Australian Privacy Foundation

enquiries@privacy.org.au

http://www.privacy.org.au/

28 September 2012

APF submission – draft Mandatory data breach notification in the eHealth record system guide.

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. I write as Chair of the Health Sub Committee of the APF.

The APF is glad of this opportunity to influence the vital "Mandatory data breach notification in the eHealth record system" draft guide, September 2012. We are keen to support the development of a national eHealth data breach notification platform to support community trust in a secure and privacy-enhancing Personally Controlled Electronic Health Record (PCEHR) system.

The APF policy document "Protections Against eHealth Data Breaches" responds to stimulus questions asked in the "Mandatory data breach notification in the eHealth record system consultation paper", 28 August 2009.[1] The APF document establishes the standard individuals expect the Australian government to implement and anything less is considered unacceptable. The document is appended to this submission and provides a response to stimulus questions about reporting and notification obligations as well as other key matters.

FEEDBACK ABOUT OTHER MATTERS RESPONDING TO STIMULUS QUESTIONS.

Notifiable data breaches

As the APF policy document suggests, a notifiable data breach arises simply where any person in an organisation becomes aware that unauthorised collection, use or disclosure of health information has, or probably has, occurred.

The APF opposes any definition of a notifiable breach that has a narrower scope than our policy statement.

Language and Format

The language and format are not transparent and are confusing in places. The term “eHealth record system” is not applied consistently throughout the document. Does the expression “eHealth record system” refer to the PCEHR system or a providers own system? For instance, on pages 3 and 4, “Data breaches that are out of scope”, we are confused by what appears to be inconsistent application of the same term. On the one hand, the section refers to eHealth systems that are not connected to the national system in the first paragraph and example box. On the other hand, in the final paragraph the section refers to private healthcare provider eHealth systems, whether the system feeds into the national system or not.

The APF requests clarification of the term “eHealth record system” in the draft guide. We also request clarification of whether private healthcare provider eHealth systems that feed into the national system are subject to mandatory data breach notification legislation and guidelines.

The APF welcomes the outline of the “Role of the System Operator” (SO) section, on page 6, although this is not sufficiently detailed. For example, it requires the SO to notify affected individuals and the general public of breaches affecting a significant number of people. There is no definition or example provided of how many records may be breached before this is considered “significant”. Neither is there any explanation of the methods or mechanisms the SO should use to notify affected individuals and the general public of breaches. Moreover, the section refers to reporting these and other breaches to the Office of the Australian Information Commissioner (OAIC). However the eHealth record system OAIC Enforcement Guidelines consultation paper, August 2012, clearly states the OAIC may choose not to act on proven breaches and not to publish information about said breaches. These guidelines indicate the role of the SO in the draft under discussion is irrelevant to consumers concerns about rectifying breaches of records held in the PCEHR system.

The APF asks for the terms “significant” and “notify” to be defined in practical terms. We also express concern the draft mandatory breach guide is not relevant to the real life concerns of patients affected by threats to the privacy and security of their health information.

The “When to report a notifiable data breach” section, page 7, suggests entities are not required to notify the OAIC of data breaches immediately if this is not practicable or at the expense of initial efforts to constrain it. We question why notification and efforts to constrain data breach cannot occur simultaneously.

Participating consumers will rely on the integrity of information stored on the PCEHR system for their healthcare outcomes. It is vital that any matter affecting an individual health record is immediately reported to the consumers concerned and to the SO so that action can be taken to ensure consumers do not suffer from adverse health errors as a consequence of such breaches, whether these are accidental or deliberate.[2-3]

The APF is receiving a rapid increase in contact from chronically ill patients where an eHealth record, including some on the PCEHR system, is inaccurate due to poor security mechanisms. In real life, these patients have been lucid and able to negotiate the matter with clinicians convinced the e-record

is a more reliable source of information about medical procedures than the individual concerned. Less lucid patients may not be similarly fortunate, risking adverse error as a consequence

The APF requests notifiable health breaches are immediately reported to affected consumers, the PCEHR system authorities and the OAIC to protect the health and wellbeing of individuals whose records may have been compromised.

The section "Responding to a notifiable data breach", pages 12 to 19, offers useful steps for providers to follow while reflecting on a data breach or when establishing an eHealth system in the first instance. However, these are not sufficiently robust to protect individuals from the results of system breach, neither are consumers seen as pivotal in this process. For example, providers are asked to "assess whether steps may be taken to mitigate the harm a consumer may suffer as the result of a breach" (p.12). The welfare of the consumer should be the key priority of this section and rather than seem an afterthought to controlling machine or operator error or misuse.

Indeed the section is replete with references to "suitable" individuals, determining whether there is a need to assemble a team to investigate a breach or not, inform others and "escalate matters internally as appropriate". The section asks providers to be careful "not to destroy evidence" that may help law enforcement agencies determine cause or take corrective action. How will providers be equipped to understand what is and is not evidence in this context? The section is vague, unhelpful and far too general.

At no stage is the health and wellbeing of the affected individual or individuals given primacy here with the exception of Section (d), page 16, where the provider, not the SOS or the OAIC, is asked to make a determination of risk to affected individuals. How will the provider be trained to make these determinations? Moreover, Step 3 on page 17, states that only the SO can notify affected consumers about notifiable data breach. The OAIC role is not specified. This is terribly confusing and overly bureaucratic for both practitioners and consumers.

