Submission

to

Senate Community Affairs Committee Enquiry

Healthcare Identifiers Bill 2010

and

Healthcare Identifiers Bill (Consequential Amendments) 2010

from

Peter West

Background to Submission

I was employed from November 2007 to September 2009 as a software developer at NeHTA, working initially with the Secure Messaging team, and later on the e-Health Collaboration Portal.

During this period, I had many opportunities to discuss with colleagues the topic of identifiers, particularly Individual Healthcare Identifiers (IHIs). Never did I see any documents that indicated that alternatives to a centralised identifier had been considered, not did any of my discussions give me any reason to believe this was the case.

Over the two years I worked for NeHTA, the IHI went from being an opt-in system, to an opt-out system, to a compulsory identifier, from which it would be impossible to withdraw. There was no comprehension that these fundamental changes were a betrayal of the undertakings that had previously been made to parties to consultations about issues surrounding identifiers.

In early September, 2009, I left, determined to demonstrate that identifiers that uniquely identify a patient need not be centralised, that a patient need not be restricted to a snuggle identifier, and that a functional Summary Electronic Health Record could be realised quickly, without the threat to privacy posed by the current Bill. A NeHTA colleague with similar convictions followed me a week later.

We developed a system known as *DIAD (StarDIAD); a set of Domain-name Identifier And Directory components to provide identifiers to professionals, organisations with any connexion to the health sector, and, most importantly, individuals. The iDIAD identifier for individuals includes an optional directory of critical clinical data, updated by a patient's GP, and available to other professionals and emergency services. Documents briefly describing the essential elements of the system are attached.

My colleague and I presented this material to NeHTA early in November, 2009. We heard nothing back until, on the 10th of December, 2009, the same day that the minister released the Exposure Draft of this Bill, a partner of Piper Alderman wrote to us on behalf of NeHTA, demanding that we surrender all of our intellectual property in *DIAD to NeHTA, and sign over all of the Internet Domains we had registered. An expensive exchange of letters and emails followed, in which we refuted every ground on which this demand was made. This process, which is on-going, had the effect of preventing our making representations to the notorious “Christmas consultations” on the Exposure Draft, which ended on the 7th of January 2010. We were not that only ones disadvantaged in responding to this pseudo-consultation process, as is evident from the submissions made.

Types of Identifier

The Bill mentions three types of identifier. These correspond to what were known in NeHTA as the Healthcare Provider Identifier – Organisation (HPI–O), the Healthcare Provider Identifier – Individuals (HPI–I) and the Individual Healthcare Identifier (IHI). These are three very different types of identifier. The uses to which each will be put, the entities to which each will be applied, and the privacy implications of each are utterly divergent.

As the names indicate, there is a closer affinity between the HPI–O and the HPI–I than between either and the IHI. However, even within the HPIs, there are major functional differences.

The National Product Catalogue and the HPI–O

While HPI–Os were clearly conceived as identifiers for organisations through which healthcare professionals operated, there is a wider range of organisations which could benefit from the

electronic integration which identifiers are supposed to facilitate. For example, the National Product Catalogue requires identifiers for organisations and organisational units. Has the possible integration of such organisational identifiers with the HPI –Os been considered?

The HPI–I and NRAS

From the Australia's Health Workforce Online website:

"The ***Health Practitioner Regulation (Administrative Arrangements) National Law Act 2008*** (Act A) commenced on Royal Assent on 25 November 2008, giving effect to the administrative arrangements for the National Registration and Accreditation Scheme for the Health Professions. The Act was passed in the Queensland Parliament."

There is an intimate relationship between the HPI–I and NRAS. HPI–Is will identify the members of the Health Workforce. The members of this workforce must be accredited, and this wil be the responsibility of NRAS. A tender has been let for the development of the registration system for NRAS.

So why has the legislation for HPI–Is not been written in the same context as the legislation for NRAS? Why is it in this particular Bill, along with unrelated identifiers, and why is the system for the assignment and querying of HPI–Is being bundled up with the systems for unrelated identifiers? Why has this system not been developed and tendered for in conjunction with the NRAS legislation and tendering?

Separate Identifiers – Separate Legislation

These three identifiers should logically have been presented in three separate Bills. The current Bill should be withdrawn, and new and separate Bills drafted. This time, there should genuine and open consultation on the nature of these identifiers.

At a minimum, the HPI–I Bill must be tightly integrated with the NRAS legislation.

