Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

18 July 2014

Linda Powell
First Assistant Secretary
eHealth Division
Department of Health
Linda.Powell@health.gov.au

Dear Linda

Re: Review of the PCEHR

Thank you for your invitation to me, in my role as Chair of the APF, to "meet with you to discuss the privacy implications of the recommendations [of the Review of the PCEHR], including to get your views on others we might consult, and the types of questions and issues that need to be explored".

APF has made strenuous endeavours over an extended period to represent patients' privacy interests, within the context of patients' interests in quality information systems to support quality health care.

Those endeavours have been sidelined by NEHTA, and by the Department, to the extent of being almost entirely ignored.

APF accordingly welcomes this invitation, but fears that, based on the record of relevant agencies to date, APF's representations will again be largely ignored. This meeting follows a long period of silence. We further fear that another long period of silence will occur before contact is made, yet again, in yet another desperate attempt to resuscitate the disaster that is the PCEHR.

I attach notes on our position on the matter, together with an index of the submissions that we have made in the past, and that declare our views on the characteristics of an appropriate health records scheme.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 6916 Chair@privacy.org.au

Australian Privacy Foundation

Review of the PCEHR of December 2013, released May 2014

Summary of Position
18 July 2014

Roger Clarke, as Chair, Australian Privacy Foundation

APF has been, and continues to be, a strong supporter of appropriate applications of information technology in support of people. In relation to applications to patients' health data, the APF's policy has long been that, for a scheme to be appropriate, it must satisfy key principles (APF Policy Statement, 2009). The most central of these are:

- The primary purpose of personal health care data is personal health care
- Other purposes of personal health care data are secondary, or tertiary
- Patients must be recognised as the key stakeholder
- Data consolidation is inherently risky
- The health care sector must remain a federation of islands
- Consolidated health records must be the exception not the norm
- Identifiers must be at the level of individual applications
- Pseudo-identifiers must be widely-used
- Anonymity and persistent pseudonyms must be actively supported
- Personal data quality and security must be assured

NEHTA and DoH resisted or simply ignored APF's submissions, with the result that the PCEHR is grosssly in breach of virtually all of these principles, and is unsupportable in anything like its current form. During 2013, in order to overcome the embarrassment of extremely low voluntary adoption rates, the Department stooped to fraudulent means of achieve enrolments.

The Review conducted during 2013 abjectly failed to reflect the submissions put to it in relation to the scheme's failure to address the needs of patients, its highly anti-privacy architecture and design, and its focus on the needs of public servants rather than patients and clinicians.

The relevant Recommendations, excerpted in the following pages, would drive the scheme, under whatever name is chosen, yet further away from patient-orientation and privacy-sensitivity.

APF emphatically opposes:

- the renege on the commitment to a consent-based scheme and the imposition of opt-out (R13)
- the further reduction in what little patient control exists (R21)
- the centralisation of the scheme within DHS (R11)
- the endeavour to divert all messages through a government-run hub (R23)
- the facilitation of a national identification scheme and database (R25)
- the centralisation of extraordinarily sensitive data (R38)
- the ongoing very low level of engagement with consumer interests (*inter alia*, R18, R26)

The sole glimmer of hope in the entire set of Recommendations is R32.

APF:

- **strongly supports "re-setting the policy standards and frameworks necessary to enable interoperability, in a decentralised model"**
- **proposes that this be adopted as the primary principle underlying the scheme**
- **proposes that the architecture and features be adapted to comply with that principle**

Australian Privacy Foundation

Review of the PCEHR of December 2013, released May 2014
Relevant Recommendations and APF's Reactions to Them

Roger Clarke – Chair, Australian Privacy Foundation

Notes of 18 July 2014

11. Centralise the system operation of the MyHR to the Department of Human Services

APF notes that this dramatically increases the risk of appropriation of sensitive personal data , and further undermines any remaining confidence that consumers might have about the national database that the PCEHR is designed to enable.

APF accordingly expresses the most serious concern about this proposal.

13. Transition to an 'opt-out' model for all Australians

APF notes that the undertakings of successive Ministers have proven to be completely worthless. The desire of the public sector for a national database has won through.

APF re-expresses its complete opposition to the proposal.

16. Commission an Information Security Risk Assessment of ... consumer information

APF notes that such an assessment was an obligatory part of the original project, and should have been conducted early, and iteratively throughout the last five years.

APF expresses its dismay at the appalling lack of professionalism of NEHTA and DoH that has given rise to the need for such a Recommendation.

18. Develop and conduct an education campaign

APF notes that, yet again, the proposal is to bludgeon the public into submission, not engage with it.

21. Implement a minimum composite of records

APF notes that not only is it proposed that the freedom not to have a hub-record created be removed, but that personal control over what it contains is to be removed as well.

APF expresses its complete opposition to this further imposition.

23. Implement a standardised Secure Messaging platform for the medical industry

APF notes that the expression 'platform' implies that messages are to pass through a hub, which creates a massive risk of appropriation of sensitive personal data.

