Australian Privacy Foundation

enquiries@privacy.org.au

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

22 November 2013

Review of the Personally Controlled Electronic Health Record (PCEHR): APF submission

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation and I write as Chair of the Health Sub Committee of the APF. The submitted response is designed to support the Federal Minister for Health the Hon Peter Dutton MP's review of the PCEHR, in particular focusing on enhanced consumer engagement. Clinician/technical perspectives are beyond the scope of this work but we have previously published several submissions in this domain.[1]

The APF suggests government attention to the points below will support consumer engagement in the PCEHR and thus help address the consequences of deficiencies in this aspect of past PCEHR project governance and direction. These include risks that core privacy and related concerns will not be understood and implemented in a way that finds favour and acceptance among the community, particularly among those with high sensitivity to potential health record privacy and security problems.

1. Health authorities should publish a simple coherent explanation of the agreed framework of the entities, kinds of information and access and control rules that govern privacy and personal information security. The explanation would help explain how PCEHR and related regulation and procedures work and how these fit into the context of the national Electronic Health Records (EHR) system as a whole. A useful exemplar, authored by Kruys, is currently available for review.[2]
2. An example of where the absence of a clear model of use seems to apply is as follows: Clinicians appear to take little or no account of patient diary input into the PCEHR system and this dismay many patients. The do not understand the relationship between their PCEHR diaries, their PCEHR and improved health outcomes. This requires explicit clarification: either the diary should, by consensus between patient interests, clinicians and other stakeholders, become a standard feature of clinical practice, or the function should be omitted. If there are special

circumstances where it should become a standard feature, they should be identified by consensus.

3. Contrary to patient/consumer expectations of personal control, clinicians and others will in practice mediate each patient/consumer interaction with the PCEHR. The notion of Patient Control either needs to be meaningfully implemented, in the context of a clear overall framework as above, or branding as a "Patient Controlled" system needs to be dropped. We would of course strongly advocate for the former, both on public interest and public and private clinical grounds. But if the profession's apparent expectation that they are in control is implemented, there should be no fudging of this fact.
4. The quality of patient care information in many settings relies upon other clinical record systems within the overall national EHR system feeding dependable evidence into the PCEHR. Recent media reports suggest this evidence is not always reliable.[3] The PCEHR could be potentially dangerous to the reliability of data derived from interactions with other systems; this is not transparently evident and taken into account. The long awaited framework for EHR privacy and personal information security therefore needs to adequately and transparently address traditional issues of accuracy (including the relevance of externally derived information in the new PCEHR context), completeness (including compatibility and usefulness of semantic metadata supporting content items) and currency. These are, of course, technical implementation issues but they need to be made visible and comprehensible at both the higher systems level, for governance and transparency purposes, and at the patient level (to enable patients to assist in identifying the inevitable errors and confusions imported with external data).
5. Many of the chronically ill and other high need or geographically isolated patients/consumers are accustomed to EHRs and familiar with a range of unintended consequences they raise. These consequences include human error resulting in the publication of private health information on the Internet, mistaken identity and time spent with their clinician or clinical team debating the accuracy of information stored on an electronic health record (EHR) before health care can commence.[4] Whether for this reason or arising from data on other systems, PCEHR/EHR records are not always a reliable foundation of patient care. The implications of this need to be addressed: it requires maximum transparency of the provenance of data and of the mechanisms employed to help minimise data errors, but also a routine, systemic expectation that patients have a role in checking, correcting and confirming the quality of data.
6. Patients and consumers often worry about the repercussions of unintended publication of their PCEHR or information from it on the Internet, where millions of ostensibly private and secure records can be obtained by third parties for accidental or deliberate misuse or data mining. The prospect of Mandatory Data Breach Notification obligations more generally has been raised in legislation which was to go before Parliament on the last day of the previous session. Unless this is immediately and effectively legislated for, with the highest level of obligation on medical record breaches, a separate Mandatory Data Breach Notification for the PCEHR should be legislated for the interim. The only way to expect trust and confidence in a system where it is known that there is no basis for absolute assurances of security is for the

data subject to know that they will be immediately informed, without having to wonder, speculate or investigate if their data is breached.

