



**Australian
Privacy
Foundation**

enquiries@privacy.org.au

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

APF feedback about the exposure draft PCEHR Bill 2011 (PCEHR Draft Bill) and exposure draft PCEHR (Consequential Amendments) Bill 2011

October 27 2011

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. Our response to your request for community feedback on the “Exposure Draft PCEHR Bill 2011 (PCEHR Draft Bill) and exposure draft PCEHR (Consequential Amendments) Bill 2011” is detailed below.

The APF submission does not explicitly respond to all concerns as these have been addressed in several previous PCEHR draft system submissions and in our policy documents (1-5). The policy documents are attached for your information. Therefore the focus of this submission is simply to add new analysis of key privacy issues from the individual citizen’s perspective.

We reiterate our position that it is completely unacceptable for any critical privacy protections to be in delegated legislation.

All protections must be in statutes, in order to ensure that they have been considered and directly expressed by the Parliament. Delegating them to statutory instruments makes them appear unimportant. It also risks them never being delivered, and enables the protections to be readily compromised by subsequent amendments that can be processed without publicity and without consideration by the Committee process or the Parliament.

In short, the credibility of such protections as are being proposed is shot to ribbons by the failure to put them high on the agenda. The Department is greatly undermining its own scheme by its intransigence on this matter alone.

Regardless, any statement in either Bill suggesting that consumers can directly review their own health information is misleading. Such statements will seriously erode consumer trust in the system once they have direct experience of such. Research findings indicate the lack of patient trust in an electronic health system has dire consequences for clinician trust in and the effectiveness of such schemes (6, 7). Logically then, misleading information contained in the Bills will erode the effectiveness of the Australian PCEHR system.

As all previous submissions suggest, APF concerns centre on 4 major themes: lack of definition, lack of evidence to support assumptions made in the Bills, quality of care and ineffective legislative issues. We are concerned that without any real-life, duplicatable evidence the notion of social value pervading the Bills presupposes a potentially dangerous scientific validity i.e. that there is privacy versus quality-of-health-care pendulum and that to get good health care one must swing the pendulum against privacy. This is simply not the case and moreover, in the context of the PCEHR Draft Bill and Consequential Amendments Bill, is seriously damaging to the quality of patient health care outcomes more generally.

New and specific concerns

New and specific concerns with the Bills are as follows:

1. The legislation does not contain an adequate definition of "health provider".

The APF asks that the term "health provider" is properly and adequately defined in the legislation.

2. The legislation excludes any discussion of new and emerging technologies, such as cloud computing, smart phones and tablets. These may pose privacy or security risks to an individual's health and personal information or clinical files. Patients and their clinicians need to feel confident applying such innovations to health care data. This is not the case at present.

The APF maintains that the legislation must specify guidelines or standards to enable the application of new and emerging technology to the PCEHR system.

3. The legislation permits health services to download PCEHR system data and store it on their own clinical information services. Researchers will be able to apply to human ethics committees to override consent using Section 95 and 95A of Australian Privacy Law to obtain PCEHR data directly from health service systems rather than from the Department of Health and Ageing (DOHA) or its agencies (8). This is of particular concern given the Public Interest Determinations (PIDs) 11 and 11A that currently permit the collection and use of contact details of genetic relatives to enable disclosure of genetic information. Recent moves to renew temporary PIDs 10 and 10A that permit the collection by health service providers of third party health information that

is relevant to a patient's family or social medical histories, without the third party's consent, are also concerning (9). The megamerger of Centrelink, Medicare and DHS without a privacy impact assessment exacerbates matters (10). Data exchanges of this nature will not manifest in the proposed technical audits of PCEHR system records. The community will have no ability to know of or control access to their PCEHR data.

The APF requests that legislative guidelines be incorporated into the Bills to control researcher access to PCEHR system data stored on health services' clinical information systems for secondary purposes without consumer knowledge or consent.

