Australian Privacy Foundation

G.P.O. Box 1196
Sydney NSW 2001

enquiries@privacy.org.au

http://www.privacy.org.au/

13 August 2009

Healthcare Identifiers and Privacy Submission
Primary and Ambulatory Care Division (MDP 1)
Department of Health and Ageing
GPO Box 9848
CANBERRA ACT 2601

ehealth@health.gov.au

APF RESPONSE TO AHMAC PAPER: *HEALTHCARE IDENTIFIERS AND PRIVACY: DISCUSSION PAPER ON PROPOSALS FOR LEGISLATIVE SUPPORT*

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. I am writing in my capacity as Chair of the Health Sub Committee of the APF*.

From at least the early 2000s, the challenges for implementing a unified, national eHealth system has centred on the development of an Australian approach to the establishment of "a single set of clear policies and procedures which complies with all relevant obligations and has universal application to all entities (whether public or private sector) and individuals in all Australian states and territories" (Health Connect, Legal issues report. Prepared by Clayton Utz for DOHA. January 2005).To achieve this, experts have indicated that a systematic and transparent approach must be taken to privacy compliance. In this context, the "Healthcare Identifiers and Privacy: Discussion paper on proposals for legislative support" demonstrates a massive failure of project policy, governance and transparency.

We will first outline these fundamental problems with the government's approach to this issue, then detail the deficiencies of the IHI proposals contained in the Discussion Paper. This submission does not deal with Individual Healthcare Provider Identifiers, though they do raise privacy issues concerning healthcare professionals.

PART 1: DEFICIENCIES OF PROJECT POLICY, GOVERNANCE AND TRANSPARENCY

Several Privacy Impact Assessments (PIAs), authorised by various health authorities over many years, have yet to see the light of day despite the billions of dollars of tax payers' money that has been expended by government on eHealth implementation thus far. Neither have many pertinent publications or consultations with key stakeholders been published. Indeed, from the Clayton Utz "Legal Issues" report, one

might infer that the feedback from a succession of PIAs have been so poor as to erode public perceptions with regard to the trust-worthiness of eHealth. Even without the benefit of a series of suppressed or now aborted PIA report findings, publications and consultations, it is clear that public trust underpins successful eHealth implementations (p.42).

The range of privacy enquiries authorised by health authorities at NEHTA include, to our knowledge, the following:

1. Some preliminary work on unique health identifiers (UHIs) for health in 2006
2. The PIAs alluded to in NEHTA's "Privacy Blueprint – Unique Healthcare Identifiers" (http://www.nehta.gov.au/privacy).
3. A series of discussions by the Consumer & Clinician Forum during 2006-07
4. NEHTA's approach to privacy v1.0, July 2006
5. The Privacy Roundtable on November 17 2006
6. Privacy Blueprint - UHIs v1.0 - December 2006 (at Privacy Context and Strategic Directions)
7. The Shared Electronic Health Record (SEHR) Privacy Roundtable on 28-29 June 2007]
8. The Secondary Uses Roundtable in November 2007
9. Privacy Blueprint for the Individual Electronic Health Record July 08
10. Privacy Blueprint for the Individual Electronic Health Record - Report on feedback November 2008, which was subsequently unpublished but is referenced in NEHTA PowerPoint presentation, of May 2009.
11. A PIA on UHIs that was conducted in early 2008
12. NHHRC Supplementary Paper to its *Interim Report - Person-controlled Electronic Health Records for Every Australian* (30 April 2009)
13. The PIA on IHIs commissioned in January 2009 and referenced at the consultation workshop on May 29th 2009.
14. Final Report of the NHHRC *A healthier future for all Australians* - June 2009

The range of PIA reports authorised by health authorities at DOHA and its predecessors include, but are not limited to our knowledge, the following:

1. The Electronic Consent Symposium 16th & 17th July 2002
2. National Health Privacy Code (draft) Consultation Paper, The Australian Health Ministers' Advisory Council, National Health Privacy Working Group, December 2002
3. COAG Health Working Group - Consumer Consultation 25 October 2006
4. National eHealth Strategy forum, 30 March 2009

Dr Ian Reinecke, former CEO of NeHTA, recognised that "the UHI Service will only be successful if it meets community expectations regarding privacy" (http://www.computerworld.com.au/article/172112/privacy_blueprint_released_e-health, 2007). Yet the evidence suggests despite a lot of work and many consultations, findings have been mostly set aside because answers were not what health authorities wanted to hear, particularly with regard to the role of consent. The "Healthcare Identifiers and Privacy: Discussion paper on proposals for legislative support" fits comfortably into this history when one considers that;

1. Part B of the discussion paper is about the overall health privacy framework and must therefore cover SIEHRs. This fact conflicts with DOHA insistence during consultations around Australia with various stakeholders indicating that at this stage, they were only looking for feedback about the UHIs. Why is fragmentation part of the consultation landscape? The fragmentation provides a telling example of the current, Australian eHealth policy shambles!

