Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

15 November 2010

Andrew Howard, CIO, NEHTA

cc. Dr Mukesh Haikerwal, National Clinical Lead, NEHTA
Bettina McMahon, Head of Policy and Privacy, NEHTA
Melanie Goldwater, Privacy Manager, NEHTA
Catherine Bramwell, DoHA

Dear Andrew

Re: PCEHR – Design Issues

The Roundtable on Wednesday 10 November was, from the advocacy perspective, a valuable event. Information was presented at the meeting. Considerable interaction occurred, some of it was responded to, some of it appeared to be assimilated, and all of it, we trust, was recorded for playback shortly.

This letter notes a number of design issues that we consider to be critical to ongoing progress. A separate letter addresses process matters.

The attachment requests specific commitments from NEHTA, in the form of positive and explicit responses to each matter, as a means of ensuring privacy-sensitive design of the PCEHR.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

The PCEHR Consultation

Design Matters

No documentation or copies of slide-sets were provided in advance of the Roundtable, nor at the Roundtable, nor in the days immediately following it. The list below therefore depends on on-the-fly note-taking during the rapid presentations.

PEHR Slide-Set

1. The PCEHR was announced by the Minister in June 2010. The slide-sets presented at the Roundtable referred to the predecessor PEHR proposal. It is essential that explicit, written undertakings be provided that all important, privacy-protective design features are commitments in relation to the PCEHR.

Personal Control

2. It essential that explicit, written undertakings be provided in relation to the design requirements of "a record that is at all times owned and controlled by the patient" and "control of access is key".

3. It essential that the above design requirements be articulated into design features, and that those features also be the subject of explicit, written undertakings. The following aspects are of particular concern to the APF:

- personal control must apply to the data in the record, not just the record
- personal control must exist irrespective of the possession or custodianship of the record
- personal control must extend to copies of the data that are extracted from the record
- all handling of data in the record must be the subject of consent
  (handling is comprehensive, including collection, recording, amendment, deletion and access)
- great care must be taken to avoid dilution through unjustified dependence on 'implied consent'
- access to the record must be proof against the wide array of demand powers that exist
- there must be clear assurances in relation to security measures against unconsented access by second and third parties
- refusal to provide access must not give rise to compromises to the person's interests, such as service denial, service reduction or cost penalties (although clearly the quality of service may be compromised by the denial, and that should be made clear to the person)
- there must be:
  - sanctions against breach
  - business processes to deal with complaints and enforcement
  - specific commitments to perform those processes

Enforceability

4. It essential that the following design features be the subject of explicit, written undertakings:

- all accesses are logged
- the log includes the identifier(s) of the individual users who gain access
- identifiers are personal not generic (e.g. duty doctor, clinic manager, secretary)
- all staff of all organisations have identifiers
- it is an offence for an individual to permit another person to use their identifier
- it is an offence for an organisation to require, encourage or permit an individual who performs a function on behalf of that organisation to permit another person to use their identifier
- there must be sanctions against breach, business processes to deal with complaints and enforcement, and specific commitments to perform those processes

[It is appreciated that this involves inter-play with the Health Identifiers system. The APF would welcome appropriate interactions with Medicare on these issues.]

Architectural Features

5. It essential that the following design features be the subject of explicit, written undertakings:
- multiple Conformant Repositories, not a single consolidated database
- existing repositories remain in place and are not merged
- a Service Coordination Layer facilitates access from remote locations
- allowance is made for differential levels of trustworthiness of remote locations

6. The APF expresses serious concern, however, about the following features:
- the personal records are to be centralised in a single national repository
- no provision is being made for storage of the PCEHR in repositories of the person's choice
- clinician databases are excluded from ever being Conformant Repositories
  This is a serious issues because it creates a strong tendency away from a 'federation of databases' model and towards a 'centralised database' model'.
  [The APF appreciates that an early implementation may need to avoid being over-ambitious.
  [The APF sees it as essential to public trust (as well as to scalabiity) that the architecture not preclude the authoritative data remaining in the appropriate clinician's repository, and copies of the data only being provided to others when the person provides consent]

Operational Features

7. It essential that the many privacy-sensitive design features that were in the mockup demonstration provided at the Roundtable be the subject of explicit, written undertakings.

[It is not possible to be more specific at this stage, because no documentation was provided, and note-taking was impractical.]

8. The APF expresses strong interest in the Organisational Access Levels feature, comprising:
- No Access
- Standard
- Standard and Sealed
- Emergency (Standard and Sealed), with post-notification of access
- Locked

9. The APF expresses serious concern about the suggestion that treatment locations would download large numbers of items from remote sources 'on the offchance' that one or more local clinicians might want to accesss them. This represents a serious breach of the relevance principle.

It essential that the following design feature be the subject of explicit, written undertakings:
- download of clinical data must be based on a positive decision by a treating clinician that the specific data is relevant to the specific work being undertaken by that treating clinician

10. It was stated that "There's no commitment to monitoring of logs. It's up to the consumer".

The APF expresses serious concern at this suggestion.

It essential that the following design features be the subject of explicit, written undertakings:
- long-term accessibility of access logs by the relevant person and their agents
- automated anomaly-detection
- action by repository-operators arising from anomalies
  [A very important example is the need for all accesses without consent – i.e. exercises of the Emergency Organisational Access Level – to be detected, and post-notified to the person]