The HPI–O must be rethought to encompass all organisations connected with the health sector, who identity must be established in communications across the sector.

Why the Omnibus?

Why has this legislation come in such an ill-considered form, as a grab-bag of unrelated identifier types? Why has the obvious mismatch not been noticed before the Bill came before Parliament? I believe it is symptomatic of the "closed-shop" mentality of NeHTA and DoHA to the development of e-health. The "consultations" on identifiers, with their short timeframes, especially the notorious "Christmas consultation," when the Exposure Draft of this Bill was released on the 10th of December, with submissions closing on the 7th of January, demonstrates a flagrant disregard for open processes by the Minister, the Department, and NeHTA.

The timeframe for this Committee enquiry is more of the same.

Issues considered by the Committee

The guidelines for submission offer the following suggestions for topics.

• privacy safeguards in the Bill

• operation of the Healthcare Identifier Service, including access to the Identifier

• relationship to national e-health agenda and electronic health records.

I shall discuss the Committee's outlined issues, starting with the last.

Relationship to national e-health agenda and electronic health records

Within NeHTA, the IHI was always discussed in association with the National Authentication Service for Health (NASH) which would provide guarantees of the valid use of identifiers by healthcare professional and organisations; i.e. that a claim by a person to be a certain healthcare professional was valid.

In an environment where professionals are personally known to one another, such a validation would be unnecessary. However, even when professionals are known to one another, their computer systems are not. In addition, where new, centralised bureaucratic agents become embedded in healthcare interactions, such external validation is demanded. If it is an aim of policy to reduce professional medical service to interchangeable commodity units, such processes are necessary. If it is an aim of policy to be able to monitor and ultimately control the (expensive) interactions between professionals and their patients, such processes are essential.

However, the NASH does not yet exist. There is no corresponding Bill setting up such a service, and in its absence, the verification of the use of the identifiers of healthcare organisations or professionals simply cannot be performed.

Note that there is, as yet, no proposal for similar validation of the identity of patients. For now, the validation is provided by the personal interaction between the patient, the clinical organisation and the clinician.

To be sure, in the presence of computer-to-computer transmission of patient data files, as opposed to transmission methods which involve multiple human inspections, demand methods of identity assurance beyond those of more leisurely times. But what type of identity assurance?

The other element that was always associated with the IHIs was the Shared (or Individual) Electronic Health Record (the SEHR or IEHR). NeHTA repeatedly tried to present a business case for the SEHR to COAG, and was repeatedly rebuffed. I was not privy to the contents of such a proposal, but figures generally talked about ranged up to almost $20 billon over 5 years. While I have no means of verifying this figure, the Committee members do.

If such a figure is within the ball-park, it gives an indication of the scale of activity that is required to initiate an SEHR in Australia. If the experience of other countries, notably the United Kingdom, is any indication, the final figure would be considerably more than the initial estimates.

In the meantime, the Government has begun to talk about drawing companies like Microsoft and Google into the mix. Such kite-flying appears to be a response by the Government to the projected cost of the SEHR. Both Microsoft and Google have consumer-controlled health-care systems in various stages of use in the United States. This speculation is relatively new, but it demonstrates that there has been no progress towards any concrete definitions of SEHRs.

This lack, and the absence of a NASH, regarded as essential for the practical application of identifiers, point to the confusion and lack of direction of E-Health policy in Australia, and raise questions about the haste with which the Healthcare Identifiers Bill is being pushed through the Parliament.

While there is an existing requirement, associated with NRAS, for identifiers for healthcare professionals, and that requirement is relatively uncontroversial, the same cannot be said for the IHI. Furthermore, given the complete confusion about the eventual design of an SEHR or of a summary record for emergency situations and “occasional” use, how can the system be designed with any confidence? In particular, why is the identifier proposed in the current Bill being pushed

through Parliament with indecent haste?

Operation of the Healthcare Identifier Service

My main concern here is the need for *any* such service in respect of IHIs.

What is the clinical requirement for this service? The individual identifier will, apparently, be accessible from the patient's Medicare card. Discovering the number from the service will require various identifying information, such as name, address and age. In a clinical setting, when the patient is with the clinician, why is the Medicare card not enough? In the majority of cases, the patient will have his or her Medicare card, or the clinician will already have that information. That, surely, is a more effective way fo determining the identifier?