2. Stakeholder submissions and consultation feedback will not be published on the DOHA website

3. Public consultations as to the paper are only open to specifically invited stakeholder organisations and not all stakeholders (public discussion is vital), and

4. The paper dismisses crucial governance concerns as something to be sorted out at a later stage, after an Australian IHI is implemented.

The APF believes the discussion paper and associated plans represent a massive failure of project policy and governance. A widely consulted and accepted governance framework needs to be negotiated with consumers before Australians can have a much needed rational debate about eHealth implementation. In the interim, despite our obvious frustration at the management of the issue, the APF will continue to engage with health authorities because it is critical to publicly and transparently debate the basis for consumer confidence in eHealth.

PART 2: SPECIFIC CRITICISMS OF THE IHI PROPOSAL IN THE DISCUSSION PAPER

The limited detail of the proposed IHI scheme provided in the "Healthcare Identifiers and Privacy: Discussion paper on proposals for legislative support" suggests that the scheme is highly privacy invasive and is remarkably similar to earlier attempts to introduce universal mandatory national identity systems, including both the Australia card in the 1980s and, more recently, the so-called 'Access card'. The APF is vigorously opposed to the introduction of, what current evidence suggests, is a new mandatory national identity scheme using a number. Nonetheless, we do **support** notions of patient centred eHealth systems and maintain a national system of IHIs has nothing to do with implementing Australian EHR. Furthermore, **the IHI scheme poses many risks to consumers while there are acceptable alternatives that do not**. Specific APF criticisms of the proposed IHI as set out in the Discussion Paper are outlined below.

PART A

1. The Medicare CDMS database underpins Medicare Card Numbers although unlike the card, which may list several family members, it stores an entry for every person. The new IHI database will be populated by a data dump from the CDMS into a new numbered database that will be linked to the Medicare number so the new number can be found – it is not clear that patient identity will be validated at this stage. This is of concern given Medicare's "well-publicised difficulties with data quality" (Dearne, K. Medicare the base for e-health IDs, the Australian IT, June 23 2009).
2. The APF seeks clarification about where the IHI data will be held. Assurances about functional separation, while using the same platform for both the IHI and Medicare claims data is a serious concern (Figure 1, p.27). Will storage be centralised in the same physical location as Medicare data is stored?
3. The APF seeks clarification of whether a patient who is anonymous for the purposes of an IHI can claim a Medicare rebate, as has been suggested by senior DOHA personnel.
4. Terminology used in the AHMAC paper is confusing. Although there is some continuity in terminology over various documents, for instance NeHTA's UHI (Unique Healthcare Identifier) program includes an IHI for individual consumers, a HPI-I for health care providers and an HPI-O for health care organisations as does the discussion paper, they seem to have been muddled. We request a plain English version of the discussion paper be made available for public debate.
5. The Foundation is also dismayed by the expenditure of at least $5 billion dollars of taxpayers' money to implement a unified Australian eHealth system that seems to establish a goal in one direction only to reverse this and work towards a contradictory goal at a later stage and so on in an ongoing loop for several years (Dearne, K. E-health strategy should be national priority in 2009, says leading software vendor The Australian IT, January 5 2009).
6. The current proposal stores data from an insurance program alongside that of a health services identity record system. The co-location of the two sets of data enhances the 'honeypot' that those with malicious intent may seek to access with regard to the growing problem of identity fraud and which will be attractive to other government agencies for other purposes.
7. The discussion paper also declares the intention not to arrange for open consultations in each state and territory, with only a series of meetings planned with specifically invited consumer groups over the coming 4 weeks or so. This is contrary to common practice for the majority of government enquiries and consultations in most Australian jurisdictions.
8. The lack of open consultation is also inconsistent with recent and pending FOI reforms (http://www.privacy.org.au/Papers/CthFOIReform-0905.pdf). Although the decision not to publish submissions is apparently intended to re-assure submitters that they can be candid, this is undermined by the mention that submissions will be shared between relevant government agencies, and subject to FOI access (p.7,

para 1). The Australian public require transparent access to information about the IHI proposal, including information about the pressures applied to the government by groups with a commercial interest in the outcome.