4. No Government can be sued or prosecuted for any harm or damage resulting from the Legislation and its implementation. No employee of these jurisdictions can be sued or prosecuted for any harm or damage resulting from the Legislation and its implementation. The APF believes that all sanctions for data breach contained in the draft Bills absolve all governments and their agents from any responsibility for personal or clinical information.

The APF believes that absolution of all Governments and their agents from responsibility from data breach should be removed from the draft Bills. It is unacceptable to absolve government jurisdictions from accountability to the community.

5. The APF asks for detail of the circumstances of deliberate data breach and asks precisely how this might occur in the context of an ordinary (not eminent) citizen's PCEHR system data.

The APF asks that deliberate acts of PCEHR system data breach are defined in the draft Bills.

6. No health service, or health professional or clinician can be sued or prosecuted for any harm or damage resulting from the Legislation and its implementation if government authorities decide no deliberate data breach occurred. Penalties outlined in the Bill are therefore unenforceable and so are irrelevant.

The APF asks for penalty details in the context of unintentional breaches of community information linked by the PCEHR system. Such penalties would include, but not be limited to, compensation to the aggrieved parties, the availability of class action in the case of major breaches to lower costs to individual plaintiffs, and to assure means are put in place to reduce the re-occurrence of breaches in the future. The latter measure would be binding upon the breaching agent.

7. Which body or organisation will be held into account in the instance of dangerous or malicious hacks of centralised databases, such as the Individual Health Identifier database, that are linked by the PCEHR system? If one accidentally kills someone on the road or accidentally walks out of a

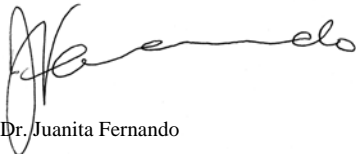
shop without paying for goods, one must still face consequences. The same is true of breaches to health data.

The APF maintains that all breaches of health data, regardless of their nature or context, must be subject to consequences for those involved in the breach.

8. Finally, the APF supports the submission made by David More regarding all governance issues and other relevant matters.

Our clear impression is that health authorities remain “rearranging deckchairs on the Titanic” rather than grappling with the real life privacy and security issues generated from all of our previous submissions and questions regarding the PCEHR system ConOps and supporting legislation.

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. Telstra security exonerated in mailing list error ITWire Jul 7, 2011 5:04 PM (15 hours ago) <http://www.itnews.com.au/News/262961,telstra-security-exonerated-in-mailing-list-error.aspx>
2. Brettingham-Moore, C. "Pharmacy-held data security questioned." Medical Observer, June 4 2010.
3. "Smartcards to give patients records control". ABC News. 12 July 2011. <http://www.abc.net.au/stories/2011/07/12/3267328.htm>
4. Wilcox, AB., Yueh-Hsia Chen & Hripcsak, G. "Minimizing electronic health record patient-note mismatches" JAMIA 2011;18:511-514 doi:10.1136/amiajnl-2010-000068
5. Hilvert, J. "Commissioner eyes tough e-health privacy laws". Jul 14, 2011. <http://www.itnews.com.au/News/263561,commissioner-eyes-tough-e-health-privacy-laws.aspx>
6. Senate Official Hansard <http://www.aph.gov.au/hansard/senate/dailys/ds150310.pdf>
7. Fernando, J. & Dawson, L. (2009) The health information system security threat lifecycle: An informatics theory. International Journal of Medical Informatics 78(12)
8. More, D. "I Think I Have Now Worked Out Why The PCEHR is A Fundamentally Flawed Idea! See If You Agree". July14 Australian Health Information Technology Blog, Thursday, July 14, 2011 <http://aushealthit.blogspot.com/>
9. Greenhalgh T, Stramer K, Bratan T, Byrne E, Russell J, Hinder S, Potts H. The Devil's in the Detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace programmes. London: University College London; 2010.
10. East, M. 'AHPRA owes doctors an apology, inquiry finds', [australiandoctor.com.au](http://www.australiandoctor.com.au/news/2f0c070f2f.asp), 3 June 2011, <http://www.australiandoctor.com.au/news/2f0c070f2f.asp>
11. Security and Access Framework http://www.nehta.gov.au/component/docman/doc_download/877-security-and-access-framework

Policy Position eHealth Data and Health Identifiers

28 August 2009

<http://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf>

This document builds on the APF's submissions over the last two decades, and particularly during the last three years, in order to consolidate APF's policy position. It presents a concise statement of general Principles and specific Criteria to support the assessment of proposals for eHealth initiatives and eHealth regulatory measures.

