Health Care Consumers Association of the ACT INC
100 Maitland Street, Hackett ACT 2602
Phone: 02 6230 7800
Fax: 02 6230 7833
Email: adminofficer@hcca.org.au
ABN: 59698548902

HCCA Submission on "Mandatory data breach notification in the eHealth record system"

September 2012

Contact: Darlene Cox
Executive Director
darlenecox@hcca.org.au
(02) 6230 7800

HCCA Submission on "Mandatory data breach notification in the eHealth record system"

HCCA welcomes the opportunity to comment on the Office of the Australian Information Commissioner's (OAIC) *Mandatory data breach notification under the personally controlled electronic health record system* consultation paper.

Background

The Health Care Consumers' Association (HCCA) was formed over 30 years ago to provide a voice for consumers on local health issues and now provides opportunities for healthcare consumers in the ACT to participate in all levels of health service planning, policy development and decision-making.

In 2009, HCCA established an *eHealth Consumer Reference Group (EHCRG)* in response to strong interest from consumers and their desire to be at the centre of the decision and policy-making processes. Membership has increased steadily and the *EHCRG* now comprises some 20 individuals, including senior ACT Health Directorate staff. The *EHCRG* has provided an excellent forum for HCCA and ACT Health Directorate to develop a solid, collaborative relationship, through a shared interest in, and commitment to, eHealth. The comments in this submission reflect the views of the consumer members of the *EHCRG*.

General Comments

In general terms, we believe the concept of the OAIC guidelines is a vital component to engender consumers' confidence in the Personally Controlled Electronic Health Record System (PCEHR). It is imperative that the key issues of privacy, access, security and governance are properly addressed in order to ensure the delivery of a robust data breach notification system.

However, we are concerned that the language used in the guidelines is too bureaucratic and is not structured in a sufficiently clear manner for its target audience, namely, consumers, GPs and pharmacists.

We are also concerned that the heavy emphasis on penalties and individual fines will discourage GPs and pharmacists from embracing the concept of the PCEHR in its early stages of implementation.

In terms of data breach notification, there are two areas of particular concern to consumers, which we believe should be specifically covered in the guidelines. Both relate to consumers rights to communication, participation and privacy under the Australian Healthcare Rights:

- Firstly, how will consumers know when their confidentiality has been breached, and what is the procedure for notifying them about breaches in confidentiality relating to their records? and
- Secondly, and in relation to the first question, if records are (accidentally) sent to the wrong clinician, is that clinician obliged to formally report the incident and will the consumer also be advised of the breach?

The following paragraphs contain more detailed comments on specific areas of the guide.

OAIC

HCCA encourages the OAIC to address the strategic functions of information management in the OAIC charter as it applies to the PCEHR legislation.

The legislation defines the ***PCEHR system*** as a system:

(a) that is for:

(i) the collection, use and disclosure of information from many sources using telecommunications services and by other means, and the holding of that information, in accordance with consumers' wishes or in circumstances specified in this Act; and

(ii) the assembly of that information using telecommunications services and by other means so far as it is relevant to a particular consumer, so that it can be made available, in accordance with the consumer's wishes or in circumstances specified in this Act, to facilitate the

provision of healthcare to the consumer or for purposes specified in this Act; and

(b) that involves the performance of functions under this Act by the System Operator.

We expect the guide to address the protection and availability of data in the PCEHR system in accordance with this definition. While the guide provides examples of disclosure or "privacy breaches", it is not clear that beaches could be result of events that compromise the integrity of the PCEHR, for example:

- data corruption such as information that is included in a person's record that should have been in another person's record.
- data that is collected for use in the PCEHR and not transmitted to the PCEHR and hence not in the "PCEHR" index;
- a repository provider preventing a healthcare organisation from access to data; and
- information that is deleted from an individual's record or group of records or rendered inaccessible by the PCEHR system.

The guide needs to address a lack of information or other omissions that may compromise the security and integrity of the system. HCCA also suggests that costs, administrative burden and process time required to identify and manage breaches are covered in the guide.

