The Personally Controlled eHealth Record (PCEHR)

Checklist of Privacy Concerns

Discussion Draft of 15 February 2011

Status of This Document

This is a discussion draft. It was prepared by the Australian Privacy Foundation. It was given preliminary review by a number of the participants in the first two Consumer Reference Forum meetings that were run by NEHTA in early 2011.

The intention is that the Checklist be considered by all relevant health consumer advocacy organisations, and amended and enhanced to reflect the interests and concerns of all of the many and diverse categories of health care consumer.

Introduction

A project to define and implement a Personally-Controlled eHealth Record (PCEHR) is being conducted by NEHTA and DOHA. The project has been under way for several years, consultative processes with clinicians have been in place since the formation of a NEHTA Stakeholder Reference Forum in early 2009, and major design decisions are scheduled for March 2011.

Until the end of 2010, however, the consumer voice was largely excluded from the process. Very belatedly, in January 2011, NEHTA established a Consumer Reference Forum (CRF). The governance and process aspects of the CRF are yet to be finalised.

The PCEHR is intended as a central element within the eHealth ecology, and hence involves almost the entire sector. It will contain data that is important to many people, and that is somewhat sensitive to some of them. Part of the Record's 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 representative and advocacy groups identify the requirements that need to be embedded in the design.

This document contains a Checklist of privacy concerns in relation to the PCEHR project.

Privacy is not the primary factor that needs to guide the design and implementation of the PCEHR. It is, however, a vital element in achieving consumer trust in the scheme, and this document is designed to be read in conjunction with separate Checklists of consumers' aspirations and concerns.

The purposes of the Checklist 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

The Personally Controlled eHealth Record (PCEHR)

Checklist of Privacy Concerns

Discussion Draft of 15 February 2011

1. Personal Control

Personal control is intrinsic to trust, and it needs to be established and sustained.

- Personal control needs to apply to:
  - creation, amendment and deletion of data in the Record
  - access by any person or organisation to the Record as a whole and to any item in it
- Personal control needs to exist irrespective of the possession or custodianship of the record
- Personal control needs to extend to copies of the data that are extracted from the record
- All handling of data in the record needs to be the subject of consent. The term 'handling' is comprehensive, including collection, recording, amendment, deletion and access
- Personal control should not be diluted through unjustified dependence on 'implied consent'

2. Access Controls

Security safeguards need to apply to all organisations and all contexts, without exceptions. The safeguards must not inhibit accesses consented to or requested by the consumer.

- Security safeguards are essential against:
  - inappropriate use by users who have legitimate access to the record
  - unconsented access by second and third parties
- Patient data needs to 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 need to be subject to pre-controls and post-controls, with the nature of the controls commensurate with the circumstances
- The primary basis for access is consent by the person whose data it contains
- An access to the PCEHR is authorised only if both the organisation and the individual have consent, and the particular data accessed is relevant to the purpose of the access
- Access to the record needs to be proof against the wide array of demand powers that exist
- Every access that is not based on consent or that overrides safeguards needs to be the subject of post-controls, in particular through notification to the individual concerned that the access has occurred
- All accesses need to be logged, in order to enable post-controls
- Logs need to include the identifier of the account through which access is gained
- All individuals who have access need to have identifiers and personal accounts
- Generic accounts (such as duty doctor, clinic manager, secretary) must not be permitted
- If, by exception, a generic account is permitted (e.g. in Emergency Departments), strong complementary controls need to be in place (e.g. per-shift passwords)
- Logs need to be accessible long-term, including by the person to whom the Record relates
- Logs need to be subject to security safeguards similar to those applying to the Record

3. Enforcement

Controls need to be credible, and subject to a comprehensive enforcement regime.