The first page contains headlines only, and the subsequent pages provide further explanation.

General Principles

- 1 **Health care must be universally accessible.**
- 2 **The health care sector is by its nature dispersed.**
- 3 **Personal health care data is inherently sensitive.**
- 4 **The primary purpose of personal health care data is personal health care.**
- 5 **Other purposes of personal health care data are secondary, or tertiary.**
- 6 **Patients must be recognised as the key stakeholder.**
- 7 **Health information systems are vital to personal health care.**
- 8 **Health carers make limited and focussed use of patient data.**
- 9 **Data consolidation is inherently risky.**
- 10 **Privacy impact assessment is essential.**

Specific Criteria

- 1 **The health care sector must remain a federation of islands.**
- 2 **Consolidated health records must be the exception not the norm.**
- 3 **Identifiers must be at the level of individual applications.**
- 4 **Pseudo-identifiers must be widely-used.**
- 5 **Anonymity and persistent pseudonyms must be actively supported.**
- 6 **All accesses must be subject to controls.**
- 7 **All accesses of a sensitive nature must be monitored.**
- 8 **Personal data access must be based primarily on personal consent.**
- 9 **Additional authorised accesses must be subject to pre- and post-controls.**
- 10 **Emergency access must be subject to post-controls.**
- 11 **Personal data quality and security must be assured.**
- 12 **Personal access and correction rights must be clear, and facilitated.**

General Principles

- 1 **Health care must be universally accessible.** Access to health care must not be conditional on access to health care data or on demonstration of the person's status (such as residency rights or level of insurance)
- 2 **The health care sector is by its nature dispersed.** Health care is provided by thousands of organisations and individual professionals, each with a considerable degree of self-responsibility. The sector is far too large, and far too complex to be centrally planned. Instead it must be managed as a large, complex and highly de-coupled system of autonomous entities, each of which is subject to regulation by law, Standards and Codes
- 3 **Personal health care data is inherently sensitive.** Many individuals have serious concerns about the handling of at least some categories of health care data about themselves. Their willingness to divulge important information is important to their health care, but is dependent on them having confidence about how that information will be managed
- 4 **The primary purpose of personal health care data is personal health care.** The protection of the individual person is the primary function of personal health care data and systems that process it. The key users of that data are health care professionals
- 5 **Other purposes of personal health care data are secondary, or tertiary.** Public health is important, but is a secondary purpose. Administration, insurance, accounting, research, etc. are neither primary nor secondary but tertiary uses. The tail of health and public health administration and research must not be permitted to wag the dog of personal health care
- 6 **Patients must be recognised as the key stakeholder.** Government agencies and corporations must directly involve people, at least through representatives of and advocates for their interests, in the analysis, design, construction, integration, testing and implementation of health information systems
- 7 **Health information systems are vital to personal health care.** People want systems to deliver quality of service, but also to be trustworthy, transparent and respectful of their needs and values. In the absence of trust, the quality of data collection will be greatly reduced
- 8 **Health carers make limited and focussed use of patient data.** Health care professionals do not need or want access to their patients' complete health records, but rather access to small quantities of relevant information of assured quality. This requires effective but controlled inter-operability among health care data systems, and effective but controlled communications among health care professionals. Calls for a general-purpose national health record are for the benefit of tertiary users (administration, insurance, accounting, research, etc.), not for the benefit of personal health care
- 9 **Data consolidation is inherently risky.** Physically and even virtually centralised records create serious and unjustified risks. Services can be undermined by single points of failure; health care data isn't universally understandable but depends on context; consolidation produces a 'honey pot' that attracts break-ins and unauthorised secondary uses and creates the additional risk of identity theft; and diseconomies of scale and scope exceed economies
- 10 **Privacy impact assessment is essential.** Proposals relating to personal health care data and health care information systems must be subject to PIA processes, including prior publication of information, consultation with affected people and their representatives and advocates, and publication of the outcomes of the study. Designs for systems and associated business processes must be based on the results of the PIA, and implementations must be rejected if they fail to embody the required features