9. Also, the Privacy Impact Assessment known to have been commissioned by NeHTA in early 2009 has not yet been made public. This is unconscionable and suggests that proponents are not being open and honest about the eHealth projects.

10. Artificial attempts to rule comment on related issues like the shared individual electronic health records (SIEHRs) as 'out of scope' are not logical. IHIs are declared to be necessary precisely because of their asserted value in facilitating other e-health initiatives, so how can anyone sensibly comment on the IHI proposals without setting them in the real-life context of those other initiatives? This seems inconsistent given reference to the other initiatives in the discussion paper when putting forward justification and asserting benefits, unsupported by any evidence (e.g. Executive Summary and p.16).

11. Deciding on IHIs before agreeing on the SIEHR context in which they will be used is putting the cart before the horse. Only when there is a clearer idea of how SIEHRs will work can one then analyse whether and to what extent IHIs are necessary and appropriate.

12. Difficulty and delay in agreeing on a national health privacy framework is given as a reason for needing to go ahead separately with a legislative framework just for IHIs, but it can equally be seen as precisely the reason why national IHIs should NOT be introduced until there is an agreed and implemented national health privacy framework and detailed consideration of all alternatives. As the old adage points out - "marry in haste, repent at leisure". While AHMAC's impatience with the slow pace of e-health reform is shared by health consumers, AHMAC's proposed solution - to proceed without resolving fundamental privacy concerns - is not. Haste in implementing IHIs without the resolution of privacy issues will surely only lead to further complications down the track. The APF's approach is consistent with that of the NHHRC in its Interim Report, which stresses the need to ensure 'that people control access to their own health information', and personal 'ownership of a person-controlled electronic health record'. They regarded this as 'a fundamental outcome of adoption and implementation of e-health applications'.

13. Despite mention of arrangements for access to information between a patient's healthcare team in the paper there is no reference to patient access to IHI information and the associated audit trails of access and use. When will routine patient access be discussed, analysed and implemented for eHealth? Legitimate concerns about the way in which the IHIs will be used, the safeguards that will apply and in particular the extent to which individuals will have control, need to be addressed urgently. The current IHI proposals are inconsistent with the NHHRC's approach, because they allow access to IHIs without explicit requirements for patient consent.

14. The policy outlined in the discussion paper is not evidence-based. Most of the benefits asserted are those associated with improved communications and record keeping. The paper does not establish any clear links between establishing a national IHI and realisation of these benefits. They are simply assumed as 'an article of faith' despite several publications casting doubt on the effectiveness of such implementations (e.g. Ammenwerth et al. 2008 The effect of electronic prescribing on medication errors and adverse drug events: A systematic review).

15. The discussion paper makes no consideration of alternatives or related developments that may deliver the improved health outcomes the paper claims as a benefit of the IHI. These include the establishment of interoperability standards for eHealth to support better communications networks between health care providers and organisations, such as has occurred in the USA (https://regepi.bwh.harvard.edu/re/projects) or multinational OpenEHR efforts (http://www.openehr.org/home.html).

16. The repeated obsession with 'identification' is misplaced – in many cases the desired objectives can be realised by appropriate 'authentication' – without the third parties necessarily needing to know the actual identity of a patient.

17. Individuals will in practice (if not in law) be required to use an IHI for two reasons. First, the IHI must be used to receive Medicare benefits, which most of us need. Second, irrespective of whether an individual claims a Medicare benefit, health care providers may decide to make use of the IHI as a condition of service, as they will be entitled to do. Overseas experience suggests this will indeed be the case in Australia (http://www.computerworlduk.com/management/government-law/publicsector/news/index.cfm?newsid=15042). In the debates over the Australia Card and the Access Card, very similar arguments for the 'voluntary' nature of these proposals were correctly derided as 'pseudo-voluntary'. The IHI is no different, and the argument is just as misleading.

