Australian Privacy Foundation

enquiries@privacy.org.au

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

16 April 2014

The honourable Senator Fiona Nash
Email: Minister.Nash@health.gov.au

CC: The honourable Peter Dutton MP

Dear Senator Nash

Re: Concerns about security and privacy aspects of the PCEHR system and negative impacts on health outcomes

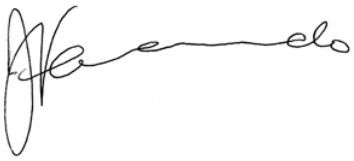
I write as the Chair of the Health Committee of the Australian Privacy Foundation (APF). The APF is concerned about security and privacy aspects of the Personally Controlled Electronic Healthcare Record (PCEHR) system, and their negative impacts on health outcomes and patient and clinician trust. Therefore the APF makes the following four requests:

1. The APF notes that another clinical safety audit of the PCEHR has been established, the fourth since its implementation in July 2012.[1] The APF requests the findings from earlier audits be made available in the public domain, to be followed by publication of the research design and findings from the forthcoming PricewaterhouseCoopers audit. It is crucial that the results of these taxpayer-funded audits be publicly and transparently available so that patients can provide informed consent to uploading their private health information to PCEHR servers.
2. The "Heartbleed" security flaw, very recently discovered, creates the scope for a serious threat to the privacy and security of patient information stored on the PCEHR when end users' rely on open SSL, or HTTPS, for information security. The flaw potentially affects consumers, clinicians and all other health professionals (such as those working at GP and specialist practices or hospitals). Several commercial services on the Internet, such as Tumblr and SurveyMonkey, have already advised clients to change their user credentials to control the threat. So the APF requests information about what "Heartbleed" user advice has been provided to the community with regards to protecting the privacy and security of PCEHR system information? Patient and health professional trust in the usefulness of the PCEHR system will be seriously eroded unless this concern is urgently addressed.
3. Also I understand that a C-CDA flaw, that is the insertion of malicious code into the CDA (does this refer to Clinical Document Architecture?) while viewing it through external documents or systems, has been recently exposed by Joshua Mandel.[2] It has been reported

that health authorities do not believe the CDA flaw affects the PCEHR core. Yet medical software industry vendors have received guidance on this issue by the National E-Health Transition Authority. What guidance has been provided to consumers and other system end-users? The APF is concerned that without such guidance, community trust in the national PCEHR will be further eroded.

4. Further, it has been reported that health authorities do not believe there is a sufficient level of community interest in the publication of findings from the recent review of the PCEHR project, initiated by Minister Dutton, to warrant its release.[4] This response by authorities seems incredible to the APF given the large number of people who ask the APF about the PCEHR and in context of every PCEHR-related submission we have made to various authorities over several years.[5] We ask to review copies of, or pointers to, the evidence used to support decisions about levels of community interest in the release of findings about a system that cost tax payers more than $466.7 million dollars.

Yours sincerely



Chair, Health Committee
Australian Privacy Foundation

Dr Fernando is in Medicine, Nursing & Health Sciences, Monash University.

Phone: 03 9905 8537 or 0408 131 535 / Mailto: juanita.fernando@monash.edu.

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

References

1. Australian Commission on Safety and Quality in Healthcare (2014) *Safety in E-Health.* http://www.safetyandquality.gov.au/our-work/safety-in-e-health/
2. Substitutable Medical Applications& Reusable Technology (2014) *Security vulnerabilities in C-CDA Display using CDA.xsl*. http://smartplatforms.org/2014/04/security-vulnerabilities-in-ccda-display/
3. McDonald, K. (2014) Exploit vulnerabilities in CDA do not affect PCEHR core, *PulseIT*, http://www.pulseitmagazine.com.au/index.php?option=com_content&view=article&id=1827:exploit-vulnerabilities-in-cda-do-not-affect-pcehr-core&catid=16:australian-ehealth&Itemid=327
4. Delimiter (2014) *No public interest" in PCEHR review release.* http://delimiter.com.au/2014/03/31/public-interest-pcehr-review-release/
5. APF (2014) Healthcare generally. http://www.privacy.org.au/Papers/indexPolicies.html#Health