34 PIA recommendations not adopted by NEHTA

Note: These recommendations were often 'referred to government' by NEHTA, but few are adopted in the IHI Bill (requires comparison)

Collated by Graham Greenleaf, UNSW Faculty of Law, 10/03/2010

Galexia preliminary PIA recommendations

To manage community expectations about the national ID potential through IHI function creep, limits should be strengthened on the use of the IHI by prohibiting its use outside the health sector in specific legislation.

The full PIA will need to consider the legal restrictions on the adoption of a Commonwealth identifier by private sector organisations. The legal restriction may be waived by prescription in Commonwealth government regulations

Clayton UTZ PIA recommendations

Recommendation 1 – The regulation of the handling of UHI Services requires a new regime instead of the current patchwork of Australian privacy laws

We recommend that there be new national privacy rules (possibly in the UHI Services enabling legislation) which cover, to the exclusion of existing privacy rules, the handling of UHI information provided to or by the UHI Services or derived from a IHI or HPI-I record. These new rules should:
• be the same for the UHI Operator and all the UHI Services User organisations and downstream users (unless there are compelling reasons for different treatment);
• not vary in their application according to whether UHI information might currently be characterised as health information or not because an organisation collected the UHI information in the course of providing a health service;
• be developed by focussing first on what the policy should be as to the intended, permitted and prohibited collections, uses and disclosures of UHI information without being constrained by current privacy law concepts of "health information", primary purpose and secondary purpose of collection of individual collectors and NPP 7 like identifier principles. These are inadequate mechanisms on their own to create the nuanced rule set needed for regulating the handling of UHI information, although they might be used as part of that rule set.

Recommendation 3 – Consent of individuals to activation and deactivation and production of IHIs and HPI-Is.

We recommend that NEHTA continue its current design setting of providing a choice to each individual as to whether to activate an IHI or HPI I and a choice to deactivate an IHI or HPI I. This is a strong pro privacy feature of NEHTA's design.

Recommendation 6 – Consent of individuals to activation and deactivation and production of IHIs and HPI-Is.

We endorse NEHTA's policy that having an activated IHI will never be a prerequisite for obtaining healthcare. However, it is not clear whether this means that an individual who has an activated IHI has a right not to produce their IHI after treatment (for example, as a health insurance or professional indemnity insurance or

professional practice obligation or other requirement) or not have the IHI later linked with the record of their treatment episode.

We recommend that NEHTA consider and state whether an individual with an activated IHI who wants not to provide their IHI in respect of a treatment episode to reduce the risk of any record of the occurrence or content of that treatment episode (held by the treating health provider or any other organisation) being linked to their IHI (and hence linked to other records about the individual which also include their IHI (whether those records are held by the treating health provider or not) will be able to effectively exercise that choice.

Recommendation 10 – Searching the IHI Record [rejected as IHIs now compulsory]

Recommendation 11 – Update of IHI records before activation [rejected as IHIs now compulsory]

Recommendation 12 – Use and disclosure of IHI records before activation [rejected as IHIs now compulsory]

Recommendation 13 – Opting out of the IHI Service [rejected as IHIs now compulsory]

Recommendation 14 – Function expansion

We recommend that the legislative and governance underpinning of the UHI Services include a public and transparent statutory process to consider all proposals for any significant function expansion of the UHI Services (as to features, Users or uses of UHI data) to ensure that proposals for function expansion on the grounds of administrative convenience, efficiency and cost savings are balanced against the privacy impact of such proposals. The advice of an independent advisory board and public submissions should be taken before any authorised expansion of features, uses or Users is permitted.

Recommendation 15 – Controlling unintended uses and disclosures of UHI information

We recommend that instead of relying on an identifier privacy principle like NPP 7, constraints on the adoption, use and disclosure of IHIs and HPI Is and the associated records would be best achieved by:
(a) legislation, which:
(i) regulates the persons and purposes for which the IHIs and HPI Is may be used within the healthcare sector and possibly allowing that such purposes may be expanded by obtaining the consent of the relevant individual; and
(ii) prohibits the use of IHIs and HPI Is outside the healthcare sector, which prohibition is (like NPP 7) not able to be overcome by obtaining the relevant individual's consent to wider user or disclosures;
(b) terms in the relevant UHI Services participation agreements; or
(c) both (a) and (b).

Recommendation 19 – Retention and destruction of UHI information

We recommend that proposed uniform national rules regarding retention and destruction of UHI information including UHIs, UHI records and information obtained from UHI records be established (possibly in the enabling legislation for the UHI Services).

Mallesons Stephen Jaques PIA

Recommendation 7.4.1

An appropriate privacy management framework should be established, including the following elements:
(a) robust, transparent and public mechanisms for the assessment of privacy impacts of each new use of the IHI
(b) robust, transparent and public mechanisms for the assessment of privacy impacts before any decision is made to widen the class of agencies and organisations that can directly or indirectly collect an IHI or other data from the HI Service
(c) robust, transparent and public mechanisms for the assessment of privacy and other impacts before any material change is made to Medicare Australia's systems and procedures affecting the HI Service
(d) robust, transparent and public mechanisms for the assessment of privacy and other impacts before any change is made to the form of participation agreement used in relation to the HI Service
(e) robust, transparent, public, well resourced and effective mechanisms for monitoring the collection, use and disclosure of IHIs or other data from the HI Service:
(i) by Medicare Australia
(ii) in the provision of healthcare services, or
(iii) in any other field of endeavour, and
(f) robust, transparent, public and decisive action, promptly taken, to prevent and mitigate the effects of any inappropriate use of IHIs or other data from the HI Service.