18. The discussion paper is inconsistent and weaves between an emphasis on security and confidentiality of the IHI on the one hand and the scheme design on the other hand. That is, the scheme is designed so one's IHI will be stored in the patient record systems of thousands of health care providers, accessible to hundreds of thousands of individual health care professionals and support staff. The discussion paper indicates that it will even be printed on discharge summaries and prescriptions (p.16). It may also become the property of commercial Personal Health Records providers so that if patients move from one provider to the other, the first provider will still "own" one's health data and IHI. In effect, an individual's IHI will not be under the control of the individual, and as a result may become something akin to public information. This is inconsistent with the NHHRC's proposal for individual ownership of health records.

19. Analogies with existing health care identifiers and record keeping systems are misleading. The IHI will, for the first time in Australian history, provide a single key to an individual's entire health care history from birth to grave.

20. Re-assurance about no change to arrangements for anonymous health care services in the discussion paper is misleading. Anonymous health care will

only be possible for the few services where one may be able to obtain health services without evidence of identity and without using a Medicare number for a rebate. Given the aftermath of recent economic downturns, cost is likely to present a significant barrier to anonymised health care services, regardless of the probability that some of these, such as a few sexual health, mental health and drug rehabilitation services may be separately funded. The discussion paper does not address the many services where privacy-conscious individuals currently rely on the fragmentation of record keeping systems and separate patient identifiers to give them 'effective' anonymity (Fernando, J. (2008) An analysis of current clinician security practices while using health information systems security in Australian public hospitals. Unpublished PhD thesis, Monash University).

21. A single national IHI, used in every health provider's patient record system, will make an individual's health care history much more 'transparent' to thousands of authorised users, and potentially to unauthorised users (no system can ever guarantee that there will never be security breaches nor unauthorised access).

22. Even without any clinical information, the audit trails of access to the IHI register, which is necessary to ensure access control and security, will in effect constitute a crude profile of an individual's health care history. It will detail all of the health care providers an individual has interacted with and when these interactions occurred. The link between individual health care professionals and the organisations they work for and their 'speciality' will be readily accessible from other sources, so that access to the IHI service audit trail will effectively reveal considerable detail about the likely health care received.

23. The discussion paper provides no guarantees about strict limits on access to the IHI service audit trails, beyond the 'standard' privacy principles (PPs). The PPs in most Australian jurisdictions allow a wide range of secondary uses and disclosures, which most people would find objectionable, and this conflicts with assurances by health authorities to the APF earlier this year that NO secondary uses or disclosures of the IHI would be permitted. Yet governance arrangements to protect the IHI have not even been planned. Moreover, the discussion paper already provides a list of permitted secondary uses of the IHI that will make it available to the Police, Centrelink and tax authorities, to name a few of the commonwealth, state and territory bodies that may access an IHI (P.16). The APF maintains that once secondary uses of the IHI are permitted, other permitted uses will follow.

24. The role of Medicare needs to be questioned. Medicare's primary functions relate to administration of health care benefits, not to health care as such. There is far too great a potential for conflict of interest concerns to put it in charge of the IHI service. It will be enormous temptation for Medicare to see the IHI as a tool for better administration and expenditure control, including in auditing health care professionals claims patterns and history (Clarke & Fernando (2009) Enquiry into compliance on Medicare audits, http://www.privacy.org.au/Papers/MBSCompAudit-Supp-090506.pdf). The history of Medicare ambitions in relation to previous national identity scheme proposals such as the original Australia Card, the proposed

Medicare smartcard and the Access Card needs to be acknowledged (APF (2008) Campaigns: The National Identifier Scheme. http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html).

