A u s t r a l i a n
P r i v a c y
F o u n d a t i o n

9 June 2009

The Hon. John Joseph Della Bosca, BA MLC
Level 30 Governor Macquarie Tower,
1 Farrer Place,
Sydney NSW 2000

CC: Senator Roxon

Dear Minister Della Bosca

Re: Health*e*link rollout throughout NSW

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

A recent report in the Sydney Morning Herald (SMH) indicates that the New South
Wales State Government has started rolling out new electronic medical records
(eMRs) technology in public hospitals to help improve patient care and safety
throughout NSW [1]. The eMR is not a new initiative; it simply extends the opt out
Health*e*link electronic records pilot that resulted in a summary evaluation report, as
outlined in our letter to you of December 2008.

The report warned the opt-out approach ought <u>not</u> to be applied across NSW. Neither
should the 'opt-out approach' be used as a model in other Australian scenarios if state,
territory and national governments are looking to support improved patient care
outcomes. Nonetheless, like a machine, the flawed program inexorably continues to
expand.

Governments and NEHTA have failed to develop a properly consulted-upon and
widely accepted national electronic health record privacy and personal information
security policy. The failure has left patients and clinicians alike in a situation where
this latest repeat of previous privacy disrespectful proposals in NSW suggests the
eMR rollout seems to be operating in a vacuum. Personal privacy, public health and
the capacity for safe engagement with the NWS health system appear to be at risk

The rollout also appears to contradict the timeline outlined in the Garling report [2]. In its Clinical Records and IT Recommendations, the report recommends that NSW Health implement several preparatory programs before a state-wide rollout of the eMR in 4 years time (Recommendation 51). The reported premature announcement of the rollout in the SMH pre-empts the work deemed essential by Garling.

The SMH story also claims a range of benefits will accrue to clinicians and patients as a result of the rollout. These benefits include ease of tracking patient records through the hospital system, clinical access to secure and reliable patient information from computer work stations, and the end of data fragmentation. These are desirable patient care outcomes however the Australian clinical workforce capacity has not kept pace with technological change. The critical shortage of clinicians who can take advantage of new and emerging technological innovations in patient care settings at present is worrying [3]. This is particularly so in the context of the expanded Health*e*link proposal to introduce a controversial and unproven new technology and patient medical record access model, the implications and risks of which clinicians will struggle to appreciate.

Suggested benefits hinge on certain assumptions about how clinicians and support staff can be expected to use these systems. However these assumptions are not reliably supported by evidence [4]. As a consequence, the capacity for eMRs to improve patient care outcomes is threatened as are the additional security protections potentially offered by eMRs [4].

Among the unresolved personal information privacy and security risks for patients with these eMR proposals are those associated with lack of foolproof mechanisms for dealing with inevitable IT system failures, large or small.

The recent power outage in NSW, although resolved in a few days, caused chaos in hospitals dependent on access to it for access to patient care records [6]. EMRs were lost and fragmented as a result. Patients trusted the system to improve their safety and protect information security; instead outcomes were clearly compromised as were their privacy concerns when paper and whiteboards were used instead of the eMRs [6].

Equally concerning are the governance and transparency problems associated with the uncoordinated efforts to implement an eMR before the risk and privacy framework is clearly under control, and in particular an unwillingness to deal properly with data loss episodes where they occur.

An e-pathology service was recently reported as posting 254 confidential patient records on the Internet. No apology was made by the company involved to the patients concerned. Search engines cached the data so they remained accessible despite their subsequent removal from the company's website [7]. The company at the centre of the furore is listed on a NEHTA website that outlines the benefits of the electronic transfer of health information without alluding to the alleged breach [8].

Finally, our understanding of the latest Health*e*link plan is that eMRs will store new patient data but there are no plans to integrate legacy data into the system. Some patient data will be stored on paper systems, other data in various e-health

applications and still other data on the NSW eMR. Thus for several years, possibly more, patient care data will be even more fragmented than it is at the present.

The APF is not against electronic medical record systems. We support proposals drawing on best practice in clinical systems development to protect patient privacy. By adopting a widely-consulted and accepted national framework for eMR privacy and personal information security these proposals put patients in effective control of their own sensitive health record information. But, as Garling points out (Point 1.211), trust and confidence in eMR systems is essential, not only for wider public acceptance but also for critical matters like public health (willingness to disclose sensitive data, including infections) and individual access to essential personal medical services (for example, sexual or psychiatric problems) [2].

The APF is worried the faulty rollout of Health*e*link and the failure to address eMR privacy in a systematic and respectful way may encourage further doubts about shortcomings linked to other eMR initiatives. Hence, we ask that you consider reviewing the rollout timeline in light of achieving an effective eMR the first time instead of employing the inevitable "bandaids" to patch up a poor system in NSW, as has occurred overseas.

Yours sincerely

Chair, Health Sub Committee
Australian Privacy Foundation

Email: juanita.fernando@med.monash.edu.au Mobile phone: 040-813-1535

REFERENCES

[1] Hall, L. (2009) Paper patients' notes out, digital records in The Sydney Morning Herald. May 02.
http://www.smh.com.au/national/paper-patients-notes-out-digital-records-in-20090501-aq6k.html

[2] Garling, J. [2008] Special Committee of Enquiry into Acute Care Services in NSW Public Hospitals
http://www.lawlink.nsw.gov.au/lawlink/Special_Projects/ll_splprojects.nsf/pages/acsi_index

[3] Australian Health Information Council (AHIC) (2007) e-Health Future Directions Briefing Paper
for AHMAC meeting 4 October 2007.

[4] Fernando, J & Dawson, L. (2008) Clinician assessments of workplace security training- an
informatics perspective.. eJHI 3(1):E7 http://www.ejhi.net/ojs/index.php/ejhi/article/view/3(1)%3Ae7

[6] Benson, K (2009) Power failure lasting 36 hours cripples hospital care. The Sydney Morning
Herald. May 6 http://www.smh.com.au/national/power-failure-lasting-36-hours-cripples-hospital-care-
20090505-au1s.html

[7] Sullivan Nicolaides leak exposes hypocrisy. Courier-Mail March 30, 2009 11:00pm (cited April 5
2009) http://www.news.com.au/couriermail/story/0,23739,25265407-13360,00.html).

[8] Persson, L (2008) Electronic Transfer of Laboratory Notifications. National E_Health Transition
Authority (NEHTA) http://www.nehta.gov.au/dmdocuments/NSW_Health_Philip_Batey_14.05.08.pdf