- The following acts need to be legislated as **offences**:
  - an individual or organisation that has consent to access a Record accesses it for a purpose other than a purpose encompassed by the consent (unauthorised use)
  - an individual or organisation accesses a Record without consent or other authority (commonly referred to as unauthorised disclosure)
  - an individual or organisation permits another person to use their account
  - an organisation requires, encourages or permits an individual who performs a function on behalf of that organisation to permit another person to use their account
  - an individual or organisation knowingly facilitates an offence by another person
- There need to be **sanctions for offences**:
  - against organisations
  - against individuals
- There need to be **investigative processes**, including:
  - automated monitoring of logs to detect breaches and anomalies
  - action arising from breaches and anomalies
  - Data Breach Notification procedures, where unauthorised disclosure occurs
- There need to be accessible and effective **enforcement mechanisms**, through:
  - clear and comprehensive allocation of responsibilities
  - business processes to deal with complaints
  - specific commitments to perform those processes
  - resources and budgets sufficient to perform those processes
  - business processes to deal with enforcement
  - specific commitments to apply the sanctions
  - resources and budgets sufficient to perform the processes and apply sanctions

4. Extraneous Uses of Personal Data

The primary aim of the PCEHR needs to be the healthcare of individual patients who choose to participate in the scheme. All other uses are extraneous. The following are secondary:

a. public health
b. indirect enhancement of patient health
c. health-related research

The following are tertiary:

d. administration and accounting
e. investigations into administrative efficiency and waste

The scheme must avoid pollution by other extraneous uses, such as:

f. insurance
g. more general social research only loosely related to health care

Features of the design that serve objectives other than individual patient health need to be implemented so as to avoid compromising patient health, and avoid compromising patient health data.

The degree of consumer concern about extraneous uses of their data depends on how remote the extraneous use is, and on the extent to which the data are, or may be, associated with the patient. The levels of association of data with a consumer are as follows:

- **Identified Data**. Any extraneous use is of 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
- **Readily Re-Identifiable Data**. Any extraneous use of such data is of nearly as serious concern as with Identified Data
- **Anonymised Data**. Extraneous use is of far less concern, and to fewer consumers – provided that independent security specialists confirm that the arrangements ensure genuine anonymity and not ready re-identifiability
- **Aggregated Data**. Extraneous use is of little concern, and to very few consumers

5. Privacy Impact Assessment (PIA)

Privacy Impact Assessment (PIA) is a process that focuses on specific projects within the overall PCEHR Program. It achieves a level of detail greater than is possible with large-scale consultative processes that consider the entire Program.

- Immediate commencement of the PIA process in relation to the Health Identifier system
- Very early commencement of the PIA process for each project as soon as it is launched
- Information provision and consultative processes as inherent elements within all PIAs
- Involvement in all PIAs by all health care consumer and privacy advocacy organisations

6. Architectural Features

Privacy-protective features need to be entrenched in the scheme, rather than tacked on at the end. For that to happen, the scheme's architecture, i.e. its elements and how the elements inter-relate, need to ensure that the scheme is practical, scalable and trustworthy.

- PCEHRs need to be able to be stored in a variety of locations, at the individual's choice, not just in a single national repository. A single repository creates what is referred to as a 'honey-pot' – a single location that contains obviously valuable data, and that therefore attracts break-ins, unauthorised secondary uses and identity thieves
- Health care data needs to be placed in, and remain in, a repository under the control of the relevant provider, with copies of the data being provided to others when the patient consents, and then becoming subject to specific and tight controls
- In relation to the repositories that the PCEHR points to:
  - Multiple repositories need to be supported, not a single consolidated database. If providers' databases were to be excluded from the scheme then it would not be a 'federation of databases' but rather a 'centralised database' model, which is deficient because of both scalability and trust problems
  - Existing repositories need to remain in place and not be merged
  - Access from remote locations need to be mediated by a trustworthy infrastructure
  - Allowance needs to be made for differential levels of location trustworthiness
- Multiple PCEHRs per patient need to be supported, as an additional data security feature
- Pseudonyms need to be supported, and links between nyms and identifying data protected
- Anonymity needs to be supported, such that a person need not provide identifying data

7. No Disadvantage

A consumer's choices must not give rise to compromises to the person's interests, such as service denial, service reduction or cost penalties, except to the extent that those compromises are inherent in or a by-product of the choice. In particular, the scheme needs to avoid design features that actively disadvantage such consumers.

Where a consumer's choice gives rise to inherent compromise to their interests, reasonable steps need to be taken to inform them, but not in such a manner as to represent undue pressure to conform.

Key aspects of consumer choice that must not give rise to unjustifiable disadvantages are:

- choice not to have a PCEHR
- choice to have more than one PCEHR
- choice to associate a PCEHR with a pseudonym
- refusal to consent to access to a PCEHR by a healthcare provider or other party