Recommendation 7.4.2

The framework should not rely on rule making powers that are not robust, public and transparent.

Recommendation 7.4.3

Consideration should be given to establishing a separate statutory authority as the HI authority which could sub-contract the issue of IHIs and the operation of the HI Service to Medicare Australia and supervise Medicare Australia's activities in its role as HI Service Operator.

Recommendation 7.4.4

Consideration should be given to whether State and Territory instrumentalities wishing to use the IHI should be required to implement the same minimum governance standards discussed in Recommendation 7.4.1, and should be subject to requirements no less effective than the IPPs that govern Medicare Australia.

Recommendation 7.4.5

It is proposed that Privacy Act restrictions on use of identifiers (NPP 7 or UPP 10) should not restrict the use or disclosure of information that includes a health identifier for funding, management, planning, monitoring, improvement or evaluation of health services and for research purposes

in the public interest subject to the same limits that apply to health information being used or disclosed for those purposes.
If that proposal is implemented, a regulatory body (such as the HI authority if established pursuant to Recommendation 7.4.3) should monitor agencies and organisations relying on that provision. In accordance with those limitations on the use of health information, the collection and use should not take place if the relevant purposes are able to be effectively satisfied without collecting IHIs.

Recommendation 7.5.1

For any change in a Medicare Australia policy that is used in relation to the HI Service, provision should be made for a PIA to be conducted to consider the impact of the change on individuals.

Recommendation 7.5.3

The enabling legislation for the HI Service should specify that NPP 7 and UPP 10 apply as though, in relation to IHIs, Medicare Australia has no functions other than its functions as the HI Service Operator.

Recommendation 7.6.1

The enabling legislation should clarify that the sole secondary use that may be made by Medicare Australia of data from the HI Service is in carrying out data quality maintenance and audits of IHI Datasets, subject to the approval of additional purposes through the process in Recommendation 7.4.1.

Recommendation 7.6.2

The governance framework should include robust, transparent and public mechanisms for the assessment of privacy impacts of each material expansion of the HI Service, or use of the IHI or other data from the HI Service.

Recommendation 7.7.1

Commonwealth, State and Territory Governments should consider explaining what designs (if any) other than a voluntary opt-in model were considered as alternatives to the present universal IHI model, including an “opt out” model or a federated model, and the reason for rejecting those alternatives.

Recommendation 7.8.1

The HI Service should make provision for services provided in highly sensitive circumstances - such as healthcare services to prisoners in custody or in psychiatric hospitals - to be provided under a pseudonymised IHI as a matter of course, or for IHIs not to be used in those circumstances.

Recommendation 7.8.2

Consideration should be given to allowing individuals to remain anonymous in respect of the HI Service, but still obtain a Medicare benefit for the healthcare service. For this purpose, the regulation framework (including

participation agreements) could encourage or require Healthcare Providers to separate the collection of IHIs at the point of treatment from the collection of Medicare card data at the point of payment. This would facilitate the true availability of anonymous services.

Recommendation 7.8.3

Rather than requiring individuals to obtain an Unverified IHI by citing one or more sets of assumed names and/ or assumed dates of birth, consideration should be given to providing for an explicit category of "anonymous" IHIs which will not require the individual to nominate a unique assumed name. One option would be to permit patients to register as, for example, "Anonymous Male Patient", with date of birth recorded simply as the birth year without day or date. At the option of the individual, the same "anonymous" IHI should be able to be used on multiple occasions.

Recommendation 7.8.4

In addition to, or as an alternative to Recommendation 7.8.3 consideration should be given to allowing Healthcare Provider Organisations to establish a single IHI for use by all individuals seeking anonymous healthcare at that organisation.

Recommendation 7.8.7

Commonwealth, State and Territory Governments should consider specific restrictions in the design of the HI Service that would prevent the use of Verified IHIs by Healthcare Provider Organisations being made a condition of State or Territory funding.

Recommendation 7.9.2

Consideration should be given to expressly preventing access to IHI Datasets, or collection or use of IHIs by organisations or government agencies for services and programs not directly related to healthcare.

Recommendation 7.11.1

Serious consideration should be given to removing the ability to batch search from the design of the HI Service, or limiting batch searching to existing, active patients.

Recommendation 7.13.1

Security breaches in relation to access to the HI Service should be subject to sanctions under the enabling legislation for the HI Service and those sanctions should be effectively enforced.

Recommendation 7.14.1

Consideration should be given to a specific legislative restriction on law enforcement and security agencies being generally able to access information held for the purposes of the HI Service.

Recommendation 7.15.3

The audit log as made available to an individual should include the name or address of the Healthcare Provider Organisation that retrieved that individual's IHI from the HI Service. This will assist individuals in identifying which organisations have accessed their IHI and identifying unauthorised access.

Recommendation 7.16.1

Individuals should be informed when changes are made to their IHI Dataset as a result of replica or duplicate IHIs, at all relevant addresses, to assist the individual in managing any privacy impacts associated with a replica or duplicate IHI.

Recommendation 7.18.2

NEHTA should consider the inclusion of a "breach reporting regime" either in the enabling legislation for the HI Service, or in the participation agreement between the HI Service Operator and Healthcare Provider Organisations.