Australian Privacy Foundation

G.P.O. Box 1196
Sydney NSW 2001

enquiries@privacy.org.au

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

6 January 2010

Re: The exposure draft Healthcare Identifiers Bill 2010

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.

The Foundations' feedback to the exposure draft Healthcare Identifiers Bill 2010 is listed below.

1. The APF policy statement in relation to eHealth data and Identifiers has been brought to the attention of senior health officials and has been publicly available for several months at http://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf (Appendix A). The policy, which restates submissions we have made repeatedly over many years, is completely overlooked in the draft HI Bill.

   The APF submits that the draft legislation fails to take account of significant privacy concerns despite these having repeatedly been drawn to the attention of senior health officials.

   Because this initiative is at odds with the APF's stated policy on the matter, we reiterate our opposition to this initiative in its entirety.

   If the Department is intent on continuing down this path, despite the serious concerns, then we draw the following specific defects to your attention.

2. The draft HI Bill enables data linkage of identifiable personal information which is designed to support an electronic health record that, according to senior government officials from NEHTA and DOHA in late November last year, has not even been drafted may never be implemented.

   The purpose of devising a national identity structure to link a health record that may never be implemented is of serious concern.

3. Confusion reigns as to whether the identifiable information will be accessible to the person about whom it concerns or their carers. This is because information provided in the "Concept of Operations" and the "Update on

legislative proposals for healthcare identifiers" documents on the one hand, refer to consumer access to the HI system from implementation, but senior spokespersons from NEHTA and DoHA indicate the contrary (1,2). The spokespersons received a question directly asking about consumer access arrangements from audience members at the HI service Stakeholder Briefing Forum in the ACT on November 20 last year. Responses to the question were, firstly, that "Consumers will be given access afterwards [sic]" and secondly, that "Consumers will eventually be able to use their PIN number and a web portal. Web services will initially be given to providers but **not** to the consumer- this needs to be added at this stage" respectively. Nonetheless information about consumers will be available to the 600,000 health workers administering batch downloads of the HI based on Medicare or Veterans Affairs data (3). Consequently, the number will be stored in several thousand local health service information systems, regardless of their security arrangements.

The draft Bill should mandate provision for consumer access to their own HI data from the date of system implementation.

The draft Bill should mandate robust local security arrangements BEFORE authorising the storage of an HI bridge to consumers' personal information by health services.

4. Although there may be no timelines scheduled to enable consumer access at present, several thousand publicly owned health services are expected to use and disclose the number as a unique reference number in their own health records and consumers will need to trust the security of arrangements protecting the used and disclosed information. However the data stored in the HI system may not be correct (3). Although publicly funded services will be required to use the HI from its implementation, NEHTA and DoHA spokespersons at the meeting last year suggested that in the fullness of time, consumer pressure means private practitioners will also use the HI.

   We are worried by the apparent fragmentation of the health sector that is likely to occur as a consequence of silos of private sector practitioners that will not use the HI, as has been the Canadian experience (4).

5. There will be no widespread pilot of the HI system before rollout. There is no governance, no evidence suggesting the system is reliable and safe, that there are no bugs and we have no way to assess whether abuse of the system is possible. Neither do we understand the designers' assumptions, which are inherent to system development. Consumers are advised about the benefits of the implementation throughout the "Concept of Operations" and the "Update on legislative proposals for healthcare identifiers" documents but not the risks (1, 2). No system is **ever** completely secure and therefore, neither can information stored on the system be secure, yet this crucial point is not made by the health authorities drafting self-referenced propaganda to support the HI system. The HI service has been presented to the public in an information vacuum of the proposed application or use of the service.

   The APF is concerned about relying on the utility of the HI system for patient privacy and health when authorities know so little about it in a "real-life" context.

6. Authorities are emphasising penalties associated with the misuse and disclosure of private patient information. However research shows the overwhelming majority of misuse is actually incidental and occurs as clinicians provide patient care in environments where resources are shared (6). Disclosure occurs as people go about their ordinary work tasks- that is, no special effort is required to overhear sensitive patient information.

   Health authorities must fund a review of the context of patient care, as recently occurred in the UK, so that "incidental" privacy breaches are minimised or even eliminated completely (5)**.**

7. Authorities may be able to track misuse of the HI system back to the end-user account name but not necessarily to the individual concerned. Research evidence suggests the end-user account names and PKI keys are already shared with clinically unqualified and underqualified users to advance patient care tasks (6). All consumers may ever know is the account name used to obtain or disclose patient information. Also, will end-user accounts and NASH accounts be issued to individuals or to organisational units? The evidence suggests that audit information may be insufficient for consumers to use for the purposes of a complaint with regard to the misuse or disclosure of their information.

