Australian
Privacy
Foundation

post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

APF Response to NEHTA's Privacy Blueprint for the IEHR

1. Introduction

The Australian Privacy Foundation (APF) maintains that NEHTA's Privacy Blueprint ('the Blueprint') for the Individual Electronic Health Record (IEHR) describes a record that will not benefit patients. The Blueprint incorporates limited consumer feedback from pertinent Roundtables. However, as the document itself points out several times, the personal health information collected in the record will primarily benefit stakeholders, such as researchers and administrators looking at research, cost-management or insurance, rather than patients. Hence, the notion of enhancing services for patients by introducing the IEHR is not convincing.

2. Enhanced patient care interests: Critique

Legal frameworks

The Blueprint states that the IEHR will ensure that an individual's right to privacy will comply with privacy principles. On the one hand NEHTA have mapped IEHR information flows against all current Australian privacy legislation. On the other hand, NEHTA alludes to devising new privacy legislation to enable the IEHR. They apparently plan to monitor liability issues under existing privacy legislation. The new legislation would be enacted when and if required to protect IEHR stakeholders from prospective liability for access to the record under existing laws. This implies that liability about access issues will be monitored for everyone. However, patients supposedly control access to to their IEHR on the basis of consent. Unlike other "IEHR stakeholders", patients cannot be held liable for access to information about themselves. Therefore, the Blueprint is confusing and conflates patient interests with those of administrators, researchers and other key stakeholders.

Consent

The Blueprint also skirts around the issue of how to deal with the problems of complexity and detail in the levels of patient consent required for an effective IEHR. Too much complexity will overwhelm patients, yet too little detail, such as occurs with bundled consent, is not useful either. This balance is at the heart of the domain and presents a real challenge. NEHTA does not appear to have put it at the heart of their analysis or thinking about IEHR privacy options. This is not simply a technical design issue, but also one with solutions. Extensive feedback from a wide range of users and their surrogates about where the balance should be and how it should be presented should inform these solutions. Thus, the APF queries whether the analytic method used by NEHTA to date has adequately engaged user feedback or that of their surrogates.

Moreover, earlier analysis of the complexities involved in ensuring patients make an informed decision were incorporated in reports by Xamax Consulting. Xamax drafted at least 2 key reports for the Acute and Coordinated Care Branch, Department of Health and Aged Care, in 2002 (Xamax Consultancy Pty Ltd #1, 2002; Xamax Consultancy Pty Ltd #2, 2002). This important prior work has apparently been overlooked by NEHTA, while reports from the United Kingdom and Canada, with health care regimes that are very different to the Australian context, have not. Hence, the APF questions the validity of information sources used to underpin the IEHR.

Also, at what point of the data collection steps feeding into the IEHR will patients be allowed to withhold consent? How will they be protected from clinical pressure to participate because it will make 'your' life easier, when it's really patient administration that may be made easier? It seems that a patient may only withhold consent before a particular incident of medical care occurs. Although the patient may wish to remove consent during treatment, there is no apparent mechanism to do so. After treatment, the data has already been marked up to the IEHR, so there is no opportunity to withdraw it, only to add a codicil. The evidence shows that patients do not always provide relevant information when they believe their privacy may be compromised (Karro 2005). Therefore, the IEHR jeopardises improved patient health care outcomes.

Indeed, the Blueprint often postulates notions that the IEHR will improve the integrity, availability and confidentiality of patient care records. However, evidence looking at the actuality of patient care work with e-health indicates otherwise. Recent Australian research shows that clinicians not only do not know how to work with electronic care data, but that they actively avoid the systems, preferring to use paper printouts instead, not to mention an entrenched scepticism about national e-health systems (Fernando & Dawson #1 2008; Fernando & Dawson #2 2008). Earlier evidence from the UK and the USA supports the Australian findings (Timmons 2003; Medlin 2007). The APF believes NEHTA should provide some real life evidence about the trustworthiness of data on an IEHR and improved quality of care for Australian patients before proceeding further.

Network infrastructure

As raised by the APF in previous Roundtables and submissions, a centralised network topology will provide a kind of 'honeypot' for hackers or others with malicious intent. A 'honeypot' entices the unauthorised use of data stored in a centralised database by intruders or hackers. When a similar ‘honeypot’ was established in Holland, hackers retrieved over 1.2 million or 8% of Dutch patient IEHRs (Spaink 2005). Moreover, NEHTA's representatives have been unwilling to consider the option of a federated, “just in time” architecture despite repeated requests by the APF. Thus, a potentially serious privacy flaw in the IEHR framework has been consistently overlooked.

The risks we see associated with the central storage of IEHRs seem to indicate an intrinsic favouring of research or administrative convenience over privacy and patient care, though the degree to which this is conscious or explicit is debatable. Until NEHTA pulls back from the data consolidation model and moves to a 'just in time' data collection process across local databanks, neither doctors nor patients should trust the system to provide the most up-to-date diagnostic information. Indeed the 'honeypot' cannot truly be considered a 'consumer centred' system when the primary benefits listed in the Blueprint are, as stated earlier, to researchers, administrators and other stakeholders.

The health information stored in an IEHR refers to real people. Patients should be given priority over all else and that involves a federated system rather than a 'single', conglomerated data storage system. No matter what is implemented, good governance will not solve this qualitative difference. A recent Health Informatics Society Australia (HISA) survey reported that NEHTA has consistently underperformed in high priority areas such as privacy, associated consent mechanisms and controlling access to patient health information (Legg & Lovelock 2007). The Blueprint indicates that this remains the case.

Conclusion

NEHTA must not continue with the pretence that the construction of an IEHR is primarily for the patient's benefit. The main drivers are administration, cost-management, insurance and research. Each stakeholder must be required to come out with their own justifications, and not use the shield of 'enhanced health services'. Further, most aspects of the IEHR are speculative, many of which are highly unconvincing, and need further work. Implementation of the IEHR continues to overlook the 'honeypot' issue and puts the interests of patients second to those of other key stakeholders. Thus, the Privacy Blueprint for the IEHR does nothing of consequence to advance patients' privacy interests.

References

Fernando, J & Dawson, L #1 (2008) Clinician assessments of workplace security training- an informatics perspective. *electronic Journal of Health Informatics 3(1): e7.* http://www.ejhi.net

Fernando, J & Dawson, L #2 (2008) The health information system security threat lifecycle: An informatics theory. *JAMIA* (under consideration).

Legg, M. & Lovelock, B. (2007). *HISA Submission to the Boston Consulting Group NEHTA Review*. Health Informatics Society, Australia Ltd., Brunswick East, Victoria

Medlin, B. D. & Cazier, J. A. (2007). An empirical investigation: Health care employee passwords and their crack times in relationship to HIPAA security standards. *International Journal of Healthcare Information Systems and Informatics*, 2, pp.39-48.

Spaink, K. (2005). *Hospital demo hacked - over 1.2 million patient records retrieved.* (viewed 12 September 2005) at http://www.politechbot.com/2005/09/10/over-12-million/

Timmons, S. (2003). Nurses resisting information technology. *Nursing Inquiry*, 10, 257-269.

Xamax Consultancy Pty Ltd #1(2002) *Consumer Consent in Electronic Health Data Exchange: Background Paper,* 1 December at http://www.anu.edu.au/people/Roger.Clarke/EC/e-C-Backgrd-Final021201.doc

Xamax Consultancy Pty Ltd #2(2002)*Consumer Consent in Electronic Health Data Exchange: Implementation Considerations* 1 December at http://www.anu.edu.au/people/Roger.Clarke/EC/e-C-Impl-Final021201.doc