7. The PCEHR legislation does not exclude the Insurance industry from obtaining individual Health Identifier (IHI) numbers and, in the future, possible linkages between individual's PCEHR information and their health insurer. Patients and consumers are anxious because Insurers are not medically qualified to read or interpret health records. The information on the PCEHR may be incorrect and read out of context by a non-clinical person, potentially misinterpreting the record and increasing some health insurance premiums. For a PCEHR to be used against the wishes of a patient for this purpose, or other possible purposes not excluded by law, raises both systemic issues of possible "scope creep" (a common source of problems in large IT system) and the question of whether the patient can either "control' it or trust that it will remain confidential. Confusion about this question of core system purpose and constraints on unwelcome re-use of information for other purposes has been one of the problems of the system to date, confusion that would have been clarified by access to a reliable, frank framework of the kind suggested above. Resolution of this ambiguity is essential.
8. The views of NEHTA-engaged-clinician 'consumers' appeared to override those of patient consumers to the dismay of many consumer representatives. Most other health organisation representatives were engaged late and have not had the same level of influence as the initial NEHTA-engaged-clinicians. The consultation process has fostered community mistrust of the PCEHR. For it to regain this trust (essential if there is to continue to be a reliable expectation of confidentiality in medical records and thus a basis for the traditionally frank and open relationship with a physician) this must be addressed by re-engaging with patients and their advocates, representatives and advisers, and placing their needs and concerns in the driving seat.
9. The clouded issue over clinician ownership of patient health care information is not resolved by the PCEHR system as it does not replace practice records but adds another layer of information to this. This creates opportunities for error and fragmentation because clinicians are required to update and maintain a government system in addition to their own practice systems. Again, a framework which explained how the PCEHR fits within the overall scheme of EHRs is essential, especially for privacy and security issues, but necessarily also describing and making visible assumptions about technical and procedural links and interactions at the levels below and above the PCEHR.
10. The PCEHR does not effectively provide tailored views of information. Diagnostically valid data or insights from association may be lost in the plethora of other, often irrelevant, information also presented on the record. Why can an orthopaedic surgeon, for instance, read that patient has suffered from ear infections or has an obstetric history while reading the PCEHR? The healthcare system is already drowning in information, much of which is unnecessary, for direct patient care. The PCEHR system risks simply adding to this ocean of information without addressing the patient care concerns embodied in it.[5] This suggests end-users in clinical practice directly serving the patient did not take precedence over data collection and presentation for other stakeholders.

11. Patients are aware of technological "downtime" and hypothesize as to the consequence of the downtime for their own care. They need to be informed of how information stored on a PCEHR, or any other EHR, can be accessed by clinicians during 'downtime'. Indeed the range of risks considered and addresses by the security, privacy, continuity and maintenance risk mitigation plan should address downtime implications for patients and consumers; these should be made transparent. While certain technical details may need to remain confidential, we were not reassured by the assertion by the system's security architects that no-one would be allowed to know what risks were contemplated because this would pose an unacceptable security threat. "Security by obscurity", as this is called, is an obsolete model which has proven to be always fallible, and to present a barrier to critical user and expert feedback about the adequacy of risk assessment to map across risks that matter to consumers, patients and other end-users (especially the most vulnerable or concerned), and about the adequacy of precautions to work for those people's interests and practical needs.
12. PCEHR regulatory rules are dynamic and subject to change by subordinate regulation, not legislation (minimising the scope for parliamentary scrutiny of matters like scope creep). The System-Operator, as a public servant, is not independent of the system but a part of it. Government agencies have the authority to share PCEHR information using the consent mechanism. However individuals do not have a clear understanding of the boundaries for their consent given the ever-expanding PCEHR system, apparent fluidity and future government plans for the data as published in the media. In the context of a more transparent framework illuminating the nature of the privacy and security architecture implemented by the system, there needs to be a reconsideration of the quality of consent, including whether it is informed, unbundled, voluntary, revocable and explicit in all relevant respects. Modelling of potential risks and hazards, and observations about mitigation measures and their likely effectiveness, visible to patients and their advocates, representatives or advisers, should form a larger part of the 'informed' part of the discussion.
13. Many commentators seem to make provocative or disparaging statements about patient engagement with the system. For example, the President of the Australian Medical Association, Mr Hambleton has been quoted as saying to patients that do not wish to engage with the PCEHR system "…you need to opt out and get out of the way … we just want the rabid consumerists to get out of the way and let's just get on with it."[6] High handed comments like this are not useful, and demonstrate overt disrespect of patients/consumers, and lack of appreciation that engaging directly with the concerns of the most sensitive and vulnerable is an accepted way to make the system adequately safe and fit for purpose for everyone. Potential patient and consumer distrust of the ethical use of information stored on the PCEHR by practitioners is a key risk for the whole enterprise. The institutional and professional stakeholders need to be encouraged to accept that trustworthiness is the necessary precondition for trust, and the best way of demonstrating trustworthiness is by transparent exposure of the basis of the system as it actually operates, warts and all, with security and privacy mechanisms for patient interests particularly clearly illuminated. To date, much of the consumer information provided has been more

like PR material, aiming mainly to reassure and persuade consumers that they should sign up, emphasizing benefits rather than the unvarnished truth about both strengths and weaknesses of the system. NB: There is already at hand an alternative medical industry model in Patient Product Information disclosures, which are obliged to refer to and put in context possible risks, side effects and contraindications to enable the patient to make their own informed choice about what risks to accept. This model of more neutral, complete and explicit explanation of all the considerations necessary to make a balanced personal choice should become the model of PCEHR information, not the current PR/spin approach aimed at downplaying any counter-considerations.