   Access control systems to support the HI seem to be inadequate with regard to protecting the privacy of Australian consumers and patients.

8. The draft HI Bill allows data linkage between citizens' personal information and the HI. Yet several researchers, some of whom are Australian, have developed HI systems that do not require linkages to personal information. Thus, the draft HI Bill facilitates technological approaches that are already out of date.

   The draft Bill entrenches outmoded technology into the HI system.

9. The definitions contained in the draft Bill are open-ended and offer no guarantees to consumers at all. For example the definitions of an identified 'healthcare provider' and a 'service operator' are circular – they are whoever government authorities decide to assign a number (**page 3** and **page 5**). The use of national HIs for "management, funding ... and the conduct of health or medical research" is also both vague and open-ended (**page 12**). The definition of a 'health service' is the most chilling of these, because during the November meeting discussed above, an insurer was advised that although they may not access the HI at this stage, **the definition of a 'health service' is likely to change over time**. Will HIS information be available to insurers, banks and potential employers over a period of time?

   The draft Bill would be vastly improved if it permanently closed potentially privacy invasive loopholes contained in definitions.

10. Section 24 Regulations leaves a plethora of consumer concerns open-ended, including new data sources, governance arrangements, security mechanisms, standards, quality and safety.

The APF seeks detailed HI provisions in the legislation rather than being left to regulation on the grounds that, even though disallowable by Parliaments, the latter are rarely subject to the same level of scrutiny and debate.

11. The scope of the draft HI Bill is limited by the lack of systems to enrol some categories of Allied Health Care worker. Such enrolments may take several years to complete. A fragmented Australian HI landscape seems likely to emerge when one considers the enrolment shortcomings in the context of private health organisations, some of whom may decide not to not use an HI system, and public health organisations that will be legally required to use an HI from implementation.

    Additional fragmentation due to the enrolment of Allied Health Care Workers may unintentionally exacerbate shortcomings with regard to silos of patient information (See 3, above).

12. The draft Act briefly refers to interaction with the Privacy Act in Section 6 adding yet another layer of complexity to clinical work within the Australian health privacy legal framework. Evidently, the law of a State or Territory will not apply unless it can function concurrently with the draft Bill. However nothing in the draft Bill will affect or restrict any rights or remedy a person might have had if the Bill was not enacted. The minister may revoke parts of the HI in States and Territories so long as these are advertised in the Government Gazette. The health legal landscape will be as fragmented and confusing as it has ever been, possible even more so for clinicians actually working with an HI.

    Although this may be harmonised in the long term, the fragmented HI privacy legal framework outlined in the draft Bill will prove confusing for practices and clinicians, increasing the present range of threats to consumer privacy.

13. Finally, the "Building the foundation for an eHealth future …" document refers to ongoing consultations with stakeholders (1). No such consultation with most consumers or consumer groups we regularly liaise with has taken place. The overwhelming majority of consumers are excluded from NEHTA's definition of "stakeholder" too (6). Moreover, when the APF has been invited to the so-called consultations, we have been instructed to limit feedback to the issue of HIs without reference to an EHR since at this stage we know neither whether an EHR will be enacted at all nor the nature of its relationship to an HI. However government officials can and do refer to the HIs in the context of an EHR as a way of justifying the need for HIs (2, 3). Public meetings have been similarly controlled. Consultation audiences are told what will occur, not asked about the implementation. Questions times are limited, controlled and cease well before the flood of questions do. Thus, the audience to such consultations is given little opportunity for meaningful input – the so-called consultations are little more than briefings to explain how the system will function.

    APF HI policies and views are repeatedly ignored during meetings with senior health officials.

For all of the reasons herein, the APF believes the current exposure draft HI Bill is deeply flawed. It is both incomplete and inadequate in relation to privacy protection and meaningful input by health consumers. The lack of clarity around aspects of governance, slipping important issues into non existent regulations, lack of any details around NASH and lack of information about how the sector will actually use the HI service suggest to me the whole thing is under-planned and should be thought out more clearly. We are very concerned the shortcomings listed in this document will impede the development of an effective HI system for all Australians. The implication of the concerns listed above is to query whether the APF is wasting our time with this and other submissions to health care authorities.

