The PCEHR Consumer Reference Group
Comments following the Meeting of 20 January 2010

Checklist of Consumer Concerns

Preliminary Draft of 25 January 2011
Iniitial Editor – Roger.Clarke@xamax.com.au – (02) 6288 6916

Introduction

NEHTA and DOHA are developing a Personally-Controlled eHealth Record (PCEHR).

A Consumer Reference Group (CRG) has been formed.

For satisfactory consultations to take place, a number of conditions need to be fulfilled. For example, the Australian Privacy Foundation has summarised the expectations that it has of organisations that it deals with, here: http://www.privacy.org.au/Papers/PS-Cons-101106.html

The PCEHR consultations are especially complex, because the record is intended as a central element within the eHealth ecology, and hence involves almost the entire sector. It will inevitably contain some data that is both important and somewhat sensitive to many people. And its purpose is to enable access to further data that is even more important and in some cases even more sensitive.

It is therefore vital that the many representative and advocacy groups involved in the consultations identify the topics that need to be satisfactorily addressed.

This document contains checklists of health consumer concerns in relation to the PCEHR project.

The purposes of these Checklists are:

- to ensure that the Agenda for the consultation process is comprehensive
- to provide a basis for evaluating progress
- to provide a basis for evaluating the outcomes once the consultation is completed

The document is provisionally divided into four sections:

1. **Process Matters**, to do with how the consultation is conducted
2. **Consumer Interests**, to do with people as patients
3. **Privacy Interests**, to do with concerns about the data in the Record, and which the Record enables access to
4, **Legislative Matters**, to record commitments made that involve statute law

The PCEHR Consultation
Checklists of Consumer Concerns

PROCESS MATTERS

Preliminary Draft of 25 January 2011
Iniitial Editor – Roger.Clarke@xamax.com.au – (02) 6288 6916

A. Information

1. Project Objectives
   a. Clarity of the Objectives
   b. Appropriateness of the Objectives
   c. Clarity about the Meaning and Scope of 'Personally-Controlled'
2. Information Provision
   a. Comprehensiveness
   b. Timeliness (in advance of each meeting, and updated at each meeting)
   c. Comprehensibility
   d. Trustworthiness
3. Parallel Activities (e.g. Clinical Reference Groups, Design Teams)
   a. Transparency
   b. CRG Interactions
4. Complementary Activities (e.g. Usability Testing, Privacy Impact Assessments)
   a. Transparency
   b. CRG Involvement

B. Personal Choice / Opt-In / Consent

1. Transparency / Clarity of Meaning
   "a record that is at all times owned and controlled by the patient"
   "control of access is key"
2. No Designed-In Disadvantage
   i.e. exercise of the choice not to opt-in must not result in denial of service, nor service disadvantages (such as lower treatment priority), nor higher costs (e.g. denial of discounts)
3. Longevity of the Personal Choice Feature:
   - Entrenchment, i.e. preclusion of renege or delayed implementation
   - Avoidance of Design Features with the propensity to enable a switch from opt-in to opt-out or to a mandatory PCEHR

C. Governance

1. Structure, including the following features:
   - a long-term Consumer Reference Group
   - direct access to the NEHTA Board
   - voices for all groups and perspectives, through a sufficiently large membership
   - requirement that the CRG represent the views of all participants, i.e. not only consensus positions but also the diversity of views must be documented and reported
2. Processes
   - Comprehensiveness
   - Sufficiently Detailed
3. Longevity, to ensure that the CRG's corporate memory is sustained

D. Commitments

1. Clarity
2. Comprehensiveness
3. Trustworthiness

The PCEHR Consultation
Checklists of Consumer Concerns

CONSUMER INTERESTS

Preliminary Draft of 25 January 2011
Iniitial Editor – Roger.Clarke@xamax.com.au – (02) 6288 6916

[Very Preliminary, due to the limitations of the Initial Editor's background]

A. Objectives and Constraints

1. The primary objective is to directly enhance individual Patient Health
2. The following objectives of the scheme are secondary:
   a. public health
   b. indirect enhancement of patient health
3. All other objectives of the scheme are tertiary, in descending order of importance:
   a. administration and accounting
   b. health care research
   c. investigations into administrative efficiency and waste
   d. insurance
   e. social research
4. The design of the scheme must reflect, above all else, the primary objective
5. Features of the design that are for the purpose of objectives other than individual patient health must not compromise patient health, nor patient health data
6. The scheme must be designed so that opting in to the PCEHR, and providing data into it, provide advantages to the patient
7. The scheme must not be designed so that not opting in disadvantages the person concerned (although disadvantages may of course be a by-product of not opting in)

B. Consumer Trust in Relation to Data Integrity

Consumers want assurances about the accuracy, precision, timeliness and relevance of data stored about them, and about maintenance of those data qualities

C. Consumer Trust in Relation to Data Access by Others

Consumer sensitivity about secondary uses of their data depends on how remote the secondary use is, and on the extent to which the data are, or may be, associated with the patient. The levels of association are as follows:

1. Availability of **identified data** for any secondary use is a serious concern, because of the risk of leakage beyond the individuals responsible for patient care; and the degree of concern increases steeply with each step down the scale of secondary and tertiary uses
2. Availability of **readily re-identifiable data** for any secondary use is nearly as serious concern as with identified data
3. Availability of **anonymised data** is of far less concern, and to far fewer consumers – provided that independent security specialists confirm that the arrangements ensure genuine anonymity and not ready re-identifiability
4. Availability of **aggregated data** is of very little concern, and to only a very small number of consumers

D. Consumer Trust in Relation to Data Access by Themselves

Consumers want full access to data about themselves (where appropriate, mediated by a professional with appropriate qualifications), and the ability to have it amended or deleted

E. Segment Analysis

There is a wide range of consumer interests, but the relevance of each of them varies considerably depending on the particular category/ies that the individual patient belongs to. Consumer interests are accordingly identified below within patient segments.

1. Patient with Chronic Condition

a. storage of a significant quantity of data, on multiple episodes and encounters, in forms compatible with the condition and suitable for the relevant categories of provider

b. accessibility by those providers, some local, some not (e.g. pathology services, specialists)

c. service / privacy trade-off mostly heavily towards service, but with exceptions

2. Patient with Complex Conditions ('Co-Morbidities')

a. storage of a significant quantity of data, on multiple conditions, episodes and encounters, in forms compatible with the conditions and suitable for the relevant categories of provider

b. accessibility by many providers, some local, some not (e.g. pathology services, specialists)

c. service / privacy trade-off very heavily towards service, but with exceptions

3. High-Dependency Aged Patient [Age is relative, but generally >75]

This segment encompasses people in medium-care and high-care, whether in residential aged care facilities or their own homes, and in closed wards

a. storage of a significant quantity of data, on multiple conditions, episodes and encounters, in forms compatible with the conditions and suitable for the relevant categories of provider, with a stronger emphasis on an Advance Care Directive

b. accessibility by many providers, some local, some not (e.g. pathology services, specialists)

c. service / privacy trade-off very heavily towards service, but with exceptions

4. Itinerant

This segment encompasses 'grey nomads', 'travelling salesmen', aboriginals living a traditional lifestyle, 'fruit-pickers', vagrants and 'street kids'

a. accessibility by any provider, anywhere, but only at the patient's request

5. Patient with Acute Condition

This segment encompasses victims who suffer injuries and illnesses such as appendicitis

a. data relevant to emergency treatment

6. The Family

This segment refers to groups of one or more persons *in loco parentis* and one or more children

a. storage of data relevant to recent episodes and encounters, in forms compatible with the conditions and suitable for the relevant categories of provider

b. accessibility by many providers, some local, some not (e.g. pathology services, specialists), but under the control of the guardian

c. ability to exercise power of attorney, and to manage each child's transition to adulthood

7. The Remote Patient (and in many cases also the Rural Patient)

a. storage of data relevant to recent episodes and encounters, in forms compatible with the conditions and suitable for the relevant categories of provider

b. accessibility by many providers, generally distant, and often with low-grade communications infrastructure

8. The Patient with a Culturally-Sensitive Condition

This segment encompasses sexually-transmitted diseases, gynaecological conditions, and mental health; conditions of especial concern within particular ethnic, lingual and religious cultures; and conditions of especial concern to particular individuals (whether rationally or otherwise) such as leprosy, diabetes, glandular fever ('the kissing disease'), etc.

a. storage of data relevant to recent episodes and encounters, in forms compatible with the conditions and suitable for the relevant categories of provider

b. very tight restriction on access, especially to providers other than those who are that patient's specialist providers in relation to that condition

9. The 'Bullet-Proof'

This segment encompasses people who see themselves as not needing the health system, and who (leaving aside acute conditions) either self-treat or don't treat at all

a. storage of no data

10. The Wary

This segment encompasses people who actively avoid exposure, particularly of their contact-points, for reasons such as personal safety of themselves or their family; and those who are generally sceptical about encounters with government agencies and/or medical professions

a. storage of a minimal amount of data

b. tight restrictions on access

c. the capability to be very specific about consents to access and denials of access

11. The Hostile

This segment encompasses people who are consciously criminal; protected witnesses; the clinically paranoid; those who are highly private particularly in relation to their bodies; victims of partner abuse (particularly those with young children); and those who are highly sceptical about encounters with government agencies and/or medical professions

a. storage of a minimal amount of data

b. very tight restrictions on access

c. the capability to be very specific about denial of consent, and about specific consents

The PCEHR Consultation
Checklists of Consumer Concerns

PRIVACY INTERESTS

Preliminary Draft of 25 January 2011
Iniitial Editor – Roger.Clarke@xamax.com.au – (02) 6288 6916

A. Architectural Features to be the Subject of Commitment

- Multiple Conformant Repositories must be supported, not a single consolidated database
- Existing repositories must remain in place and not be merged
- Access from remote locations must be mediated by a trustworthy infrastructure
- Allowance must be made for differential levels of location trustworthiness
- The personal records must not be in a single national repository, because this creates a 'honey-pot' that attracts break-ins, unauthorised secondary uses and identity thieves. The scheme must faciitate storage of the PCEHR in repositories of the individual's choice
- Clinician databases must not be precluded from being Conformant Repositories. To do so would create a strong tendency away from a 'federation of databases' model and towards a 'centralised database' model'. It is appreciated that an early implementation may need to avoid being over-ambitious. But it is 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 consents, and then becoming subject to specific and tight controls
- Pseudonyms must be supported, and links between nyms and identifying data protected
- Anonymity must be supported, such that a person need not provide identifying data