APF expresses its complete opposition to the notion of a 'platform', and re-expresses its support for a decentralised model of secure clinician-to-clinician messaging.

Further, APF notes that support for secure messaging has been a responsibility of DoH for two decades, yet the Department, and subsequently NEHTA, has failed to establish this crucial building-block for effective health care information systems.

APF expresses its dismay at the appalling lack of professionalism of NEHTA and DoH that has given rise to the need for any Recommendation about secure messaging.

25. Review the NASH platform ... to align with the recommendations for Digital Identity

APF notes that terms such as 'Digital Identity' are commonly used within the public service as code-words for a universal national identifier, underpinning a national database.

APF expresses the most serious concern about the risk of consolidation of personal data and the imposition on individuals of a single identity or the correlation of their multiple identities.

26. Review the ... development program ... in partnership with industry

APF notes that, yet again, consumers are excluded from participation, despite the pretence that the scheme is intended to benefit patients.

28. Notify the consumer via an SMS when their MyHR is opened or used by default

APF notes that this was a mandatory design feature of the original scheme.

APF expresses its dismay at the appalling lack of professionalism of NEHTA and DoH that has given rise to the need for such a Recommendation.

Further, APF notes that many individuals may not want to receive, or may not be able to receive, SMS messages.

APF expresses its dismay at the failure of NEHTA and DoH to comply with their undertakings and implement an effective notification scheme.

31. ... update the MyHR strategy to actively enable decentralisation of information across multiple data repositories ...

APF notes that this is mystifying and disturbing. The scheme was supposed to feature a hub-record that provided links to data in multiple, decentralised repositories.

APF expresses the utmost concern that NEHTA may have implemented a scheme that breaches even those very limited undertakings that had been given in relation to the scheme's architecture.

32. Reset the policy standards and frameworks necessary to enable interoperability, in a decentralised model ...

APF notes that this is a critical feature that APF and other consumer organisations have sought from the outset two decades ago.

APF strongly supports this proposal, and argues that the only way in which the scheme will serve the interests of patients is for this to be the primary principle around which all others revolve.

38. Alter the Medicare Item number requirements from January 1st 2015, for health assessments comprehensive assessments, mental health care plans, medication management reviews and chronic disease planning items to require a copy of the information to be uploaded to the MyHR.

APF notes that this is a quite gross proposal, using the power of the purse as a means of imposing draconian provisions, placing highly sensitive personal data at risk.

APF expresses its complete opposition to any such proposition, and submits that it undermines the willingness to participate of even the most ardent supporters of the scheme.

Australian Privacy Foundation

Electronic Health Records and the PCEHR
Key Policy Statements and Submissions

Over the last two decades, APF has committed considerable resources to this topic, in an endeavour to assist in the achievement of schemes that deliver quality information systems in support of quality patient care, but with privacy-protection embedded in them. For the complete index, see: http://www.privacy.org.au/Papers/indexPolicies.html#eH

eHealth Data and Health Identifiers
Policy Statement (28 August 2009)
http://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf

Review of the PCEHR
Response to the Health Minister (26 May 2014)
http://www.privacy.org.au/Papers/HlthMin-PCEHRRev-140526.pdf

Security and Privacy Aspects of the PCEHR
Submission to Minister for Health (16 Apr 2014)
http://www.privacy.org.au/Papers/PCEHR-140416.pdf

The PCEHR
Submission to the Review of the PCEHR (22 Nov 2013)
http://www.privacy.org.au/Papers/PCEHR-131122.pdf

Personally Controlled Electronic Health Record (PCEHR)
Public Statement (3 Nov 2013)
http://www.privacy.org.au/Papers/PCEHR-131103.pdf

PCEHR – FAQ for Clinicians
Public Advisory Statement (11 Aug 2013)
http://www.privacy.org.au/Resources/AS-PCEHR-Clin.pdf

PCEHR – FAQ for Consumers
Public Advisory Statement (11 Aug 2013)
http://www.privacy.org.au/Resources/AS-PCEHR-Cons.pdf

The PCEHR Concept of Operations
Submission to NEHTA (30 May 2011)
http://www.privacy.org.au/Papers/NEHTA-ConOps-110530.pdf

Checklist of Privacy Concerns about the Personally Controlled eHealth Record (PCEHR)
Submission to NEHTA (15 Feb 2011)
http://www.privacy.org.au/Papers/PCEHR-Privacy-110215.pdf

Checklist of Consumer Concerns
Submission to NEHTA (25 Jan 2011)
http://www.privacy.org.au/Papers/PCEHR-CRG-ChkLst-110125.pdf

Consultation Process re PCEHR
Submission to CEO of NEHTA (8 Nov 2010)
http://www.privacy.org.au/Papers/PCEHR-Fleming-101108.pdf

eHealth Care Data Breach
Policy Statement (28 August 2009)
http://www.privacy.org.au/Papers/eHealth-DataBreach-090828.pdf