Yours sincerely

Chair, Health Sub Committee
Australian Privacy Foundation

Dr Fernando is in Medicine, Nursing & Health Sciences
Monash University
Phone: 03 9905 8537 or 0408 131 535
Mail to: juanita.fernando@med.monash.edu.au

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

References

1. Australian Health Ministers Conference. November 2009. Building the foundation for an eHealth future … update on legislative proposals for healthcare identifiers. Commonwealth of Australia, ACT. p.12
2. NEHTA. Concept of operations. 2009. http://www.nehta.gov.au/connecting-australia/healthcare-identifiers
3. AIHW. Health and community services labour force 2006: no. 42. National health labour force. 6 March 2009. Retrieved 2 January, 2010, from http://www.aihw.gov.au/publications/index.cfm/title/10677
4. Shaw, N., Kilkarni, A., & Mador, R. Patients and health care providers' concerns about the privacy of Electronic Health Records. Presented at HIC 2009 Frontiers of Health Informatics. HISA. National Convention centre Canberra 19-21 August 2009
5. Robert, G., Greenhalgh, T., MacFarlane, F. & Peacock, R. Organisational factors influencing technology adoption and assimilation in the NHS: a systematic literature review: Report for the National Institute of Health and Research Service Delivery and Organisation programme. 2009. © Queen's Printer and Controller of HMSO 2009
6. Fernando, J. & Dawson, L. The health information system security threat lifecycle: An informatics theory. International Journal of Medical Informatics 78(12). 2009.
7. NEHTA. Stakeholder reference forum. http://www.nehta.gov.au/about-us/stakeholders © 2004-2009

APPENDIX A

Australian Privacy Foundation

Policy Position
eHealth Data and Health Identifiers

28 August 2009

http://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf

This document builds on the APF's submissions over the last two decades, and particularly during the last three years, in order to consolidate APF's policy position. It presents a concise statement of general Principles and specific Criteria to support the assessment of proposals for eHealth initiatives and eHealth regulatory measures.

The first page contains headlines only, and the subsequent pages provide further explanation.

General Principles

1 **Health Care Must Be Universally Accessible**

2 **The Health Care Sector is by its Nature Dispersed**

3 **Personal Health Care Data is Inherently Sensitive**

4 **The Primary Purpose of Personal Health Care Data is Personal Health Care**

5 **Other Purposes of Personal Health Care Data are Secondary, or Tertiary**

6 **Patients Must Be Recognised as the Key Stakeholder**

7 **Health Information Systems are Vital to Personal Health Care**

8 **Health Carers Make Limited and Focussed Use of Patient Data**

9 **Data Consolidation is Inherently Risky**

10 **Privacy Impact Assessment is Essential**

Specific Criteria

1 **The Health Care Sector Must Remain a Federation of Islands**

2 **Consolidated Health Records Must Be the Exception not the Norm**

3 **Identifiers Must Be at the Level of Individual Applications**

4 **Pseudo-Identifiers Must Be Widely-Used**

5 **Anonymity and Persistent Pseudonyms Must Be Actively Supported**

6 **All Accesses Must Be Subject to Controls**

7 **All Accesses of a Sensitive Nature Must Be Monitored**

8 **Personal Data Access Must Be Based Primarily on Personal Consent**

9 **Additional Authorised Accesses Must Be Subject to Pre- and Post-Controls**

10 **Emergency Access Must Be Subject to Post-Controls**

11 **Personal Data Quality and Security Must Be Assured**

12 **Personal Access and Correction Rights Must Be Clear, and Facilitated**

General Principles

1 **Health Care Must Be Universally Accessible**. Access to health care must not be conditional on access to health care data or on demonstration of the person's status (such as residency rights or level of insurance)

2 **The Health Care Sector is by its Nature Dispersed**. Health care is provided by thousands of organisations and individual professionals, each with a considerable degree of self-responsibility. The sector is far too large, and far too complex to be centrally planned. Instead it must be managed as a large, complex and highly de-coupled system of autonomous entities, each of which is subject to regulation by law, Standards and Codes

3 **Personal Health Care Data is Inherently Sensitive**. Many individuals have serious concerns about the handling of at least some categories of health care data about themselves. Their willingness to divulge important information is important to their health care, but is dependent on them having confidence about how that information will be managed

4 **The Primary Purpose of Personal Health Care Data is Personal Health Care**. The protection of the individual person is the primary function of personal health care data and systems that process it. The key users of that data are health care professionals

5 **Other Purposes of Personal Health Care Data are Secondary, or Tertiary**. Public health is important, but is a secondary purpose. Administration, insurance, accounting, research, etc. are neither primary nor secondary but tertiary uses. The tail of health and public health administration and research must not be permitted to wag the dog of personal health care

6 **Patients Must Be Recognised as the Key Stakeholder**. Government agencies and corporations must directly involve people, at least through representatives of and advocates for their interests, in the analysis, design, construction, integration, testing and implementation of health information systems

7 **Health Information Systems are Vital to Personal Health Care**. People want systems to deliver quality of service, but also to be trustworthy, transparent and respectful of their needs and values. In the absence of trust, the quality of data collection will be greatly reduced