B. Personal Control Aspects to be Articulated Into Design Features

- 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. (The term 'handling' is comprehensive, including collection, recording, amendment, deletion and access)
- Great care must be taken to avoid dilution of personal control through unjustified dependence on 'implied consent'
- The record must be proof against the wide array of demand powers that exist
- Unconsented access by second and third parties must be precluded by effective security mechanisms, which are proof not only against break-ins but also non-consensual accesses through the exercise of any discretions and legal authority
- 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)

C. Enforcement Aspects to be Articulated Into Design Features

Controls must be real not nominal, and must be demonstrably effective, including the following:

- Data must be subject to security safeguards commensurate with its sensitivity, at all times, including when it is in use, in storage and in transit
- All accesses must be subject to pre-controls and post-controls, commensurate with the circumstances
- The primary basis for access is consent by the person whose data it contains
- In order to enable post-controls, all accesses must be logged

- All accesses of a sensitive nature must be monitored, and prompt action taken when exceptions are detected, e.g. access to data not relevant to the patient's treatment
- All accesses that override protections must be the subject of post-controls, in particular through notification to the individual concerned that the override has occurred
- The log must include the identifier(s) of the users who gain access
- Identifiers must be personal not generic (such as duty doctor, clinic manager, secretary)
- All staff that have access, in all organisations, must have identifiers and personal accounts
- It must be an offence for an individual to permit another person to use their identifier
- It must be an offence for an organisation to require, encourage or permit an employee, contractor or agent to permit another person to use their identifier
- There must be sanctions for breaches:
  - against organisations
  - against individuals
- There must be business processes to deal with complaints
- There must be specific commitments to perform those processes
- There must be business processes to deal with enforcement
- There must be specific commitments to apply the sanctions

Because the Health Identifiers system is run by Medicare, interactions with Medicare are essential.

D. Conduct of Privacy Impact Assessment (PIA)

PIA processes focus on specific projects within the overal PCEHR Program, and achieve a level of detail greater than is possible with large-scale consultative processes

- The PIA process in relation to the Health Identifier system must commence immediately
- PIA processes for each PCEHR-related project must commence very shortly
- Information provision and consultative processes must be inherent elements within PIA
- The CRG must have involvement in all PIAs

E. Operational Features to be Articulated Into Design Features

The many privacy-sensitive design features were in the mockup demonstration provided at the Roundtable. These must 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).

- <u>Privacy-Positive Aspects of the Demonstration</u> included:
  - The Organisational Access Levels feature, comprising:
    No Access; Standard Access; Standard and Sealed Access; Emergency (Standard and Sealed), with post-notification of access; Locked
- <u>Privacy-Negatiive Aspects of the Demonstration</u> included:
  - Treatment locations could 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
    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
  - "There's no commitment to monitoring of logs. It's up to the consumer".
    The following design features must be included:
    - 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]
    - Data Breach Notification procedures, where unauthorised access occurs

The PCEHR Consultation
Checklists of Consumer Concerns

LEGISLATIVE MATTERS

Preliminary Draft of 25 January 2011
Iniitial Editor – Roger.Clarke@xamax.com.au – (02) 6288 6916

Commitments that are made that need to be expressed in, or supported by, features of the legislation.

The commitments must be progressively documented.

A. Entrenchment of the Commitments

1. Legislation
   i.e. all Key Commitments must be expressed in legislation
2. Highest Standard, not Lowest Common Denominator
   i.e. the principles must not be contaminated by political deals among powerful groups
3. Nationally Consistent Legislation
   i.e. much effort must be invested in achieving commonality across jurisdictions
   To cater for States or Territories retaining their existing privacy laws as they affect the health care sector, a set of principles must be established that reflects the privacy-relevant undertakings given in relation to the system, which all States and Territories agree to ensure are implemented in their laws

B. Specific Aspects of the Legislation

1. New (or possibly heavily amended) laws are essential, because current privacy laws are too heavily qualified, and cannot be relied upon
2. New eHealth-specific privacy laws must be passed and implemented prior to the commencement of PCEHR operations
3. Consumer and privacy protections must be specific, not general and vague
4. Consumer and privacy protections must be entrenched
5. Consumer and privacy protections must not be dependent on subsidiary legislation (such as Regulations) or on deferred legislation
6. Clear legal obligations must apply to:
   a. organisational providers
   b. individual providers
7. Sanctions must apply to breaches of legal obligations
8. Powerful and health-specific regulation is essential, because the scope, powers, processes and resources of existing regulators are completely inadequate to the task
9. The regulator must have powers to investigate, enforce and impose sanctions
10. The regulator must have responsibilities to investigate, enforce and impose sanctions
11. The regulator must be assured of sufficient resources