nehta

Level 25, 56 Pitt Street
Sydney NSW 2000
Telephone: (02) 8298 2600
Facsimile: (02) 8298 2666
www.nehta.gov.au

12 May 2014

Professor Barbara McDonald
Commissioner
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001

Dear Professor McDonald

The National E-Health Transition Authority (**NEHTA**) welcomes the opportunity to provide a submission to the Australian Law Reform Commission's Serious Invasions of Privacy in the Digital Era Discussion Paper (**Discussion Paper**).

NEHTA is the lead organisation supporting the national vision for eHealth in Australia; working with consumers, healthcare providers, the ICT industry and Governments to enable safer, higher quality and sustainable healthcare. NEHTA was the managing agent for the development of the Personally Controlled Electronic Health (**eHealth**) Record on behalf of the Department of Health.

The eHealth record system, launched in June 2012, is an electronic record for a patient that contains a summary of their health information. It is a key element of the national health reform agenda around making the health system more agile and sustainable. As at 24 April 2014, over 1,570,000 consumers had registered for an eHealth record with 6,887 healthcare organisations participating.

NEHTA acknowledges its previous submission to the ALRC in November 2013 on the Serious Invasions of Privacy in the Digital Era Issues Paper, in particular the submissions that:

1. The privacy framework for the eHealth record system provides an effective deterrent against unauthorised use, collection or disclosure of personal and health information in the eHealth record system. The framework provides significant penalties for privacy breaches by participants of the eHealth record system.

2. Consumers who participate in the eHealth record system have a range of privacy controls available to them, including the ability to limit access by others to their record as a whole or of certain documents, to request notifications, remove documents from their record and to view an audit log.

3. The existing privacy framework of the eHealth record system is appropriate given the combination of punitive measures preventing misuse of personal information in the eHealth record system and the empowering of consumers to control how their information is used and disclosed.

4. The *Personally Controlled Electronic Health Records Act 2010* provides for a review of the legislation to commence on 1 July 2014. The review may significantly impact on the privacy framework by changing the consent model to opt-out and the system's governance framework. Bearing in mind that the eHealth record system is still in an early adoption phase and given that the first review is forthcoming, it would be premature to impose a new cause of action for serious privacy invasion upon the eHealth record system.

This submission addresses the Discussion Paper from the perspective of NEHTA's role in shaping eHealth technology in Australia, including the eHealth record programme. Specifically, this submission covers;

- NEHTA's understanding of privacy issues within the digital era relating to eHealth.
- How the eHealth record system and other eHealth initiatives are designed to support secure management of health information.
- How the adoption of eHealth products can make an individual a controller of their personal information and can aid with privacy protection.

1. eHealth and the Digital Era

> We see the effect of rapid communication in other areas of our life, and we're getting to a point now where we expect that in healthcare. When I see you in an emergency department, in a general practice setting, in a specialist room, I'll have more rapid access to up to date information about what's happened to you in the past.
>
> *Resident Medical Officer, Perth*

NEHTA recognises that it is important for health services to meet the expectations of consumers who are increasingly connected and empowered through technology. In addition to the changes in technology, there has been a shift toward patients playing a more active role in the management of their own health. This, combined with well documented trends such as the rising cost of healthcare, the growth of chronic conditions and an ageing population, call for changing the way information is shared to enable the right information to be accessed for the right person, at the right time and place.

NEHTA notes that the provision of quality healthcare requires the sharing of health information between various healthcare providers within the private and public sectors including general practices, hospital, imaging centres, specialists and allied health practices. Having access to accurate personal information and sharing it securely and efficiently is essential for the high quality healthcare that Australians expect.

> In my 20 years of practice, I've administered around 20,000 anaesthetics and I can count on one hand the number of times I have seen GP information before my pre-operative assessment.
>
> *Anaesthetist, Melbourne*

NEHTA understands that healthcare providers treat patients most effectively when they have access to all the necessary clinical information. It is therefore important that a healthcare provider's access to timely and accurate health information not be unduly restricted.

Since 2006, NEHTA has engaged with key stakeholders in the healthcare sector about eHealth. Despite the sensitive nature of health information, consumers who frequently engage in Australia's healthcare system have been the stakeholders most favourable toward sharing health information via the eHealth record system.

The recent Office of the Australian Information Commissioner's Community Attitudes to Privacy survey supports this by highlighting that:

- Respondents were asked to state the extent to which they trust twelve different types of organisations. Health service providers continue to enjoy the highest levels of trust with nine in ten (90%) Australians saying they are trustworthy — the same level (91%) as when measured six years ago.[1]

- Respondents were asked to nominate which of four options best described their views on access to health information. One in three (31%) respondents was happy for their healthcare information being shared for a specific health related matter. One in four (25%) respondents stated that their health information could be shared between healthcare providers for anything to do with their health.[2]

- Respondents were asked to what extent they thought their doctor should be able to discuss their personal medical details with other health professionals without their consent. Two in three (66%) respondents stated they were prepared to accept their doctor discussing personal health details without their consent. This number has increased over time from six in ten (59%) in 2007.[3]

The eHealth record system has significant potential to address the problems created by fragmented information in the current healthcare system and to meet the expectations of a community within the digital era by providing individuals and their healthcare providers with better access to their health information.

2. Secure Management of Health Information

> My patients can go to hospital and not have to carry bits of paper that I've had to print out, and that they often lose en route, or they can't decipher at the other end.
>
> *GP in eHealth lead implementation site, Sydney*

In the design and development of eHealth products and systems, NEHTA is implementing numerous security controls to safeguard both the services, and those who will be using them. As such, these eHealth products and systems are designed to support the secure management of health information, which in turn improves the ability for providers to uphold privacy requirements.

