Healthcare Identifiers Bill 2010
Healthcare Identifiers (Consequential Amendments) Bill 2010

Comments for the Senate Community Affairs Committee

4th March 2010

We wish to offer comments in relation to Division 2, Subdivision B –

Disclosure of healthcare identifier by service operator

1. We assume that individual and batch disclosures by the Service Operator and between healthcare providers always occurs in a full PKI authentication environment.
2. This ensures that electronic transmissions (Health identifiers, for the individual called IHIs; and associated data) are secure, cannot be altered, and cannot be repudiated.
3. Use of digital certificates (creating a digital identity) is therefore deemed mandatory within the Service Operator and Healthcare Provider environment.
4. Tight regulations for these processes will be agreed with Ministerial Council
5. We note that the Office of the Federal Privacy Commissioner is to provide independent oversight of the Healthcare Identifiers Service, and to consequently have over-ride rights over State privacy regulations where they are deemed inadequate.
6. Data Security standards have not been detailed in the requirements of this Bill. These should be addressed with some urgency.
7. We note the Concerns raised by the Privacy Commissioner in their January 2010 submission to the Exposure Draft, over compliance with data security obligations, and the obvious need for privacy safeguards.
8. A requirement for individuals to access their information, and to access “audit trails” of their IHI, is noted by the Privacy Commissioner on page 6 of their January response to the Exposure Draft.
9. This again prompts for a requirement to have appropriate data security controls.
10. We argue that the standards appropriate for data flows between the Healthcare Service Operator and Healthcare providers seeking or exchanging IHIs be the same as for information flows from an individual seeking details on use of their IHI. This requires an exchange of digital identities, with accompanying encryption standards
11. The argument can be taken further by considering the issues with referrals for an individual between Healthcare Providers, and for despatching an ePrescription for subsequent collection by the individual.
12. This therefore implies the allocation of a digital identity (a virtual certificate), in a PKI environment, to individuals before they are able to communicate with either their Healthcare Provider or the Healthcare Service Operator.
13. We urge the Senate to move to regulate to satisfy these wider

implications for privacy safeguards.

14. A sound knowledge base on PKI mechanisms, managing digital identities and their requirements exists within NeHTA, (and via it's preceding forms within Medicare Australia and before that within the then Health Insurance Commission) . This knowledge base now covers ten years.
15. It is proposed that for a HealthCare Provider to gain an individual's consent (ref Privacy Commissioner response to the Exposure Draft, Cl 19, p5) for utilising the IHI, this consent initiates a process for the issuing of a digital identity to the individual.
16. This proposal for consideration by the Senate therefore involves the following :
    a) a Voluntary uptake of an IHI by an individual
    b) Triggering a system request to the Healthcare Service Operator, for a replacement Medicare Card.
    c) This replacement card to have an embedded microprocessor on the card, of sufficient integrity to be PKI enabled.
    d) This should then be processed transparently along with the current daily practice for Medicare card issue.

G&D are happy to discuss in detail any elements of these brief points.