In a situation in which the patient is unconscious or incoherent and alone, the clinician will be relying on information carried by the patient. This would in most cases include a Medicare card. When it does not, is such demographic data as can be determined going to be reliable in any case. The only way to obtain such information reliably is to be able to question a coherent patient, or a coherent companion of the patient. Why would the information not have access to either a Medicare card, or a card of some kind from which the actual identifier is obtainable?

There may indeed be clinical “corner cases” where demographic data is available in the absence of direct data. Do these cases justify a query system to which 600,000 people will have legitimate access? No.

An observer will naturally draw the conclusion that the primary purpose of the enquiry system is to allow those who have access to the demographic data, in the absence of the patient, to determine the identifier. What's going on?

It is this reality that necessitates the controversial pseudonyms, which have the effect of alerting consumers to the openness of the system to abuse. The announcement of these pseudonyms was greeted with outrage by large numbers of commentators when it became public knowledge recently.

Privacy safeguards in the Bill

Privacy concerns centre on the fact that the individual identifiers are only being brought into existence to provide a key to patient data. That key will be available not to the patient's known and trusted GP, and the specialists to whom the patient has been referred, but to 600,000 healthcare workers. What will that key unlock?

We don't know. But, in the absence of this knowledge, we are assured that the confidential medical data will be safe. No-one can make such assurances.

The identifier is being pushed through before any decisions about medical information have been made. Further, it is being pushed through as a compulsory identifier.

The retreat of privacy

Moira Patterson, then Associate Professor, Faculty of Law, Monash University, in an article entitled *Shared electronic health record systems: the significance of the privacy dimension* , in Volume 16, Number 7 of the Australian Health Law Bulletin of April 2008, wrote of her consultations with NeHTA in 2007 on this issue. At one point she wrote, “The most basic, and arguably the most fundamental control mechanism, is to ensure that participation in an SEHR is voluntary (and that people may choose to cease participation if they do decide to register)... It would seem, from its Preliminary Privacy Blueprint, that NEHTA reamins committed to an opt-in model (as well as an option to opt out once in). This is very important from a privacy perspective as it ensures that

participation results from an act of informed volition..."

So much for the informed volition of the Australian electorate. In the course of two years, the opt-in model has collapsed, not to an opt-out model, but to legislated compulsion. It would be yet another act of cynicism to claim that the identifier is not the SEHR, and that, therefore, NeHTA had not betrayed it's earlier commitments.

Legislative creep

Moira Patterson, then Associate Professor, Faculty of Law, Monash University, in an article entitled *Shared electronic health record systems: the significance of the privacy dimension* , in Volume 16, Number 7 of the Australian Health Law Bulletin of April 2008, wrote about the dangers of *function creep*.

"Once the system is in place and there is an increased awareness of the potential value of the information stored within it, there will be an inevitable pressure to make that information available for new uses..."

When the proposals of this Bill regarding individual identifiers are examined in the light of the absence of any concrete proposals from NeHTA of DoHA for an SEHR, their reality is crystallised by the above description of *function creep*. The same driving force is at play, and the legislation that for decades has protected the uses of the existing Medicare numbers is being overturned on the promise of the potential value of that information. With this precedent set, the method of further eroding the privacy protections of ordinary Australians has been established. Offer a wonderful set of benefits to be realised in some indefinite future, by some undefined means. Using this slight of hand, push through Parliament the open-ended changes that are essential if these future benefits are to be achieved.

The retreat of privacy

Moira Patterson, also wrote of her consultations with NeHTA in 2007 on this issue. At one point she wrote, "The most basic, and arguably the most fundamental control mechanism, is to ensure that participation in an SEHR is voluntary (and that people may choose to cease participation if they do decide to register)... It would seem, from its Preliminary Privacy Blueprint, that NEHTA reamins committed to an opt-in model (as well as an option to opt out once in). This is very important from a privacy perspective as it ensures that participation results from an act of informed volition..."

So much for the informed volition of the Australian electorate. In the course of two years, the opt-in model has collapsed, not to an opt-out model, but to legislated compulsion. It would be yet another act of cynicism to claim that the identifier is not the SEHR, and that, therefore, NeHTA had not betrayed it's earlier commitments.

Excessive authorisations

The Bill authorises (clause 24.1.a.ii) disclosure of individual identifiers for " the management … monitoring or evaluation of healthcare." This is far too large a grab-bag of authorisations.

The Bill authorises (clause 24.1.a.iv) disclosure of individual identifiers for " the conduct of research that has been approved by a Human Research Ethics Committee." I cannot see any justification for this clause. Only de-identified, and unidentifiable, data should be released, with the consent of the subject, for research. In 2005, there were over 220 such committees in Australia.

