



**Australian
Privacy
Foundation**

G.P.O. Box 1196
Sydney NSW 2001
enquiries@privacy.org.au

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

Senator The Hon John Faulkner
Cabinet Secretary
Special Minister of State
Privacy & FOI Policy Branch
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON 2600 ACT

25 February 2009

Dear Senator Faulkner,

Re: Response to the Australian Law Reform Commission (ALRC) (Part H of Report 108)

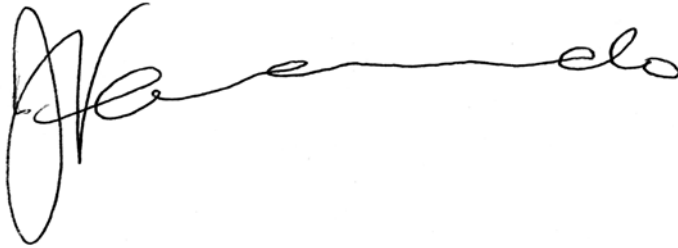
I am writing in my capacity as Chair of the Health Sub Committee of the Australian Privacy Foundation (APF).

Thank you for our invitation to the Health Privacy Forum on February 3rd in Sydney. The APF was glad to contribute to the discussion of recommendations from the Australian Law Reform Commission's (ALRC) report (Part H of Report 108) "For your information: Australian privacy law and practice".

Unfortunately as an all volunteer organisation, currently facing a number of consultations, we have not been able to resource an independent submission on part H of report 108. However, we are satisfied that the Cyberspace Law and Policy Centre (CLPC), UNSW, has identified some significant privacy threats in the current recommendations. We support the CLPC's suggestions for amendments to provide greater privacy protection.

From an advocacy perspective, some key concerns remain though. We have attached our submission responding to recommendations from the ALRC report to this correspondence. The submission supports the CLPC submission and outlines our further concerns.

Yours faithfully

A handwritten signature in black ink, appearing to read 'Juanita Fernando', written in a cursive style.

Juanita Fernando

Chair
Health Sub Committee
Australian Privacy Foundation
GPO Box 1196 Sydney NSW 2001

email: mail@privacy.org.au

web: www.privacy.org.au

CC: Senator The Hon Nicola Roxon

Mike McGrath

Dr. Bridget Bainbridge



**Australian
Privacy
Foundation**

APF RESPONSE TO PART H OF REPORT NUMBER 108, THE AUSTRALIAN
LAW REFORM COMMISSION'S (ALRC) PRIVACY REPORT "FOR YOUR
INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE"

Submission to the Australian Government

The Australian Privacy Foundation (APF) submission supports the concerns raised by the Cyberspace Law and Policy Centre (CLPC), UNSW in its submission to the Australian Government.

As an all volunteer organisation currently facing a number of consultations we have not been able to resource an independent submission on this matter. However, we are satisfied that the CLPC has identified some significant privacy threats in the current recommendations. We support the CLPC's suggestions for amendments to provide greater privacy protection.

Nonetheless some concerns remain, as outlined below.

1. Patient-centred health systems

A recent Health Privacy conference concluded that 4 key elements were the central planks of what patients want from health information systems. The elements are trust, quality of service, transparency and respect (Whitaker, 2009). While some aspects of quality of service may be achieved by sharing health information, many patients do not want this to occur unless they can quarantine or control some of health data.

Certainly the "Privacy Blueprint for the Shared Electronic Health Record", when referring to accountability to patients, states:

"An audit trail will record all activity on the IEHR [Individual Electronic Health Record], and will identify who accessed the IEHR, what they accessed and when they accessed it. The audit function is an important accountability mechanism that enables individuals to check who has accessed their record while ensuring the privacy of the individual is protected (NEHTA, 2008)."

If NEHTA is devising a technology that identifies an individual on a computer rather than an account name, then it is possible to make a quarterly or half yearly statement showing all access to one's health record available to individual patients if required. The introduction of a two tiered system for access is a logical approach to the matter since immediate access to details of all named health care professionals who have accessed one's records may be an unacceptable privacy (and safety) risk to the professionals. However, a patient's initial right to a list of all access events - time, date, location, and then a right to query further if concerned, followed by mediated access to the details of specific professionals, may balance the privacy interests of both groups on individuals. The idea needs further work than outlined here, but provides a useful direction for further work. In one move, national health privacy laws can ensure that health information systems will provide what it is that patients want without affecting quality of care outcomes or the privacy concerns of the health professionals treating them.