Guide

The background to the discussion paper needs to recognise that the PCEHR includes information provided by consumers and entities other than health care providers. All data in the PCEHR system needs to be protected.

Role of the system operator

The role of the system operator needs to be clarified. Current legislation requires the system operator to notify all affected consumers in the event of a breach and, if a significant number of consumers are affected, notify the general public.

Notifying consumers about notifiable data breaches

We interpret the legislation as *mandating* public disclosure if a significant number of consumers are affected. Instead, the guide states that the system operator "may" …. and also lists additional "criteria" before the system operator "may" decide to notify the public. The Guide needs to encourage the system operator to provide full and open disclosure of all information relating to the breach. It could also list specific information requiring mandatory disclosure.

Mandatory information would include:

- the notification date the breach was notified to the System Operator and OAIC
- the date the individual consumers and representatives were advised
- the date the public were advised
- content disclosed and number of consumers affected
- the period over which the breach occurred—start and end dates
- entities involved and their role
- entities that have not disclosed a breach but may have similar processes and risks.
- duration of the unauthorised access or breach—start and end dates
- the number of people who had unauthorised access needs to be disclosed and over what period
- steps taken to contain the breach, any risk evaluation and actions taken (or proposed) to prevent recurrence
- date of additional advice can be expected
- contact person for additional information.

Health information plays a significant role in the health, wellbeing and care of individuals. As such, it would be good for the OIAC to recommend that the advice include information about organisations that can provide assistance or support that is available to distressed people.

In addition, there needs to be clear account of action taken by the OIAC and any further process individuals can take including appeals processes. It is important that these processes are neither costly nor administratively onerous for consumers to pursue.

Ideally, there would be a public register of all breaches so that consumers could access breaches that have affected their data. Consumers need to have an easy way of identifying when their data was compromised and by whom. Alternatively there could be part of the PCEHR which captures this information into the record.

Investigating possible notifiable data breaches

HCCA does not agree with OAIC's administrative decision not to deal with a complaint occurring more than 12 months after the initial breach. Often, the details of the breach are not fully disclosed until a long time after the event. In addition, consequences of a breach may not be apparent when the individual is first advised of the breach. Setting an arbitrary time limit is not useful.

Transparency and Audits

The guide does not provide any advice with regard to audit trails and accessibility for consumers. This will be key when handling breaches. Audit trails should be available online and provide the identity of the person accessing the data and not require significant administrative effort by consumers to determine who accessed their record and why.

For instance, if an entire jurisdiction (e.g. the NSW Government) is treated as the organisation identified in the audit trail then this renders the audit trail meaningless, because hundreds of thousands of people could have accessed the information. As a result, the consumer would need to apply to the NSW Government to determine who accessed the data; they might then be directed to a particular administrative region, which might lead the consumer to a hospital, then a hospital department and finally to an unnamed individual.

Additions to the Guide:

We recommend the following issues be covered in the Guide:

1. Divided responsibilities of the OAIC and state counterparts might result in "buck-passing". The PCEHR is a national initiative and hence a single issue could have implications across federal and, one or more, state jurisdictions.

Consumers believe all requests should be passed through a single entity to coordinate responses.

2. The OAIC needs to promote disclosure of consumer rights and options and address administrative obstacles in order to facilitate compliance with the legislation. The guide could also address issues regarding “informed consent” and the need for the System Operator to advise consumers of their options. The “default access controls” set by the system operator (paragraph 61. b.ii of the legislation) in the current implementation would undermine the effectiveness of the “personal control” and the privacy mechanisms for the PCEHR.
3. It is important to ensure that basic or default controls allow consumers to exercise their rights.
4. We believe the OAIC should to provide a public register of all breaches and capture reports to state government entities.

In conclusion, we reiterate the importance of:

- operational transparency and accountability;
- the pivotal role of the PCEHR in improving patient safety and quality in healthcare, backed by a rigorously enforced data protection system; and
- active consumer participation in the governance and ownership of the PCEHR system.

The Health Care Consumers' Association of the ACT would be happy to discuss the points raised in its submission further should the opportunity arise.

HCCA

25 September 2012