An alternative

The Australian Privacy Foundation wrote an excellent paper in an earlier submission on the issues

raised by healthcare identifiers. http://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf

The attached discussion of the privacy provisions of the *DIAD system describes the ways in which *DIAD meet the privacy criteria set out in that document. As such, it demonstrates that claims of the necessity of this identifier and its mode of operation are unfounded.

Peter West

Appendices

The following documents are attached.

Introducing *DIAD

Privacy and the *DIAD (StarDIAD) System

A modest proposal for e-health identifiers based on DNS

Introducing

✱DIAD

✱DIAD or StarDIAD (Domain-name Identifier and Directory) is an innovative approach to electronic identifiers using the Domain Name System (DNS) to produce identifiers that are globally unique but locally generated, efficient but personalised, a name not a number. (✱DIAD patent application has been lodged).

FUNCTIONAL DESCRIPTION OF ✱DIAD

✱DIAD is a method of providing electronic identifiers for large target populations, be they persons, organisations, places or objects in any combination.

The population to be named has the following characteristics:

- The population can readily be arranged into a hierarchy of entities. In one aspect, each entity falls into one of two categories; it is either a *simple entity* or a *naming authority entity*. Naming authority entities will hereinafter be referred to as *naming authorities*. Any nameable entity can be a simple entity, but in general only organisations will be naming authorities.
- Each entity except one, the *root naming authority*, is assigned its identifier by a responsible naming authority. Each naming authority also has an identifier. There is no difference in kind between the identifiers assigned to naming authorities and to simple entities.
- Each naming authority may issue identifiers to simple entities, and it may issue identifiers to other naming authorities. There may, consequently, be a multi-level hierarchy of naming authorities and simple entities in the form of a tree, with branches emanating from each naming authority, and with the end points of all branches being simple entities. These end points are known as the leaf nodes of the tree. The identifier of the naming authority that issues any particular identifier is known as the *parent* of the particular identifier. Correspondingly, the identifiers which are issued by a naming authority are known as the *children* of the authority's identifier. Note that, strictly speaking, the terms *parent* and *children* refer in this discussion to *identifiers*, not *entities* as such. However, the entities may loosely be referred to as parents and children, while keeping the strict meaning in mind.
- Only one naming authority is responsible for any identifier. The root naming authority issues an identifier to itself. Note that while a naming authority is responsible for all of the identifiers it issues, it is not responsible for identifiers issued by any naming authorities it has identified. Such children are in turn responsible for identifiers they issue.

As a consequence of this structure, each entity can be uniquely named by combining the identifier of the issuing naming authority with a name component which is unique amongst the children of the issuing authority's identifier. That is, the problem of unique naming is, by this naming structure, reduced to the problem of uniquely naming only the direct children of each naming authority.

Naming, and associated responsibility, is thereby localised to each naming authority.

While the naming responsibility is localised, in order to be functional as a population-wide identifier, the identifier must be able to be checked by anyone with an interest in the population.

✱DIAD addresses these concerns by a novel application of an existing technology – the Domain Name System (DNS). The DNS is a distributed database that associates small sets of data with a key. The key is a hierarchically-organised name which is readily comprehensible and communicable by both human beings and computers. DNS names are ubiquitous on the Internet and on the World Wide

Web. They form part of all modern email addresses, and part of every textual Universal Resource Locator (URL) used on the Web. Without DNS, the Web could not exist, and email could not function. DNS is consulted across the world many millions of times every day.

The key to the success of DNS is its hierarchical and distributed nature. There is no central repository of DNS names. Nor could there be. No centralised system could keep track of the constantly evolving space of DNS names. Technical and commercial experience of DNS systems is correspondingly widely distributed.

DNS was designed for a specific purpose: to associate human-comprehensible and human-communicable names with the numerical Internet addresses that underlie all Internet communication. These associations are described by *A* (address) and *AAAA* (IPv6 address) records within the DNS database. Many other types of records have been defined, and continue to be defined for DNS. To discover the Internet address associated with a given domain name, the DNS database is queried using the name as a key, and, if the name is present in the database, the address is returned.