The APF maintains that trust, quality of service, transparency and respect are critical health security elements and should be at the forefront of the recommendations, yet there is no evidence that this has occurred when the ALRC reflected on raw data underpinning the changes.

The APF believes the recommendations must be informed by the development of a new conceptual model that places trust, quality of service, transparency and respect at the forefront of health privacy policy development.

2. Recommendation 60-3

The recommendation concerns consultation with relevant stakeholders to develop and publish guidelines on the handling of health information.

The APF believes direct reference to consumer groups should be added to the recommendation along with the Department of Health and Ageing. Consumers are "relevant stakeholders" when it comes to the privacy of their health information.

However this is not always acknowledged. For instance, a recent report by Deloitte's for NEHTA claims it undertook "extensive consultations with key stakeholders" yet the APF was not consulted (Dearne, 2009).

The APF believes direct reference to consumer groups should be added to the recommendations where "consultation with relevant stakeholders" is required.

3. Recommendation 61-1

The Recommendation concerns the importance of enabling legislation with regard to Shared Electronic Health Records (SEHR) and Unique Health Identifiers (UHI).

The enabling legislation needs to address the important issue of consent for SEHRs and UHIs in accordance with the 2006 COAG commitment to a consent-based national e-health system (COAG 2006). The consent-based system must address issues such as 'express consent', 'implied' consent, 'bundled' consent and 'changing' consent (Stokes, 2008). Consideration should also be given for tailored views of health information in SEHRs so that patients can deny access to specific information and to specified persons, since this often seems to be the aim of individuals contacting the APF (See our response to **Recommendation 63-1** of this submission, below).

The APF maintains enabling legislation that will address the key issue of consent, especially government commitment to a consent-based national SEHR system, remains to be addressed in the Recommendations.

4. Recommendation 63-1

The Recommendation concerns sharing health information between service providers.

Research has shown that many patients do not want their information shared. As a result, they may not seek treatment when it is needed (Fernando & Dawson, 2008). Studies from NZ and the US have provided strong evidence to say a lack of confidence in the privacy of health information results in undermining of e-health systems and may create a health black economy, even where the patient's health may

be adversely affected (Crompton 2002; OFPC 2003). At the same time, the APF is aware of circumstances where medical professionals may want to share information to avoid medical error and so enhance quality of care outcomes. Thus, without a means of tailoring views of health data, some patients will withhold relevant information from medical professionals, potentially creating a black health economy or contributing to medical error.

The APF supports the idea of tailored views of a patient's health information when it is shared between medical professionals.

References

- Council of Australian Governments (COAG) (2006) Council of Australian Governments' Meeting, 10 February 2006. (Cited 14 February 2009)
http://www.coag.gov.au/coag_meeting_outcomes/2006-02-10/index.cfm#reform
- Crompton, M. (2002) Privacy, technology and the healthcare sector (A background paper). (Cited 12 July 2003) <http://www.privacy.gov.au/publications/>
- Dearne, K. (2009) Canberra stalls on e-health details. The Australian IT Section, February 3. (Cited 3 February, 2009) <http://www.australianit.news.com.au/story/0,24897,24998724-15306,00.html>
- Fernando, J & Dawson, L. (2008) Clinician assessments of workplace security training- an informatics perspective. eJHI 3(1) p.e7
- National E-Health Transition Authority (NEHTA) (2008) Privacy blueprint for the individual electronic health record (Cited February 13 2009) <http://www.nehta.gov.au/privacy>
- Office of the Federal Privacy Commissioner (OFPC) (2001) Guidelines on privacy in the private health sector. (Cited 24 May 2003)
http://www.privacy.gov.au/publications/hg_01.pdf
- Stokes, D. (2008) Is privacy a privilege or a pain? Presentation at Health Privacy Futures 2008, Brisbane, 10-11 November. (Cited February 13 2009)
<http://www.healthprivacy.org.au/downloads>
- Whitaker, J. (2008) Health Privacy: What Consumers Want. Presentation at Health Privacy Futures 2008, Brisbane, 10-11 November. (Cited February 13 2009)
<http://www.healthprivacy.org.au/downloads>