Australian Privacy Foundation

enquiries@privacy.org.au

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

24 September 2012

APF submission - eHealth record system OAIC Enforcement Guidelines.

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 and refer to the eHealth record system OAIC Enforcement Guidelines consultation paper, August 2012. The APF welcomes this opportunity to influence the important eHealth record system Office of the Australian Information Commissioner (OAIC) Enforcement Guidelines instrument.

The eHealth record system OAIC Enforcement Guidelines instrument can provide a useful way to support community confidence in the Personally Controlled Electronic Health Record (PCEHR) system. It outlines several sensible and appropriate matters for OAIC intervention. However the instrument is **fatally** flawed as currently drafted. It proposes a set of guidelines, **not regulations**, allowing the OAIC, headed by the Privacy Commissioner/Information Commissioner (IC), to decide whether to

1. follow up complaints about a breach or not
2. publish information about proven breaches, and
3. decide the nature of compensation to affected people suffering a proven breach

The instrument provides no direction or accountability for the OAIC in regard to a PCEHR system enforcement function. There is scope for the IC to choose **not** to act on proven breaches in the guidelines and **not** to publish information about said breaches. The IC can also decide the nature of appropriate restitution, if any at all, without "hearing" the complainant.

Over recent years, the APF has begun to receive experiential feedback from clinicians and other Australians complaining about the utility of the OAIC in the context of health information privacy and security. The High Court has agreed to hear one of these complaints so far, the Supreme Court is hearing another and more are in the offing. This fact is supported by data showing the OAIC has not responded in a timely fashion to many community complaints, declined to consider a large number of complaints and was not in effect appellable. The current Commissioner has made a single s52 determination under the Privacy Act (1988) during his time in office, and the previous Commissioner did not make one single determination during five years in office. In the twenty-three year history of the Privacy Act (1988), successive Commissioners have made a mere nine determinations, four of which were sub-determinations of a single issue, so an actual total of six determinations.[1.] The Commissioners also failed to use "name and shame" options or to create any realistic "reputation risk" for those entities engaged in controversial potential breaches of privacy expectations. [2.]

The APF does not agree with the Commissioner's proposed approach to eHealth record system enforcement. The OAIC's draft Enforcement Guidelines set out the Commissioner's proposed approach in a clear but unhelpful manner. It informs the community that the OAIC's approach to PCEHR system security is founded on complex, opaque, and potentially discretionary information security and privacy rules and risk assessments. The Office has consistently failed to embark on responses to address problems at a systematic level. Rather the OAIC (formerly the Office of the Privacy Commissioner) has restricted considerations to the individual case, and that effectively in secret. The role outlined for them in the eHealth record system OAIC Enforcement Guidelines instrument would not be effective against systemic risk mitigation design flaws. The community cannot rely upon or trust measures outlined in the instrument for PCEHR system participants.

The APF is keen to see our national eHealth developments support community trust in a secure and privacy-enhanced PCEHR system. But mixed messages due to government confidentiality concerns that exclude large sections of the community from sharing in relevant information and an ostensible lack of respect for patients and their human rights permeate PCEHR system arrangements. The Guidelines instrument, as presently drafted, erodes community trust in the national eHealth system further.

For example, a recent publication quotes Dr Steve Hambleton, President of the Australian Medical Association, as saying to a consumer who did not want to share their health information with clinicians over the PCEHR system, "… you need to opt out and get out of the way … we just want the rabid consumerists to get out of the way and let's just get on with it".[3.] Another section of the publication refers to PCEHR-linked incidents, "… which can best be described as patient misadventure near misses".[4.] In the same publication, Mr Timothy Pilgrim, the IC, comments on the theoretical OAIC investigative powers over the PCEHR system. Mr Pilgrim said, "… consumers should ensure they understand how their personal and health information will be collected, used and disclosed". He continued, "… you can decide which healthcare providers can see your record and what information they can access".[5]

Mixed messages permeate this publication. In a single issue of it the community is firstly advised that some clinicians want people to get out of the way while the PCEHR system evolves in a living laboratory regardless of adverse patient care outcomes. Secondly they are told that new patient care errors are emerging from inconsistent implementations of the PCEHR system. Finally, they are advised to trust in new, optional, OAIC enforcement powers should the PCEHR system fail to protect the privacy and security of their health information, potentially triggering adverse care outcomes. The mixed messages are not confined to this single publication. Rather, the publication reflects a confusing range of messages the community currently receives from the Department of Health and Ageing (DoHA) and the National E-Health Transition Authority (NEHTA) websites, social media, newspapers, submissions and other publications.