8 **Health Carers Make Limited and Focussed Use of Patient Data**. Health care professionals do not need or want access to their patients' complete health records, but rather access to small quantities of relevant information of assured quality. This requires effective but controlled inter-operability among health care data systems, and effective but controlled communications among health care professionals. Calls for a general-purpose national health record are for the benefit of tertiary users (administration, insurance, accounting, research, etc.), not for the benefit of personal health care

9 **Data Consolidation is Inherently Risky**. Physically and even virtually centralised records create serious and unjustified risks. Services can be undermined by single points of failure; health care data isn't universally understandable but depends on context; consolidation produces a 'honey pot' that attracts break-ins and unauthorised secondary uses and creates the additional risk of identity theft; and diseconomies of scale and scope exceed economies

10 **Privacy Impact Assessment is Essential**. Proposals relating to personal health care data and health care information systems must be subject to PIA processes, including prior publication of information, consultation with affected people and their representatives and advocates, and publication of the outcomes of the study. Designs for systems and associated business processes must be based on the results of the PIA, and implementations must be rejected if they fail to embody the required features

Specific Criteria

1 **The Health Care Sector Must Remain a Federation of Islands**. The health care sector must be conceived as islands that inter-communicate, not as elements of a whole. Health care information systems must be conceived as independent services and supporting databases that inter-operate, not as part of a virtually centralised database managed by the State. Coordinating bodies must negotiate and facilitate inter-operability, not impose central schemes

2 **Consolidated Health Records Must Be the Exception not the Norm**. A small proportion of the population may benefit from linkage of data from multiple sources, primarily patients with chronic and/or complex conditions. Those patients must be the subject of consent-based, specific-purpose data consolidation. This activity must not apply to people generally

3 **Identifiers Must Be at the Level of Individual Applications**. Each of the large number of dispersed health care information systems must use its own identifier for people. A system-wide or national identifier might serve the needs of tertiary users of personal data, but does little for the primary purpose of personal care, and it creates unnecessary risks for individuals

4 **Pseudo-Identifiers Must Be Widely-Used**. Particularly when personal data moves between organisations, the maximum practicable use must be made of one-time-use and other forms of pseudo-identifiers, in order to keep people's identities separate from the data itself, and minimise the risk of personal health care data escaping and being abused

5 **Anonymity and Persistent Pseudonyms Must Be Actively Supported**. Anonymity is vital in particular circumstances such as ensuring that people are treated for sexually transmitted diseases. Persistent pseudonyms are vital in particular circumstances such as for protected witnesses, victims of domestic violence, and celebrities and notorieties who have reason to be concerned about such threats as stalking, kidnapping and extortion

6 **All Accesses Must Be Subject to Controls**. Access to personal data must be subject to controls commensurate with the circumstances, including the sensitivity of the data and the potential for access and abuse of access. This requires identification of the category of person and in many cases of the individual who accesses the data, and authentication of the category or individual identity. However, the barriers to access and the strength of authentication must balance the important value of personal privacy and effective and efficient access by health care professionals

7 **All Accesses of a Sensitive Nature Must Be Monitored**. Non-routine accesses and accesses to particularly sensitive data must be detected, recorded, and subject to analysis, reporting, sanctions and enforcement

8 **Personal Data Access Must Be Based Primarily on Personal Consent**. The primary basis for access to personal data is approval by the person concerned. Consent may be express or implied, and may be written, verbal or non-verbal, depending on the circumstances. All accesses based on consent must be detected, recorded and subject to analysis, reporting, investigation, sanctions and enforcement

9 **Additional Authorised Accesses Must Be Subject to Pre- and Post-Controls**. All accesses that are not based on personal consent must be the subject of explicit legal authority that has been subject to prior public justification. All such accesses must be detected, recorded and subject to analysis, reporting. investigation, sanctions and enforcement

10 **Emergency Access Must Be Subject to Post-Controls**. Health care professionals (but only health care professionals) must have the practical capacity to access data in apparent violation of the personal consent principle, but must only do so where they reasonably believe that it is necessary to prevent harm to some person. All such accesses must be detected, recorded, reported and subject to analysis, investigation, sanctions and enforcement

11 **Personal Data Quality and Security Must Be Assured**. Data must be of a quality appropriate to its uses, and retained only as long as it remains relevant. Personal data in storage, in transit, and in use, must be subject to security controls commensurate with its sensitivity, and with the circumstances

12 **Personal Access and Correction Rights Must Be Clear, and Facilitated**. Each person must have access to data about themselves, and access must be facilitated by any organisation that holds data that can be associated with them. Where appropriate, the access may be intermediated, in order to avoid misunderstandings and misinterpretation of the data. Where data is not of appropriate quality, the person must be able to achieve corrections to it