Serious Invasions of Privacy in the Digital Era
Australian Law Reform Commission Issues Paper 43 – October 2013

Submission to the Australian Law Reform Commission

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

NEHTA was established in 2005 by the Council of Australian Governments to help transform Australia's health system by building the foundations for a national eHealth infrastructure. In 2010, the Commonwealth Government appointed NEHTA as the managing agent for the Personally Controlled Electronic Health Record (**eHealth record**) System.

Launched in July 2012, the eHealth record system is an electronic record for an individual that contains a summary of their health information. It is a key element of the national health reform agenda, aimed at making the health system more agile and sustainable. The eHealth record system is still in an early adoption phase. As at 29 October 2013, 1,042,966 consumers had registered for an eHealth record with 5,681 healthcare organisations participating.

Now that the eHealth record system is operational, NEHTA's programme of work represents a new focus on adoption and implementation. NEHTA will continue to build capacity in life-cycle management of the underlying technologies and standards for eHealth and continue to engage with software vendors and implementers to ensure comprehensive adoption of eHealth products and solutions.

Part A: The privacy framework for the eHealth record system

The following information is presented by way of background to NEHTA's submissions:

1. The health information contained within a consumer's eHealth record, including the healthcare identifier, is regulated by the *Healthcare Identifiers Act 2010* (**HI Act**) and the *Personally Controlled Electronic Health Records Act 2012* (**PCEHR Act**). These Acts operate concurrently with Commonwealth, State and Territory privacy laws.

2. The HI Act and the PCEHR Act each set out clear purposes for which a consumer's health information, including the healthcare identifier (**IHI**), can be used. Any collection, use or disclosure of health information or the healthcare identifier not for an authorised purpose set out in the Acts, is an unauthorised use, collection or disclosure. Each Act allows for a range of remedies, including civil penalties.

Authorised purposes

3. Under the HI Act, the authorised purposes for which healthcare identifiers may be used or disclosed include:

    - the provision of healthcare to the patient;

- the management (including investigating or resolving complaints), funding, monitoring or evaluation of healthcare;
- the provision of medical indemnity cover for a healthcare provider;
- the conduct of research that has been approved by a Human Research Ethics Committee;
- lessening or preventing a serious threat to an individual's life, health or safety or to public health or safety; and
- purposes authorised under another law. For example, a provider may be legally compelled to disclose an individual's IHI if issued a subpoena by a court for the provision of information. [1]

4. Under the PCEHR Act, the authorised purposes for which health information included in a registered consumer's eHealth record may be collected, used or disclosed include:

- providing healthcare to a consumer (noting that access must be consistent with the access controls set by the consumer)
- necessary to lessen or prevent serious threat to an individual's life, health or safety (and your consent cannot be obtained)
- necessary to lessen or prevent a serious threat to public health and safety
- for the management or operation of the eHealth record system
- for another purpose authorised or required by law or for law enforcement purposes
- to a consumer's nominated or authorised representative, in accordance with the consumer's access controls
- any purpose that the consumer has consented to; and
- for purposes relating to indemnity cover for a healthcare professional. [2]

Consequences of unauthorised collection, use or disclosure

5. The HI Act provides civil penalties and criminal sanctions, where there is an unauthorised use or disclosure of a healthcare identifier. Pursuant to section 26 of the HI Act, the use or disclosure of an IHI for an unauthorised purpose is an offence and a person convicted of this offence may be imprisoned for two years or fined $20,400, or both. If a body corporate is convicted of this offence, a court may impose a fine of up to $102,000.

6. The PCEHR Act similarly provides penalties for privacy breaches by participants in the eHealth record system. Pursuant to sections 59 and 60 of the PCEHR Act, the collection, use or disclosure of health information in a consumer's eHealth record for an unauthorised purpose is an offence and a person convicted of this offence may be fined up to $13,200. If a

[1] Part 3 of the *Healthcare Identifiers Act 2010* (Cth).
[2] Part 4 of the *Personally Controlled Electronic Health Records Act 2012* (Cth).

body corporate is convicted of this offence, a court may impose a fine of up to $66,000. However, for a court to impose a fine, the person must have known or was reckless as to the fact that the use, collection or disclosure of health information in a consumer's PCEHR was not for an authorised purpose.