Regardless of nomenclature, the draft breach guide indicates the PCEHR is not personally controlled but SO controlled. The APF wonders whether providers are able to notify consumers of breaches to the PCEHR systems that are not deemed notifiable under the draft guideline. The notification processes outlined in the draft are vague, empower neither consumer nor practitioner and are unnecessarily bureaucratic to the cost of patient health outcomes and empowering clinicians to maintain secure eHealth networks. The guide reads as if directed to administrative staff working for the Australian government and managing abstract issues rather than consumers and clinicians in real life.

The APF maintains that the guidelines do not reflect the seriousness of data breach to consumer health and wellbeing. Neither do these provide adequate emphasis on the consumer's human right to access or know information about their own health record, an ostensible feature of the PCEHR system that now seems countered by the breach guidelines.[4] The draft guideline is abstract and emphasises administrative processes that disempower patients and clinicians alike.[4] The guide is not transparent or useful in relation to mandatory notification of breaches in the eHealth record system.

The mandatory breach guidelines "must build defences against harm, including safety processes, system redundancies and training, to minimise unsafe use or the creation of unsafe settings".[2] The draft does not accomplish this aim.

The APF believes that failure to rectify these matters will undermine community confidence in the utility of the PCEHR system, fostering project failure, as has already occurred with similar implementations in other countries.[3]

Finally the Privacy Act and legislative amendments supporting the PCEHR system simply set a minimum reporting requirement for breaches. The APF requests that action is taken according to our policy document (appended) so that the Australian government does not replicate the errors made by other nations implementing similar projects[1,3]. Our national policies and procedures must be set at a level that actually achieves the aims of protection of sensitive data and transparency in relation to breaches. In this context, the "Mandatory data breach notification in the eHealth record system" draft guide September 2012 sets the minimum far too low to be acceptable.

Yours sincerely

Dr. Juanita Fernando

Chair, Health Sub Committee

Australian Privacy Foundation

Dr Fernando is in Medicine, Nursing & Health Sciences, Monash University 03 9905 8537 or 0408 131 535

mailto:Juanita.Fernando@monash.edu

Dr Fernando's son is a project leader with Accenture, which is the lead contractor on the PCEHR implementation.

Dr Fernando is a former councillor of the Australasian College of Health Informatics.

http://www.achi.org.au/

Contact Details for the APF and its Board Members are at: http://www.privacy.org.au/About/Contacts.html

REFERENCES

1. Australian Privacy Foundation (2009) eHealthcare Data Breach Policy Statement, August 28. http://www.privacy.org.au/Papers/eHealth-DataBreach-090828.pdf
2. Coeira, E. Kidd,M. & Haikerwal, M. (2012) A call for national e-health clinical safety governance. MJA 196 (7) · 16 April 2012
3. Moynihan, R. (2012) e-Health records: be aware of assumed benefit. MJA 197(6) 17 September 2012
4. Hilvert, J. (2012) Doctors could reject e-health records. Itnews.com, September 20 2012. http://www.itnews.com.au/News/316321,doctors-could-reject-e-health-records.aspx

Australian Privacy Foundation

Policy Position

Protections Against eHealth Data Breaches

28 August 2009

http://www.privacy.org.au/Papers/eHealth-DataBreach-090828.pdf

Personal health data is by its nature highly sensitive, so unauthorised access and disclosure is of even greater concern than it is with other categories of data. Irrespective of what laws and norms might apply to data breaches generally, it is vital that clear and effective protections exist for personal health care data. The APF has accordingly adopted the following policy on the matter.

A **data breach** occurs when personal health care data is exposed to an unauthorised person, and there is a reasonable likelihood of actual or perceived harm to an interest of the person to whom the data relates.

1. **An organisation that handles personal health care data must**:

   (a) take such steps to prevent, detect and enable the investigation of data breaches as are commensurate with the circumstances

   (b) conduct staff training with regard to security, privacy and e-health

   (c) subject health care data systems to a programme of audits of security measures

   (d) when health care data systems are in the process of being created, and when such systems are being materially changed, conduct a Privacy Impact Assessment (PIA), in order to ensure that appropriate data protections are designed into the systems, and to demonstrate publicly that this is the case

2. **Where gounds exist for suspecting that a data breach may have occurred, the organisation responsible must**:

   (a) investigate

   (b) if a data breach is found to have occurred, take the further steps detailed below

   (c) document the outcomes

   (d) publish information about the outcomes, at an appropriate level of detail

3. **Where a data breach has occurred, the organisation responsible must**:

   (a) promptly advise affected individuals (and/or their next of kin or carers)

   (b) provide an explanation and apology to affected individuals

   (c) where material harm has occurred, provide appropriate restitution

   (d) publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information

   (e) advise the Office of the Federal Privacy Commissioner

4. **Where a serious data breach has occurred, the Office of the Federal Privacy Commissioner must**:

   (a) review the outcomes of any investigation undertaken by the responsible organisation

   (b) where any doubt exists about the quality, conduct its own independent investigation

   (c) publish the results of the review and/or investigation

   (d) add the details of the data breach to a publicly available register, including any decision made as the result of the investigation, in order to ensure that information is available to support informed public debate about protections for personal health care data

5. **Where a data breach occurs that results in material harm**, the affected individuals must have recourse to remedies, both under the Privacy Act and through a statutory cause of action