The ***novelty*** of ✱DIAD is that the database for an entire sub-tree, or *zone*, of the DNS name space associates no Internet addresses with its domain names. A query using the domain name as a key will return a possibly empty set of *directory* data, not including A or AAAA records. The most important information returned from the query of a name within the zone is the fact of its existence or non-existence. The ***domain-names*** are just names; ***identifiers*** associated with human and corporate agents or other nameable entities. In a name of the form *A.B.C*, the structure of the identifier implicitly asserts that the entity named *A.B.C* has been *named by* the entity *B.C*. This implication provides a foundation for the hierarchical assertion of identity, because only the controller of the domain *B.C* can issue subdomains such as *A.B.C*.

The ***directory*** associated with each name is optional. If used, it is defined primarily in *TXT* (text) and *NAPTR* (naming authority pointer) resource records in the DNS database. Other resource records, for example *SRV* (server) and *LOC* (location) records may also be used. All information in the directory is public. However, such information may be represented directly and publicly, as in the form of TXT records, or may be represented indirectly, as in the form of NAPTR records, which re-direct enquiries to systems entirely external to DNS, where appropriate levels of access security may be enforced. That is, whilst the re-direction details are public, the information available from the re-directed query may be public or private.

The hierarchy of names would be based on functional, legal and practical categories determined by the nature of the application domain. Individual entities (be they persons, organisations, places, objects or any other nameable entity) would obtain or be assigned identifiers at their point or points of contact with the application domain. The characteristics of individual names would, again, be determined by the requirements of individual components of the application domain. For example, in the e-health system, individual patients could have “opaque” identifiers congruent with their need for privacy. On the other hand, registered professionals may be required to use an identifier which could be readily confirmed as belonging to a particular person.

DNS offers security at a number of levels. All of the names and associated information for a zone is regularly transferred between the master and slave nameservers of each zone. It is common practice to validate requests for this transfer by signing such requests, and to validate the transferred zone data by signing the return message. The signing is done with a key shared by the master and slaves. This process ensures that the complete zone data cannot be readily obtained by parties other than zone administrators. As a result, whilst the zone can be queried for individual names, the complete zone contents could only be discovered by exhaustive queries for all possible names within the zone.

In standard DNS, guaranteeing the validity of all of the data returned in response to queries is more difficult. It can be achieved by applying DNSSEC.bis (DNSSEC hereafter) security to the zones. Whether DNSSEC is used would depend on the security requirements of each application domain. However, in the case of the e-health application domain, it would be essential. When used, DNSSEC

would have to be applied to *all* zones within the application domain sub-tree.

Examples

N.B. All of the following examples are notional. The particulars of domain names, and the syntax and semantics of directory information are beyond the scope of the ❋DIAD. They would be determined as part of the specification of the application domain.

Example: GP Clinic and Patients

Identifiers are not restricted to persons; organisations may also possess them. For example, a medical general practice within the Sunshine Coast Division of General Practice, may have the identifier:

dh-clinic.scdgp.gpq.ehealth.id.au

A patient called James M. Brown, attending a general practice clinic might have the identifier:

james-brown002.dh-clinic.scdgp.gpq.ehealth.id.au

Another patient of the same clinic might choose the the identifier:

thegecko.dh-clinic.scdgp.gpq.ehealth.id.au

In the first case, the patient is not concerned that a casual observer of the identifier would deduce that a person called James Brown, one of at least two living in the area served by the clinic, was the one referred to by this identifier.

In the second case, the patient does not want such conclusions to be drawn, and chooses a *handle*, i.e. pseudonym, as the individual component of the identifier. Such pseudonyms are now familiar from social networking sites on the Web. Note that in both cases, the usual medical records will be maintained, with the addition of this identifier. At the clinic, the patients will be known to the staff as usual. However, no casual observer would be able to make that association.

The identifying entity for both identifiers is *dh-clinic.scdgp.gpq.ehealth.id.au*.

Example: Professional Study and Registration

Professional health care workers will generally have different levels of authorisation at different stages of their careers. For example, student, intern, registrar, specialist. If an identifier were to be associated with each stage, the identifying entity would be different in each case.

Assume health-care professionals are registered by a national body, known as National Registration and Accreditation Scheme (NRAS), and that accrediting educational institutions and training hospitals are affiliated with the NRAS.