14. The PCEHR system is not transparent and relies upon a series of fragmented, historically problematic and related legislation to devolve security and privacy responsibilities to a range of contractors and sub-contractors beyond the Crown and its agents, down through to the patient/consumer. Crown authorities are not accountable for any quality matter linked to adverse patient care outcomes related to PCEHR implementation. The absolution of the Crown from these penalties is deeply concerning to many individuals. While it may seem convenient to the Crown, it should be noted that this is not a viable basis for any other entity to operate the system, and as a matter of both trustworthiness and competitive transparency, the Crown should, like any commercial operator, accept that they should be liable for foreseeable, preventable hazards arising from their 'owning' (planning, designing, implementing) the system as a whole. ''All care but no responsibility, don't call us if something goes wrong" is no longer a basis for trust in the new digital environment.

15. Patients and consumers are concerned by Government stewardship of a centralized information source over which the Crown controls access, complaints resolution and information accuracy, but where they have no liability. Potential Crown abuses of the data as a source of revenue in the current economic climate cannot be ruled out.[7] Unresolved problems in law, such as the lack of a right to sue for breach of privacy, and the failure of the Privacy Act to adequately address electronic medical records issues, and the apparent lack of an overarching framework for personal information security and privacy of electronic medical records within which the PCEHR must fit, must both be resolved for these concerns to be addressed. Additionally, as noted above, Mandatory Data Breach Notification (Privacy Alert) laws must be passed immediately, ideally on a general basis, at the very least for the PCEHR.

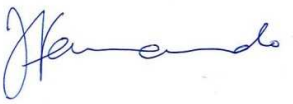
16. Support for the PCEHR will be enhanced if development is seen to be informed by international best practice (for example OECD work regarding the privacy aspects of EHRs). A PCEHR system subject to Freedom of Information legislation would be helpful in building this trust. Uptake of the PCEHR by consumers/patients will be fostered if those people can see that their interests are being recognised and that system registration is not misrepresented by health authorities regarding enrolment. Alternatively, if their interests are not recognised, and the implications of enrolment are not met with wide support and consensus, it is appropriate that many may decline to give consent until this is rectified.

17. The PCEHR system design and current useage have been cast by the legislation and regulations supporting it. The legislation acts as a barrier to the interests of

improved consumer/patient security, privacy and health outcomes. The community recognises and has broadly adopted these concerns, so a review and amendment to this legislation is likely to be a necessary foundation for the success of a new iteration of the PCEHR.

We would be happy to provide further information or evidence for these observations, and look forward to a change to participate in a more open and consultative design review for PCEHR 2.0, should a decision be taken to pursue it.

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 a 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. Australian Privacy Foundation. Splash page. http://www.privacy.org.au/

2. Kruys, E. Your e-health record – a good idea? (Video) 4/11/2013
http://doctorsbag.wordpress.com/2013/11/04/your-e-health-record-a-good-idea-video/

3. Connolly, B. Victorian Department of Health slammed in ICT system audit; CIO.com: 30 October 2013
http://www.cio.com.au/article/530432/victorian_department_health_slammed_ict_system_audit/

4. Anonymous. Comment 2, Public Statement: PCEHR, the Australian Privacy Foundation in D, More; The Privacy Foundation is not happy with government regarding the PCEHR; others also have concerns. 3 November 2013.
http://aushealthit.blogspot.com.au/2013/11/the-privacy-foundation-is-not-happy.html

5. Berner, E.S & Moss, J. The practice of Informatics; Informatics challenges for the impending patient information explosion (Viewpoint Paper). J Am Med Inform Assoc. 2005;12:614-617 doi:10.1197/jamia.M1873

6. PulseITMagazine.com.au. Mechanics of PCEHR are driving us mad": AMA. Pulse IT; 20 August 2012:pp.24-25

7. Jeremy Hunt plans sale of confidential patient medical records to private firms
http://www.telegraph.co.uk/health/healthnews/10250585/Jeremy-Hunt-plans-sale-of-confidential-patient-medical-records-to-private-firms.html