Can you respond to the statement by Dr Vincent McCauley from the Medical Software Industry Association to the Committee on 9 March 2010 that NEHTA has "chosen to ignore the international standards for the implementation of healthcare identifier service" and has "basically made up" standards?

The statement by Dr Vincent McCauley does not reflect NEHTA's approach to standards.

NEHTA has identified a number of International and Australian Standards that meet policy and stakeholder requirements for the design, development and implementation of the HI Service. We have adopted a range of standards (**Attachment A**) in close consultation with key stakeholders, software vendors, and standards organisations such as Standards Australia. Some of these standards relate specifically to the implementation of the HI Service.

When determining a standards solution for the HI Service, NEHTA considers International Standards first and Australian Standards second to determine which standard meets the business or technical requirements. We also consider the maturity and acceptance of the standard, and the standard's appropriateness in the Australian context.

NEHTA is aware of the MSIA's view that the Identification Cross Reference Service ("IXS specification") should be used for the implementation of the HI Service. However, NEHTA has concerns about the suitability of this specification for use in this context. For example, the specification only recently moved out of draft form so is still fairly immature. It is also specific to the US; stating "This … specification primarily reflects the contributions of US-based submitters and supporters" and "These service interfaces are intended to be used within a healthcare setting in which security of data exchanges is both important and regulated by laws such as Health Insurance Portability and Accountability Act (HIPAA) in the United States". As Australia does not currently have comparable laws to HIPAA, in our view there would be a regulatory gap if this standard were to be implemented without accompanying legislation. In addition, the use cases in the specification allude to the necessity to browse patient information. However, the HI Service does not allow for a healthcare provider to browse patient information which is an important privacy protection raised by our stakeholders, so this feature causes us some concern.

While this specification does not appear to be suitable for the HI Service at this point in time, NEHTA has certainly not ruled out using parts of it in the future or in another e-health context if appropriate. Indeed, we used the draft of the HL7 Services specification for the Entity Identification Service (the forerunner of the IXS specification) as an input into the design of the HI Service. We did this with the view that should the specification become an International Standard in the future, it could be adopted if demanded by Australian industry.

We will continue to work with our stakeholders to determine what role this standard could play in e-health systems.

Attachment A – Standards adopted for use with the HI Service

Standards Description	Area of Standards Application in the HI Service
AGIMO, Gatekeeper PKI Framework, February 2009 (replaces 2008 version previously endorsed**)**	HI Service Authentication
ASCI 33:2007, Australian Government Information and Communications Technology Security Manual	HI Security
AS/NZS 4360:2004, Australian Standards – Risk Management	HI Security
AS 4846:2006, Australian Standards – Healthcare Provider Identification	HI Design Reference
AS 5017:2006, Australian Standards – Healthcare Client Identification	HI Design Reference
AS 8015:2005, Australian Standard for Corporate Governance of Information and Communication Technology (ICT)	HI Design Reference
AS/NZS ISO/IEC 27001:2006, Information technology - Security techniques - Information security management systems - Requirements.	HI Security
AS ISO 17090.2:2003, Australian Standard, Health Informatics - Public Key Infrastructure - Certificate Profile, April 16 2003	HI Service Authentication
AS 3523.2:2008, Identification Cards – Identification of Issuers - Part 1: Numbering system	HI Numbering Specification
AS 3523.2:2008, Identification Cards Identification of Issuers - Part 2: Application and Registration Procedures	HI Numbering Specification
ISO/IEC 7812-1:2007, Identification Cards – Identification of Issuers - Part 1: Numbering system	HI Numbering Specification
ISO/IEC 7812-2:2007, Identification Cards – Identification of Issuers - Part 2: Application and Registration Procedures	HI Numbering Specification
ISO DIS 21091, Health informatics - Directory services for security, communications and identification of professionals and patients	HI Design Reference
ISO/TS 8000-110:2009, Data quality - Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, and conformance to data specification	HI Metadata Directory
ISO/TS 25237:2008, Health informatics - Pseudonymization	HI Design Reference
ISO 20302:2009 Health Informatics – Health cards – Numbering	HI Numbering

system and registration procedure for issuer identifiers	Specification
ISO 20302:2006(E), Health informatics - Health cards - Numbering system and registration procedure for issuer identifiers	HI Numbering Specification
ISO/TS 22220:2009 Healthcare Informatics – Identification of subjects of healthcare	HI Database Design
NIST 800-12: 1996, An Introduction to Computer Security - The NIST Handbook, Chapter 18: Audit Trails	HI Security
NeAF:2009, (National e-Authentication Framework)	HI Service Authentication
SAML version 2.0: 2005, Security Assertion Markup Language	Secure Messaging
Secure XMLL: 2007- W3C, XML Encryption Syntax and Processing	Secure Messaging
OASIS Web Services Security: 2007, SOAP Message Security 1.2	Secure Messaging
OASIS 0193:2008 WS-Security Policy 1.2	Secure Messaging
W3C 0172:2008, W3C, Web Services Addressing 1.0, Metadata	Secure Messaging
W3C 0192:2008, Web Services Policy 1.5, Framework	Secure Messaging
W3C HTTP:1999, Hypertext Transfer Protocol, Version 1.1 (IETF RFC 2616)	Secure Messaging
W3C SOAP: 2003, SOAP Part 1: Messaging Framework, Version 1.2	Secure Messaging
W3C SOAP: 2003, SOAP Version 1.2 Part 2: Adjuncts, SOAP Version 1.2 Part 2: Adjuncts	Secure Messaging