25. The IHI service cries out for independent governance – even if Medicare is contracted to operate the service. Separation of governance and implementation is emphasised by the National Health and Medical Research Council (NH&MRC) when outlining respectful and ethical ways to avoid community perceptions of coercion (National Statement on Ethical Conduct in Human Research (2007) Section 5: Processes of Research Governance and Ethical Review. http://www.nhmrc.gov.au/publications/ethics/2007_humans/section5.htm). The IHI scheme as outlined in the discussion paper is not a respectful service and so does not comply with the Australian Charter of Healthcare Rights that was recently endorsed by all COAG members (http://www.safetyandquality.gov.au/internet/safety/publishing.nsf/Content/52533CE922D6F58BCA2573AF007BC6F9/$File/17537-charter.pdf).
26. National consistency is important not only between states for information handling, movement of health providers among jurisdictions, as well as movement of consumers, but it is also important for the cross-over aspects between public and private providers. The design of an appropriate eHealth system would therefore fit a common standard and reduce cost.
27. Besides the law, governance and implementation must also be consistent. This will simplify the training of both providers and consumers.
28. The APF is not simply concerned about the identifiers, but also about the actual information collected, stored, shared, accessed, secured, modified, saved and amended, to which the IHI will be a key. The discussion paper has a sole focus – on identity. What steps have been developed to ensure ongoing and consistent data quality that does not depend upon the individual correcting potential errors?
29. If no technical barrier, legislation alone won't stop banks etc using the IHI as a defacto national ID number. This is contrary to federal government policy, and in particular to promises made by Ministers Roxon (as Health Minister),
30. Ludwig (as Human Services Minister) and Plibersek (when she was Shadow Human Services Minister, 2006-2007).
31. Date of birth and name do not provide an adequate basis for selecting an IHI from a list given the frequent issue of mistaken identity that we have noticed on social networking sites such as “Facebook”. The system outlined in the discussion paper cannot guarantee that the patient wouldn’t be mistaken and the wrong records updated as a result (p32). Human error may result in deadly consequences for the patient.
32. The APF has serious questions about data quality and the IHI scheme design if, as explained, Medicare will use its existing records to initially assign IHIs. Existing data quality problems have been acknowledged by health authorities and are likely to be built into the IHI service from the outset. How then will the IHI prove to have higher integrity and be more reliable than current health information? And if it isn’t then many of the claimed benefits of an IHI

Table 1 Updated comparison between the Australia Card proposal, the Access card proposal and the IHI proposal

This table edits and updates 'Table 1 Compulsion and Coverage', Greenleaf, G. Australia's proposed ID Card: Still quacking like a duck (2007) http://www.austlii.edu.au/au/journals/UNSWLRS/2007/1.html with (a) details of the final version of the Access Card proposal (Exposure draft, *Human Services (Enhanced Service Delivery) Bill*) from Greenleaf, G (2008) 'Function creep defined but still dangerous in Australia's ID card Bill' *Computer Law & Security Report*, (2008) Vol 24 No 1, 56-66 at http://law.bepress.com/unswwps/flrps/art64/ and (ii) publicly available information about the IHI proposals, particularly from the Discussion Paper.

Point of comparison	***'Australia Card' proposal 1986-87***	***Access Card proposal 2006-***	***IHI Proposal 2009***
Adult coverage	Every adult	Every person eligible for a Cth benefit (cl 19)	To 'all individuals who receive healthcare in Aust.' (DP A.3.1)
Children	Card from birth	No card until 18; Listed on parents' cards	IHI from birth
Compulsory?	'Pseudo-voluntary' – top marginal rate of tax payable unless presented for transactions; no access to social security or health insurance benefits	'Pseudo-voluntary' – no Medicare benefits or other medically-related government benefits unless produced; any other parties free to 'request' card when services are provided	IHI automatically assigned; ascertainable from MCN; production of MCC 'pseudo voluntary' – *de facto* condition of Medicare benefits; uncertain whether may be required by HCPs[1]
Carriage?	No legal compulsion to carry (cl 8) – except when required to produce (very often)	No legal compulsion to carry – except when required to produce (to a medical practitioner assessing eligibility for a Cth benefit; and where claiming a concession)	No legal compulsion to carry – except when required to produce MCC (as above)
Confiscation?	• Illegal to confiscate if produced voluntarily (cl 170(1)) • Uncertain - confiscation 'for good cause' on compulsory production	Purported individual ownership of card (cl 88) deceptive, as normal rights of ownership removed in cl 80 and elsewhere. Position of confiscation uncertain.	Can MCC be confiscated and by whom?[2]
Registration requirements	Attend government office to prove identity	Attend government office to prove identity; POI documents necessary, as determined by Dept. (cl 19, cl 22)	Automatic allocation if current MCN (DP A.3.1) [uncertain] Reliance solely on Medicare CDMS as basis is implausible (low security)
Preventing issue of fraudulent IDs	Registration requirements	Registration requirements and comparison of photograph templates (Case Study – Fraud; Fact Sheet - Technology); documents presented to be checked against new Document Verification Service (DVS)	[uncertain] May be partial re-registration necessary to obtain higher security.
Re-issue	[uncertain]	7 years; new photo required (original proposal)	[uncertain]
Lost/stolen cards	[uncertain]	[uncertain] Fee to re-issue	Lost/stolen MCCs now more dangerous

1 DP A.3.1: 'will not need to be declared to obtain health services'; does not say HPI-Is will be prohibited from requiring IHIs; leaves open HPI-Is 'requesting' IHIs (which can be used in all e-health information transactions: A.3), and provision of services being slower and more difficult if it is not provided; since Medicare number ***is required*** in order to obtain Medicare (insurance) benefits, and IHI is linked to MCN and accessible by any HPI-I, IHI ***in effect*** must be provided whenever Medicare benefits are sought.