If a student named John Stephen Smith were to enrol in medicine at Queensland University, for example, he might be assigned an identifier of the form:

smith-john-s-19731106-01.uq.nras.ehealth.id.au

On graduation, John Smith obtains an internship at Princess Alexandra Hospital, a recognised tertiary teaching hospital. He might be assigned a new identifier of the form:

smith-john-s-19731106-01.pah.nras.ehealth.id.au

Once his internship has been successfully completed, John Smith is eligible for registration with NRAS, when he might receive the identifier:

smith-js-19731106-01.mbbs.nras.ehealth.id.au

The person is identified as *smith-js-19731106-01*, whose identifier was provided by the entity *mbbs.nras* within the Australian health-care application domain. In the case of professional identifiers,

it would probably be considered advantageous to have an identifier which is readily associated with the person identified, as in this example.

Example: Directory Linking Multiple Identifiers

The professional registration example shows that multiple identifiers may both be required, and required to be linked. It would be necessary to be able to trace the path to accreditation of professionals within the system.

Linking could be achieved in a number of ways through DNS records. One possible method is to use NAPTR records to establish a double-linked list. The Application Unique String for this application would the identifier for which links were required. The First Well Known Rule would use the identifier unchanged to request NAPTR records. The expected service in the NAPTR records would be *alias* with either *next* or *prev* as secondary service protocols. The possible values of the service field would then be *alias+next* or *alias+prev*. An application program can then derive the complete set of links starting from any point in the chain.

If there were no aliases, no appropriate NAPTR records would be returned. If there were one alias only, both the *next* and *prev* entries would transform to the same alias. In other cases, the chain could be followed in either direction.

The same process allows the optional linking of multiple identifiers that individual patients may choose to have.

Example: Location capability for service or care facilities location finding

Where a specific location is required, for example the exact location of a hospital, DNS provides a Location (LOC) Record function (known as LOC RR) that might be assigned or attributed to the e-identifier of the service. The LOC RR permits the addition of latitude, longitude and altitude to e-identifier – should this be required.

Example: Directory Publicly Available Health Information for Patient

If a patient chose to have some demographic or medical information associated with his or her identifier, the TXT records associated with the identifier might contain the following strings:

birthyear=1960
eyes=blue
height=170cm
blood=Oneg
allergies=penicillin,bee-sting
medications=Warfarin:2mg

Such information is *public*; it would be available to anyone with Internet access.

Example: Directory Private Health Information for Patient

If a patient chose to participate in a service supplying certain information from his or her medical records as held by the clinic, in an Internet-accessible service whose interface were well-known, a combination the patient-specific label (the first label of the domain-name) and the clinic identifier (the remainder of the domain-name) could be used in conjunction with NAPTR and SRV records associated with the clinic domain-name to access the service with a query about the patient. Note that the NAPTR and SRV records are publicly readable, but the service to which they point can be public or private. If private, this access would be subject to the authentication and access policies governing such sensitive data.

Example: Directory Information for Professionals

For a professional identifier, some publicly accessible information may be associated with the identifier by means of TXT records. It might, for example, be considered that a professional registration number should be published with the identifier. In addition, because the professional may also use his or her professional identifier as a patient identifier, the same basic personal medical facts may also be recorded.

Professional registration bodies may define interfaces to web services with confidential information concerning the professional's registration and history. Such services might be accessed through NAPTR and SRV records on the registration body's identifier, using that identifier and the professional's identifier to locate and query the service. As with patient data, this access would be subject to the authentication and access policies governing such sensitive data.

✱DIAD – a name, not a number.

Privacy and the *DIAD (StarDIAD) System

*DIAD provides an optional universal identifier without any requirement for personal identifying or demographic information. As such it offers a unique combination of universality and privacy.

The Australian Privacy Foundation issued a policy position paper on eHealth Data and Health Identifiers on the 28th of August 2009. It is available at

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

It is structured around the following principles and criteria, which *DIAD addresses as described below. To understand the privacy implications of the *DIAD system, one must appreciate that the set of identifiers issued by any one issuer is, by default, known only to that issuer. Active measures must be taken to overcome this restriction. A consequence is that a patient's identifier is known to the patient, and to his or her clinical advisors, and to others at the patient's or clinicians' option. This is a characteristic of the system design, preceding any policies that may be put in place to further restrict access.

Identifiers may have a small publicly accessible set of text notes associated with them. These will be accessible to anyone who knows the identifier. These notes are the basis of support for emergency medical information. Identifiers may also have a small set of pointers to other services on other systems. The policies and procedures governing such external services are beyond the control and scope of the *DIAD system.

Both of these ancillary components are optional.

General Principles

1 **Health Care Must Be Universally Accessible**

iDIAD identifiers (for individual patients) are universal and optional. The relationship between a patient and his or her clinicians is unaffected by the presence or absence of an identifier.

