individual. A person should be able to access health services anonymously (as supported by 3.11 of the Blueprint), and accessing information about an individual using the IHI as a key, where this information is not given to the provider by the individual, may undermine the possibility for anonymity.

### Section 2.3.6

It is stated that the mechanism for managing authorised representatives for individuals may involve the UHI Organisation linking two IHIs. While it is not made explicit in the Blueprint, we take this to mean that the IHI of a carer and the patient, or a parent and their child, for example may be linked. No reason is given as to why this linkage would be necessary. A person should be able to act as an authorised

representative of another without recourse to their IHI. Furthermore, it would seem to involve a potential breach of the primary (or even secondary purpose) for which the carer/parents IHI was issued in the first place – that is, it is not issued to further the health care interests of another person. We request clarification on this point, and suggest it be subject to further consultation.

### Section 3.11

We welcome the support given in this section of the Blueprint to the anonymity principle, where it is practicable. As the Blueprint acknowledges, there are significant areas of health care where anonymity is essential to ensure that individuals present for diagnosis and treatment, and this is not just in the interests of those individuals but also for public health objectives.

### Section 4.1

The question of the scope of activities that can be reasonable characterised as ‘healthcare’ requires further consideration. The first issue is whether the scope of ‘healthcare’ providers should be defined by NeHTA alone or by a wider consensus. The second issue is whether the individual will be bound by this definition, or whether they will be able to chose or ‘opt out’ of using their IHI for certain providers even if they are defined as ‘healthcare providers’ by the overall system. For example, if NeHTA were to include dental practitioners in their definition, but an individual did not wish to use their IHI for dental visits, such a choice must be supported by the system. (This is the same as the point made in the third paragraph under Section 4.2 below.)

### Section 4.2 Key questions

The best way to ensure consent requirements meet relevant privacy laws is to adopt an ‘opt in’ approach. Unless an ‘opt in’ approach is taken, it is difficult to ensure that any consent given is fully informed. An ‘opt out’ approach will not meet the test of ‘informed consent’, as it is impossible to know whether each individual has understood or even read information that is sent to them informing them about the proposal. An ‘opt in’ approach allows individuals to make an active choice about being part of the UHI system, and it is therefore easier to be assured that informed consent has been provided.

If NeHTA were to take an approach of ‘lawful authority and notice’ described in Question 3 of this Section, it is important to note that such an authority must not simply provide NeHTA with blanket authority to apply a UHI to every individual without still also applying the consent requirements. Any such law developed would still need to include guidelines around how informed consent would be sought from each individual before being issued with a UHI. The development of legislation does not therefore take away from NeHTA the decision as to how best to handle consent requirements (as the individual should still be given a choice as to whether or not they want a IHI), though it would have the effect of clarifying in legislation the role of Medicare in collecting information on behalf of NeHTA.

Another consideration with consent requirements is not just a person’s consent to being issued a UHI in the first instance, but their ongoing consent in regards to each transaction. For example, will the individual be able to access the health care system without reference to their IHI if they so choose to do so for a particular transaction? Such an opportunity needs to be supported in the system design to maximise the degree of control individual can exercise over the handling of their health information. (See privacy tenet 3 in Section 1.3)

### Section 4.3.3

We agree with NeHTA that, on a practical level, there will be healthcare administrators who will require access to IHI records for the purpose of processing details relating to a particular health care event. In general, this practice would be reasonably expected by most individuals accessing a health care service. However, while this practice may be relatively straightforward to monitor in relation to single or small health care providers, problems are likely to arise in relation to large health care providers (such as hospitals or health care groups). Therefore, it is important that strict guidelines are developed for access to the IHI by health care administrators to prevent abuse and the chance of errors within the system.

It is important to note that there are some non-health care providers who should in no circumstances be able to access an individual's information via the IHI. Amongst these would be health insurance providers, many of whom are often closely linked to health care organisations. There need to be clear and binding rules preventing such access as an incidental result of particular corporate affiliations.

#### Section 4.4

This section outlines the data fields that will be included on a person's IHI. What is not clear from the Blueprint is whether all fields will be compulsory, or whether some remain optional for the individual to include – clarification is needed on this point. Also, in some instances, the purpose for which a particular data field is collected is not clear – it should be clear to the individual exactly why certain data fields are being collected (for example, for identification purposes only, or to facilitate possible secondary research purposes, or any other reason).

Some of these data fields may raise privacy concerns:

- Home phone number – Is the purpose of this data field to accurately identify the individual? Or is it to provide a contact number for the individual? If for identification purposes, what provision is made for individuals with silent home phone numbers who would prefer not to provide this? If for contact purposes, what provision is made for the individual to provide the preferred contact phone number, rather than home phone number?
- Mother's original surname – Once again is this for identification purposes?
- Birth plurality and birth order – It is difficult to see that such data would be necessary for identification purposes. Is it therefore being collected to envisage possible future health research purposes? As NeHTA has not yet made any decisions about the scope of secondary uses to be supported (see Section 4.8), the inclusion of these data fields cannot be supported at this stage. Further clarification and consultation would be required on this point.

#### Section 4.6

One question raised here relates to a Shared EHR, and asks whether the future potential for this raises further questions. The short answer is yes. A Shared EHR raises numerous privacy questions, none of which have been addressed or considered within the proposed Blueprint. At present the IHI only provides the health care provider with a pointer to basic identification information about the individual – clinical records are explicitly excluded from the project. Using the IHI to access a Shared EHR in effect provides a health care provider with access to clinical information about the individual, not just basic identification data. Such a proposal therefore lies way beyond the scope of this Blueprint. If it is possible that such a use may be permitted in future, then it needs to be dealt with in the scope of this project, and not simply viewed as an 'add on' at a later stage. In that case, NeHTA needs to be open about the fact that the proposed IHI may in future provide a health care provider with access to an individual's clinical information. Without such advice, individuals may not be able to make an informed choice about whether they want to have a UHI, and the privacy tenets on which the proposal is based would be severely undermined.

One approach to this issue would be to make explicit in this Blueprint, and in an accompanying legislation, that the use of an IHI to access an individual's Shared EHR would only occur with the informed and explicit (ie 'opt in') consent of the individual concerned. And further, that the scope of the access would be fully explained to the individual, with the individual being given the ultimate say about which providers may access their Shared EHR using the IHI.

Thank you for the opportunity to comment on the NeHTA Privacy Blueprint. Please do not hesitate to contact us if there are any matters raised here that you would like to clarify or discuss further.