Security Protections in the eHealth record system

The eHealth record system utilises multiple layers of technical and non-technical controls in order to maintain security. These controls include authentication of authorised users, robust

[1] Page 27, OAIC Community Attitudes to Privacy survey Research Report 2013.
[2] Page 31, OAIC Community Attitudes to Privacy survey Research Report 2013.
[3] Page 31-32, OAIC Community Attitudes to Privacy survey Research Report 2013.

audit logs, proactive monitoring and reporting, rigorous security testing, governance and the provision of education and training materials to the users of the system.

The layers of security protection associated with the eHealth record system ensure that:

- people seeking access to information are who they claim to be and healthcare providers uploading information are who they claim to be;
- information transmitted across networks is encrypted and arrives at its destination point without interference; and
- access to information is appropriately authorised.

Core to the security development of the eHealth record system is compliance to Commonwealth security standards, policies and frameworks, namely the Protective Services Policy Framework, the Information Security Manual and the National eAuthentication Framework, in addition to alignment to the international best practice security management standards ISO/ECI27001. The security requirements for NEHTA's products are mapped to these frameworks.

The National eHealth Security and Access Framework (NeSAF)

NEHTA has also developed the NeSAF, a set of tools designed to support organisations engaged in national eHealth. The NeSAF provides guidance to businesses in how to establish an information security infrastructure, for example by helping to assess security risks, and selecting the appropriate controls.

The NeSAF encourages businesses to adopt a consistent approach to the application of health information security standards, and provides better practice guidance in relation to eHealth-specific security and access practices. NEHTA has itself used the NeSAF in designing the eHealth record security architecture.

3. Adoption of eHealth Products

> Secure electronic health records can support better auditing of how health information is shared and managed. In turn, helping a provider meet ongoing privacy obligations.
>
> *Clinical Governance Unit, NEHTA*

NEHTA submits that the adoption of eHealth products by healthcare providers can help with privacy protection. Amongst other things, eHealth products can reduce the risk of inappropriate or unauthorised access and support healthcare providers in meeting their obligations under privacy law.

Secure Message Delivery

Secure Messaging is the secure point-to-point delivery of healthcare messages to a single known receiving organisation.

Secure Message Delivery (SMD) is a set of three Australian Technical Standards which, when coupled with other foundational eHealth specifications and services, provide the basis for technical interconnectivity between Secure Messaging services.

SMD enables healthcare providers to communicate electronically with other healthcare providers irrespective of the secure messaging vendors they use. Having an efficient, secure communication mechanism with fewer constraints than existing systems has the potential to reduce barriers to the timely exchange of health information.

The security measures in SMD minimise the risk that sensitive information will be intercepted or disclosed without authorisation. SMD prevents unauthorised interception of message content and provides verification that the message has not been altered since it was sent. The SMD payload, or 'message,' is encrypted prior to transmission such that it can only be read by the intended receiving organisation. The sending organisation can be confident that the message reached the *intended* receiving organisation through a receipt notification.

Audit capability of the eHealth record system

The eHealth record system provides an audit service to record all activity on the National eHealth infrastructure services and eHealth record conformant repositories. The audit log contains information such as:

- the date and time the eHealth record was accessed/edited;
- the organisation that accessed/edited the eHealth record and the role of the individual who accessed it;
- whether the record was accessed because of an emergency; and
- details of the action(s) that occurred, for example, clinical document created or deleted.

Healthcare organisations will only be able to view a log of their own access to an individual's eHealth record. However, the *Personally Controlled Electronic Health Records Act 2010* authorises the System Operator to comply with a subpoena to disclose health information in a consumer's eHealth record of the subpoena is given in the course of proceedings relating to indemnity cover to a healthcare provider.[4] This would include circumstances where an insured provider is defending a negligence claim brought by a consumer.

> PCEHRs that meet the needs of consumers can build consumer confidence and trust in the health system … they can empower consumers to be active partners in their health and make informed decisions about their healthcare.
>
> *Consumer Health Forum of Australia*

NEHTA notes the Discussion Paper's Guiding Principle 9: privacy protection is an issue of shared responsibility, and the comment that:

> *Organisations that collect, store, process, or disclose information have a responsibility to empower individuals to control their own personal information as much as practicable and appropriate, but also to take steps to protect the privacy of individuals.*[5]

Prior to registering for an eHealth record, an individual has limited control over what happens to their health information and very limited access to their health records, unless the

[4] Personally Controlled Electronic Health Records Act 2010 (Cth), section 69.

[5] Australian Law Reform Commission Serious Invasions of Privacy in the Digital Era Discussion Paper 2014, at 2.36.

individual visits the healthcare professional where their records are stored and asks for them. However, central to the eHealth record system is the concept of personal control.

The eHealth record system empowers individuals to exercise control over their own health information, in keeping with the commentary above. An individual can control their eHealth record in the following ways:

- decide whether or not to have an eHealth record;
- access information in their eHealth record;
- set controls around healthcare provider organisation access;
- authorise others, such as carers or family members, to access their eHealth record;
- choose which information is published to and accessible through their eHealth record;
- view an activity history for their eHealth record;
- set up notifications about certain types of activity on their eHealth record, for example being sent a text message when a new healthcare organisation has accessed their eHealth record; and
- make enquiries and complaints in relation to the management of information in their eHealth record.

I hope this submission assists the ALRC in its consideration of this important aspect of potential law reform. I would be pleased to discuss any aspects of NEHTA's submission with you if required.

Yours sincerely

Bettina McMahon
Head of Risk & Assurance
NEHTA