Specific Criteria

- 1 **The health care sector must remain a federation of islands.** The health care sector must be conceived as islands that inter-communicate, not as elements of a whole. Health care information systems must be conceived as independent services and supporting databases that inter-operate, not as part of a virtually centralised database managed by the State. Coordinating bodies must negotiate and facilitate inter-operability, not impose central schemes
- 2 **Consolidated health records must be the exception not the norm.** A small proportion of the population may benefit from linkage of data from multiple sources, primarily patients with chronic and/or complex conditions. Those patients must be the subject of consent-based, specific-purpose data consolidation. This activity must not apply to people generally
- 3 **Identifiers must be at the level of individual applications.** Each of the large number of dispersed health care information systems must use its own identifier for people. A system-wide or national identifier might serve the needs of tertiary users of personal data, but does little for the primary purpose of personal care, and it creates unnecessary risks for individuals
- 4 **Pseudo-identifiers must be widely-used.** Particularly when personal data moves between organisations, the maximum practicable use must be made of one-time-use and other forms of pseudo-identifiers, in order to keep people's identities separate from the data itself, and minimise the risk of personal health care data escaping and being abused
- 5 **Anonymity and persistent pseudonyms must be actively supported.** Anonymity is vital in particular circumstances such as ensuring that people are treated for sexually transmitted diseases. Persistent pseudonyms are vital in particular circumstances such as for protected witnesses, victims of domestic violence, and celebrities and notorieties who have reason to be concerned about such threats as stalking, kidnapping and extortion
- 6 **All accesses must be subject to controls.** Access to personal data must be subject to controls commensurate with the circumstances, including the sensitivity of the data and the potential for access and abuse of access. This requires identification of the category of person and in many cases of the individual who accesses the data, and authentication of the category or individual identity. However, the barriers to access and the strength of authentication must balance the important value of personal privacy and effective and efficient access by health care professionals
- 7 **All accesses of a sensitive nature must be monitored.** Non-routine accesses and accesses to particularly sensitive data must be detected, recorded, and subject to analysis, reporting, sanctions and enforcement
- 8 **Personal data access must be based primarily on personal consent.** The primary basis for access to personal data is approval by the person concerned. Consent may be express or implied, and may be written, verbal or non-verbal, depending on the circumstances. All accesses based on consent must be detected, recorded and subject to analysis, reporting, investigation, sanctions and enforcement
- 9 **Additional authorised accesses must be subject to pre- and post-controls.** All accesses that are not based on personal consent must be the subject of explicit legal authority that has been subject to prior public justification. All such accesses must be detected, recorded and subject to analysis, reporting, investigation, sanctions and enforcement
- 10 **Emergency access must be subject to post-controls.** Health care professionals (but only health care professionals) must have the practical capacity to access data in apparent violation of the personal consent principle, but must only do so where they reasonably believe that it is necessary to prevent harm to some person. All such accesses must be detected, recorded, reported and subject to analysis, investigation, sanctions and enforcement
- 11 **Personal data quality and security must be assured.** Data must be of a quality appropriate to its uses, and retained only as long as it remains relevant. Personal data in storage, in transit, and in use, must be subject to security controls commensurate with its sensitivity, and with the circumstances
- 12 **Personal access and correction rights must be clear, and facilitated.** Each person must have access to data about themselves, and access must be facilitated by any organisation that holds data that can be associated with them. Where appropriate, the access may be intermediated, in order to avoid misunderstandings and misinterpretation of the data. Where data is not of appropriate quality, the person must be able to achieve corrections to it

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 grounds 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