7. There are also other provisions in the PCEHR Act which allow for civil penalties where certain actions occur that might compromise the security or integrity of the eHealth record system.[3]

Enforcement powers of the Information Commissioner

8. The Office of the Australian Information Commissioner regulates the handling of IHIs by all entities and regulates the handling of health information under the eHealth record system by Commonwealth government agencies, private sector organisations and some state and territory bodies in particular circumstances.

9. Under the eHealth record system, the functions and enforcement powers available to the Information Commissioner include:

   - using existing Privacy Act investigative and enforcement mechanisms, including conciliation of complaints and formal determinations;
   - accepting data breach notifications from the System Operator, and certain repository operators and portal operators;
   - seeking an injunction to restrain or require particular conduct;
   - accepting enforceable undertakings; and
   - seeking a civil penalty order from a Court.[4]

Part B: NEHTA's submissions

10. NEHTA submits that 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. As detailed above, the framework provides significant penalties for privacy breaches by participants of the eHealth record system. Specifically, civil penalties may be imposed where there is an unauthorised use, collection or disclosure of information in a consumer's eHealth record or where certain actions occur that might compromise the integrity of the eHealth record system.

11. Consumers who participate in the 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. They can also request notifications where information is uploaded or has been disclosed and can view who has accessed their record by way of the audit log. Further, individuals can remove documents from their eHealth record instantaneously via the

[3] Sections 74 and 76 of the *Personally Controlled Electronic Health Records Act 2012* (Cth).
[4] Part 2 to Part 4 of the *PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013*.

internet or a dedicated phone line. 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 lead us to submit that the existing framework is appropriate.

12. The PCEHR Act provides for a review of the legislation to commence on 1 July 2014. The review will consider, amongst other things, alternative governance structures for the PCEHR system. It will also consider the opt-in nature of the system including the feasibility and appropriateness of a transition to an opt-out system. The review may significantly impact on the privacy framework by changing the consent model and 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 in less than a year, it would be premature to impose a new cause of action for serious privacy invasion upon the PCEHR system.

Part C: Responses to questions posed in the Issues Paper

Question 1

13. Question 1 of the Issues Paper asks:

> *What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?*

14. Central to the eHealth record system is the concept of personal control. Consumers can exercise control over 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; and
- make enquiries and complaints in relation to the management of information in their eHealth record.

15. This notion of making an individual a controller of their personal information underpins many other platforms, programs and apps. An entity must take sound steps to empower an individual to control their personal information and properly inform them of this fact. The responsibility for protecting the personal information of the individual is then a joint one. Accordingly, NEHTA submits that, the principles guiding the development of the proposals for reform should include:

'**Personal responsibility**': individuals must be empowered to protect their own privacy and, once empowered, share a responsibility to protect their personal information.

Question 3

16. Question 3 of the Issues Paper asks:

    What specific types of activities should the ALRC ensure are not unduly restricted by a statutory cause of action for serious invasion of privacy?

17. NEHTA submits that, any cause of action for serious invasion of privacy should not impinge on the free flow of health information where sharing of that information is needed. The importance of appropriate sharing and communication of health information to treat a patient or bring about better health outcomes is well recognised by stakeholders. The OAIC's recent *Community Attitudes to Privacy* survey indicates that:

    - Australians want their information shared between healthcare providers for healthcare purposes. 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.[5]
    - Australians are comfortable with their doctor discussing their personal health details with other health professionals without their consent. 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.[6]
    - Healthcare providers are trusted with personal information. 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.[7]

NEHTA

8 November 2013

[5] Page 31, OAIC Community Attitudes to Privacy Survey Research Report 2013.
[6] Page 31-32, OAIC Community Attitudes to Privacy Survey Research Report 2013.
[7] Page 27, OAIC Community Attitudes to Privacy Survey Research Report 2013.