2 Medicare legislation and regulations do not refer to the Medicare Card.

evaporate. If new enrolment or evidence of identity processes will be introduced then this needs to be made clear, and will understandably arouse suspicions about whether this is yet another national identification scheme in disguise See Table 1, above).

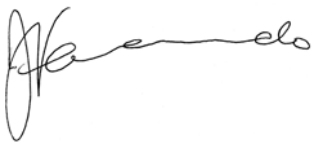
Part B:

The second part of the discussion paper, Part B, has put the cart before the horse for a number of reasons:

1. The Privacy Impact Assessment has not been released.
2. The Privacy Act itself should be the foundation. It is not appropriate for a health focus to be leading the way on redesign of the Privacy Act and the implementation of the UPPs. There is no guarantee that the ALRC's proposed reforms to the Privacy Act will ever occur, and even less likelihood that they will occur within the time-frame of the proposed introduction of IHIs.
3. UPP2, Modification to 2.5(f) is of concern and must involve guidance from the Privacy Commissioner and human research ethics committees.
4. UPP6 has no health function. What is the purpose of incorporating direct marketing provisions into the UPPs?
5. UPP6: Individual informed consent MUST be obtained for the use or disclosure of health information for direct marketing purposes as well as for the use or disclosure of patient information for commercial purposes. NPP6 would be improved by affording this protection both to identified and unidentified patient information. The Discussion Paper's approach is inconsistent with the NHHRC's insistence on patient consent as the foundation of electronic health records.
6. Point 5.1.4 assumes many access exemptions without debating the need for amendments to the Privacy Act in the first instance, focussing on access for the media or under FOI rather than enhancing individual privacy. A Privacy Act amendment debate needs to occur BEFORE reviewing or editing the UPPs, not as an afterthought. The discussion paper suggests health authorities are more concerned about exemptions enabling access to sensitive information rather than in protecting individuals. Why are we discussing draft UPPs at this point, isn't this yet another case of putting the cart before the horse? Are amendments to the Privacy Act an afterthought?
7. In response to the treatment of deceased persons, health information should be protected differently from other information because of the potential revelations about third parties (relatives). The comparison should be to protections of other persons, not just compared to 'other information about deceased persons'. The Foundation would support a time limit for this additional protection, possibly of 10 years.
8. Patient trust, especially with regard to the health privacy legal context, is evidently at the heart of plans for a national e-Health system (p.42). Yet the APF continues to receive communications like this:

> "*a junior Dr [name deleted] at X hospital, ([name deleted]) disclosed sensitive and damaging information about me to a ward full of patients. Not only did the breach occur but the information she gave out was completely incorrect. Regardless it has had devastating effects for me, both in my career and personal life and also in the respect that I now have to try and trust health professionals.*
>
> *[Name deleted] hospital's staff and management have proven beyond a shadow of a doubt that medical professionals should not be trusted for any reason. In terms of eHealth I wonder if there is a way to let the general public know exactly how "above the law" doctors and hospitals already are, before we grant them even more power. Furthermore, how about we give some power back to us "consumers". If doctors can electronically send around whatever information they like about us in a deregulated fashion then it is only fair that the general public is protected. I believe strongly that misusing patient information and breaching privacy should result in a doctor being heavily fined or deregistered. If there is no punishment for such behaviour (let's face it our privacy commission is nothing more than a token gesture) then why WOULD eHealth be used properly?"*

In closing, the APF wish to reiterate the point made earlier. Unified national eHealth implementations do not technically require an IHI, although bureaucrats may find them useful. Interoperability standards or archetypes or both, not an IHI, underpin future-proof and effective eHealth implementation.



Dr. Juanita Fernando
Chair, Health Sub Committee
Australian Privacy Foundation

Dr Fernando is in Medicine, Nursing & Health Sciences
Monash University 03 9905 8537 or 0408 131 535
mailto:Juanita.Fernando@med.monash.edu.au

* This work has benefitted from consultation with the Board Members, Australian Privacy Foundation

Contact Details for the APF and its Board Members are at:
http://www.privacy.org.au/About/Contacts.html