As another example, the Australian newspaper recently published an article claiming that a week before national implementation, the PCEHR system contained more than sixty high-severity and critical bugs and several defects remained in place when the system was actually implemented. This report has been denied by the national Health Minister[4] Moreover, the national security system foundation, the National Authentication Service for Health (NASH), is not available for application to the PCEHR system so an interim, a logically less robust system (given the amount of government funding used to devise the NASH service), is currently in real-life use.[6.] The link between system security and patient care health outcomes has been well established.[7] A community looking to improve their health and wellbeing is properly advised to follow Mr Pilgrim's advice about understanding the PCEHR system in practice although no systemic or transparent platforms to accomplish this end presently exist.

It may tempt some to maintain that social control of information in the public domain is a solution to the points made herein. However community trust can only develop when PCEHR system governance is transparent and simple. Spokespersons and health authorities must not propagandise the supposed penalties of breaching records stored in the PCEHR system and embodied in OAIC guidelines without evidence. No such Australian evidence currently exists nor will this exist in the foreseeable future regardless of the draft eHealth record system OAIC Enforcement Guide. They should also support community tools to help the people appraise PCEHR system risk in the context of their own health records. This is not occurring, hence community confusion about whether PCEHR system security, and so their privacy and care outcomes, are reliable or not.

The APF maintain the OAIC's draft Enforcement Guidelines can be improved if the AOIC is accountable to the community. The IC **must** be directed to investigate complaints of information breach and report within a specific timeframe. An example of a "small breach" should be provided in the instrument. Grounds for appeal against decisions made by the OAIC must be detailed and published. The basis for the OAIC to decide not to investigate a complaint must also be published in the public domain.

The APF further believes that government health authorities and organisations are well serviced by lawyers, medical indemnity insurers, professional associations and suitably qualified experts. Most members of the community protecting their human right to privacy are not similarly advised or protected. Community organisations should be included in bodies that have complete oversight of the PCEHR system and OAIC Enforcement Guidelines. If a matter is referred to court, we ask that the obligations on the person who is the complainant are specified. Will people or health services complaining about an alleged breach be required to employ lawyers, meet costs and be involved in stressful legal processes, as with the High Court and Supreme Court examples provided above? Finally, the APF asks that the level of proof required before action through the OAIC can be taken is detailed to the community.

In summation, the APF is concerned the eHealth record system OAIC Enforcement Guidelines instrument is a Monopoly-like (the board game) "get out of jail free card" for all Australian health professionals working on the PCEHR system. Community and organisational trust in the PCEHR system cannot flourish as the draft Guidelines instrument currently stands and so system architects will not be able to maximise related health outcome metrics and other social benefits, mooted foundations of the national eHealth system.

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. AustLii. Federal Privacy Commissioner of Australia Complaint Determinations. Last updated: 9 September 2012: http://www.austlii.edu.au/au/cases/cth/PrivCmrACD/
2. Connolly, C and Vaile, D. Communications privacy complaints: in search of the right path, Cyberspace Law and Policy Centre at UNSW, with support of ACCAN, September 2010 http://cyberlawcentre.org/privacy/ACCAN_Complaints_Report/report.pdf
3. PulseITMagazine.com.au. "Mechanics of PCEHR are driving us mad": AMA.. Pulse IT; 20 August 2012: pp. 24-25
4. McDonald, K. Messaging quality is critically important, Pulse IT, PulseITMagazine.com.au.; 20 August 2012: pp.14-15
5. PulseITMagazine.com.au. Privacy Commissioner reveals investigative powers over PCEHR. Pulse IT; 20 August 2012: p.29
6. Foo, F. Document proves defects in e-health. IT Section, The Australian: 4 September 2012. http://www.theaustralian.com.au/australian-it/government/document-proves-defects-in-e-health/story-fn4htb9o-1226464247152
7. Fernando, J. The Emperor's new clothes: PCEHR system security. Annual AusCERT Information Security Conference 2012 - Security on the Move. Gold Coast, Australia; http://conference.auscert.org.au/conf2012/ http://www.privacy.org.au/Papers/AusCERT-PCEHR-120518.pdf
8. Medicare. eHealth Record PKI Certificate, Public Key Infrastructure. Department of Human Services, Australian Government http://www.medicareaustralia.gov.au/provider/vendors/pki/index.jsp#N100A5