Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

10 December 2010

Dr Mukesh Haikerwal, National Clinical Lead, NEHTA

cc. Andrew Howard, CIO, NEHTA
Bettina McMahon, Head of Policy and Privacy, NEHTA
Melanie Goldwater, Privacy Manager, NEHTA
Catherine Bramwell, DoHA

Dear Mukesh

Re: PCEHR – The November Roundtables

I refer to our letters to yourself and Andrew of 15 November, and the 'Summary of key issues raised at PCEHR roundtables' document sent out this morning.

1. The summary is very scant, and does not reflect either the scope or the depth of the discussions at the Consumer Roundtable.
2. An undertaking was given to distribute copies of the slide-sets that were presented on the day. It does not appear that we've received them. Would you please despatch copies, as per NEHTA's undertakings.
3. In view of the brevity of the Summary, would you please distribute to all participants in at least the Consumer Roundtable the attached summaries of Process and Design Issues. These were sent to Mukesh and Andrew on 15 November, but I have yet to receive even acknowledgements let alone the requested substantive responses.

We would appreciate responses both to this letter and to our previous letters to your organisation.

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
Comments following the Consumer Roundtable on 10 November 2010

Process Matters

General

1. No documentation or copies of slide-sets was 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. That is not a good way to achieve effective consultation.

2. During the self-introductions, there were multiple expressions of concerns about:
- real engagement
- proper governance
- benefits for consumers not just administration

Several mentions were made of aboriginal health services being undermined by limited infrastructure and late engagement, and of the challenges involved to privacy and confidentiality.

3. APF expressed four first-round areas of concern:
- 'personally-controlled' means what?
- the role of consent
- the missing privacy component of the legislative package
- the Minister has committed to PIAs, but when do they start, and what process will be used?

Deep-Level Consultation Arrangements

4. It was stated that Workshops have already been held on specific aspects, under NDAs. APF was not aware of them, and was not invited to any such events.

5. The APF expresses serious concern about the existence of multi-level consultation arrangements, and the exclusion of relevant civil society from some of those levels.

6. The APF draws to attention its longstanding policy in relation to confidentiality, and its in-principle agreement that a proportion of the information that arises in deep-level consultations are by their nature in-confidence. It would welcome such a statement being applied to such events.

7. It is essential that:
- multi-tier consultation arrangements be known to relevant civil society
- relevant civil society organisations be able to participate in relevant deep-layer workshops
- the APF in particular be engaged in relevant deep-layer workshops

Personal Choice / Opt-In

8. It was stated that the scheme was, at the Minister's directions, opt-in / consent-based.

This is crucial to public trust. There will be strong motivations for patients with chronic and complex conditions to opt-in, because they stand to gain from the scheme. The motivations for other categories of patients to opt-in will be lower, and – at least until the credibility of quality, security and privacy assurances are established – many people will rationally prefer to remain outside the scheme.

9. It is essential that:
- an explicit, written undertaking be provided that the scheme will be, and will remain, opt-in / consent-based
- to the extent practicable, this will be entrenched in legal, organisational and technical designs

- the legal, organisational and technical designs will not be devised in order to leave open the option of switching to a compulsory scheme
- to the extent practicable, there will be no penalties for not opting in
- the legal, organisational and technical designs will not be devised in order to create or exacerbate penalties for not opting in

Governance Structures

10. It was stated that there is to be "rigorous governance and oversight to maintain privacy", but also that the specifics have not been decided yet.

11. APF expresses concern in the following areas:
- current privacy laws are grossly inadequate. In particular:
  - they are general rather than specific
  - they provide almost no sanctions
  - where regulators exist, their powers are extremely limited
  - where regulators exist, they are seriously under-resourced
  - the Australian Privacy Commissioner and OAIC are completely inadequate to the task, and a much more powerful and specific regulator is necessary
- the enabling legislation for eHealth has to date included no privacy protections
- despite the explicit commitments given by the Minister, the APF is not aware of any PIA processes having been commenced, even on the health identifier system
- no proposal for governance structures has yet been brought forward
- the Roundtables were declared by NEHTA to not be part of the consultation process
- no mechanism was proposed whereby governance structures would be formed
- no commitment was given that civil society would be consulted in the development of the governance structures

12. APF reiterates the specific proposals it put forward at the Roundtable, as follows:
- a Consumer Steering Committee, reporting to the NEHTA Board
- a Consumer Reference Group, beneath the Steering Committee
- very broad and open membership of the Reference Group
- sufficiently large membership of the Steering Committee that all perpectives have a voice
- formal requirements that the Steering Committee represent the views of the Reference Group i.e. under no circumstances can the Steering Committee be appointees with independent standing, acting as principals rather than as agents of the Reference Group

Governance Processes

13. Mentions of 'governance' were primarily focussed on institutions, representation and relationships.

By itself, governance structure does not provide protection.

14. It is essential that:
- governance structures be accompanied by processes
- goverance processes be specified at a sufficient level of detail
- governance processes be mandatory, and non-compliance be an offence

Interplay Between Federal and State Laws

15. It is understood that (some?) States and Territories wish to retain their existing privacy laws as they affect the health care sector.

16. It is essential that a set of principles be established, reflecting the privacy-relevant undertakings given in relation to the system, which all States and Territories agree to ensure are implemented in their laws.

Australian Privacy Foundation

The PCEHR Consultation
Comments following the Consumer Roundtable on 10 November 2010

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]