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

iDIAD identifiers are issued and controlled at the point of contact with the health sector.

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

iDIAD identifiers may optionally have de-identified emergency care health information attached to them for immediate access. iDIAD identifiers may optionally have pointers to external services attached to them. The access policies and procedures governing such external services are outside the scope of the *DIAD system.

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

iDIADs are issued at the point of care, by the clinical carer. The association between the identifier and the patient is known only by the issuer, and is electronically recorded only be the issuer's computer system.

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

Because the association between identifier and identified is known only at the point of issue, revealing that association can only be done by the issuer, who is generally the

primary clinical carer, with the consent of the patient. There is, however, no structural impediment to the issuers' revealing that association. There is no direct electronic connection between the identifier and any sources of the patient's information.

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

iDIADS are issued by the primary care clinician, not by the patient. The patient does not, therefore, have direct control over the identifier. However, the identifier is issued an maintained at the closest point of patient contact to the health system.

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

Health information systems, as such, are outside the scope of the *DIAD system. The system provides a globally unique identifier to act as the glue between various existing and projected health information systems.

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

Limited and focussed patient data is optionally available directly through the iDIAD identifier. This is typically critical emergency care information, like allergies and current medications, and chronic conditions. This de-identified information is associated with the identifier, but the identity of the patient is available only from the patient or the patient's clinician. Other health information systems, which may provide other views of the patient's data, may be pointed to through the identifier, but the policies and procedures governing access to that data are not in scope.

9 **Data Consolidation is Inherently Risky**

Aside from the limited optional data mentioned in point 8, no data consolidation is required by iDIADs. Data remains in the systems on which it was collected, at the patient's point of contact.

10 **Privacy Impact Assessment is Essential**

The creators of the *DIAD system welcome external privacy impact assessment and auditing.

Specific Criteria

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

This is a fundamental design principle of the *DIAD system.

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

Only emergency medical data is associated with the iDIAD, and it is de-identified.

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

*DIAD identifiers are intended to complement existing application identifiers. The association between identifier and patient, in particular, remains with the local computer (or manual) system of the issuer. iDIADs provide an opaque means of transferring a reference to a particular individual between one clinician and another, where a new local association between identifier and identity will be established.

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

iDIADs may reflect the patient's name, or they may be any pseudonym or “handle” that the patient chooses. This reflects the common practice of social networking web sites. While each identifier uniquely names one individual, an individual may have more than one

identifier. For example, a patient may seek a second identifier for mental health consultations.

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

A patient may choose a name that closely reflects his or her actual identity, an opaque "handle", or a name that is misleading. All iDIAD identifiers are persistent.

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

Access to the public information attached to an identifier, whether actual clinical data or pointers to external services, are necessarily public. The link between the identifier and the denoted individual's actual identity is known to the patient, the patient's clinical advisers and anyone to who those people choose to make it known. Further, even access to the public data associated with an identifier requires that the identifier be known. The set of iDIADs issued by a clinic, by default, is known only on the systems controlling the DNS database for that clinic. It is not feasible to discover by "brute force" methods, the set of names issued by an issuer.

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

Unless a patient chooses to place sensitive data in the public component of his or her identifier, there are no accesses of a sensitive nature that the iDIAD itself makes available.

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

The personal data that is made publicly available must be attached by the patient's primary health care provider. From a technical point of view, that data can be attached without the patient's consent. However, the relationship between patient and primary health care provider is already constrained by professional and legal considerations.

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

There are no *additional* accesses beyond those of the party assigning the identifier; in the case of iDIADs, this will generally be the patient's GP. Access to related systems is beyond the control of the *DIAD system.

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

Access to the text notes on a iDIAD is available to anyone who knows the identifier and who has Internet access through a relatively modern system. Among this group would be emergency services, if the patient chooses. The identifier would be established by emergency workers in one of the same ways that the actual identity of an injured person is established; by checking the person's belongings. Any post-controls in these circumstances would be minimal.

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

The *DIAD system assures data quality by leaving it in the hands of the clinician who directly deals with the patient. Any enquiries concerning data associated with a iDIAD must be directed in the first instance to the issuing authority for the identifier; usually the patient's general practice clinic.

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

Access to iDIAD contents, as noted in point 10, is available to anyone who knows the identifier, and who has Internet access through a relatively modern system. This data is added in consultation with the patient's health care provider, where the types of data, its accuracy, and whether it goes on the public record, are discussed.

A modest proposal for e-health identifiers based on DNS.

