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.