My colleague Phil Johnson and I have provisional patents filed for an identifier system known as ***DIAD** (StarDIAD). Here's an example of the way that *part* of the *DIAD naming tree might look.to implement patient identifiers (iDIADs).

Root domain-name for e-health **oz-ehealth.org.**

This domain-name is controlled by the Australian e-health naming authority. The authority only authorises the names of top-level e-health domains, which are delegated from the DNS server of this domain.

This domain-name is to some extent arbitrary. However, the optimal domain root exists under a DNSSEC signed domain. In practice, that is .ORG. The public key for the root servers is to distributed by 1st July 2010. .ORG is now signed, and owners of .ORG domains can now participate in operational testing of the procedures.

General Practice Queensland **gpq.**oz-ehealth.org.

A top level naming authority, authorised by the root level naming authority. This authority only authorises the names of practices within its ambit. Those names will occur within the domain's DNS server.

Sunshine Coast Division of General Practice **scdgp.**gpq.oz-ehealth.org.

authorised by General Practice Queensland. This naming authority only authorises the names of practices within the division. Those names occur within the domain's DNS server.

The fictional dh-clinic **dh-clinic.**scdgp.oz-ehealth.org.

The clinic is on the Sunshine Coast. This naming authority only authorises patients of the clinic. Those names occur within the domain's DNS server.

A patient **thegecko.**dh-clinic.scdgp.oz-ehealth.org.

The patient accepts an optional identifier from the clinic. This is a terminal in the tree, and is not a naming authority. That is, there is no DNS server for this domain. Note the use of a *handle*, as is common on social networking sites, where people have learned to protect their identities.

Who is *thegecko.dh-clinic.scdgp.oz-ehealth.org*? The patient knows, obviously. His consulting doctor knows, and the association of actual identity with the identifier is maintained in the internal records of the clinic. Apart from them, only people to whom they reveal the association will know who *thegecko* is. *Thegecko*'s specialists will be informed, for example.

It's a simple enough structure, but it has some notable differences from a normal DNS structure. For a start, all of these names are just that - *names*. None of them denote any device that is connected to the Internet.

None of them have an associated IP address.

What do they have? Naming authorities will have NS records with the names of their name servers. Others have, at the least, a TXT record with an empty string.

Opaque Identifiers

At each level then, there is a set of names which is available, by default, only to the controlling name servers. Discovering the set of names without the co-operation of the naming authority is akin to cracking passwords by brute force methods over the Net.

Each name uniquely denotes an individual entity, if the naming authority does its job correctly. There is no restriction on the number of names that an entity may possess. Each naming authority creates names unique to the authority, which guarantees global uniqueness for all names.

Resolving Identities

The association between name and identity is maintained by the naming authority. The identifier can be passed around safely, and resolution of the identity requires some interaction with the naming authority, for example, dh-clinic.

Another way of resolving identity is to put a sticky label with the identifier on a driver's licence or Medicare card or credit card. The presence of this sticker indicates that the person referred to on the card is also the owner of the identifier. No electronic connection here. But if an unconscious person is attended by para-medics, that association will be available.

Knowledge of the identifier set is restricted. Knowledge of the identity associated with the identifier is restricted. Yet information associated with the identifier is public.

Payloads

Identifiers, by default, have no payload. They are simply name. However, they may optionally carry some information.

Let's say we associate a TXT record of the following form with the identifier.

```
TXT "allergies=penicillin,latex medication=warfarin:2mg"
```

Now anyone with an internet connection can issue a command like

```
$ dig thegecko.dh-clinic.scdgp.oz-ehealth.org txt
```

to read the content of that TXT record. Anyone. Anywhere.

This is not the patient's medical record. That is still held securely by the clinic. This is an emergency summary, which can only be associated with the patient when the patient's identifier is known.

The identifier of the issuing clinic is part of the patient identifier, giving access to additional information about the patient.

The identifiers are also a gateway to external systems. NAPTR records provide a means of

constructing a variety of strings from a given input. The input might be, for example, be the patient identifier. An enquiry against the issuing clinic's identifier returns a series of recipes for manipulating the patient identifier in order to determine more information about the patient. At the simplest level, that might be the telephone numbers of the clinic and treating doctor. At the other extreme, a web service might be defined by which qualifier enquirers could determine demographic and contact details about the patient, or extract a summary medical history.

Note that these are externally defined and managed systems. All the identifier can provide is an address to attempt to access them.