Australian Privacy Foundation

enquiries@privacy.org.au

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

21 December 2011

APF submission to Inquiry into the provisions of the Personally Controlled Electronic Health Records Bill 2011 and a related bill.

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. I write as Chair of the Health Sub Committee of the APF. I refer to the Community Affairs Legislation Committee Inquiry into the Personally Controlled Electronic Health Records Bill 2011 and the Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011.

Our submission is organised in two Sections. Section one is a summary of our submission; section two details this in full.

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 the 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

Section 1

Executive Summary

The APF welcomes this opportunity to influence much needed eHealth Bills in Australia. Government focus on these endeavours is to be applauded. Examples of effective programs exist overseas and we are anxious to learn from them. An effective Australian eHealth system existed in many States and Territories prior to the commencement of work on the national PCEHR system. We are keen to see our eHealth system function at least as effectively as other useful International programs. Thus our feedback on the system enshrined in the Bills is summarised below.

1. The APF is concerned that reverse engineering of governance issues at the heart of the PCEHR system will adversely affect health professional and patient use of such.
2. The APF believe it is crucial that Non-Government funded citizen Organisations (NGOs) are offered permanent advisory roles on governance bodies that will probably be established post PCEHR system roll-out, as has been mooted during discussions with health authorities this year.
3. The APF maintains that the Bills require governance benchmarks so that citizens may verify PCEHR system performance, security and privacy functionality themselves, independently of Government agencies.
4. The APF is not comfortable as to the conflict of interest that Government employees must manage under the Bills should an individual citizen be concerned about unauthorised access to their IHI, PCEHR and associated data.
5. The APF asks that minimum terms, rights and responsibilities for individuals' and healthcare providers' participation in the context of the PCEHR system are legally specified in the Bills.
6. The APF is concerned that the proposed PCEHR standards mash-up will trigger a cascade of costs and barriers that health practitioners, island-Australian software manufacturers and the community will be forced to suffer, while individual patients will suffer adverse health errors due to the resultant loss of data confidentiality, integrity and availability.
7. The APF enquires whether the Australian Government, and so all tax payers, will bear the industry and health practice costs of failed PCEHR system standards implementation.
8. The APF requests information about what else, other than standards, will be compromised in order to meet the PCEHR system deadline of July 2012.
9. The APF believes it is fundamentally important, in keeping with patients' basic rights, that the absolution of Government jurisdictions and their agents is removed from the Bills. Misuse of the data must be subject to consequences, especially given many unwilling patient participants at Lead Sites. The right to litigation when unfairly impacted by another's action occurs in the general community and is supported by the recent ALRC review of Privacy laws**.** The Bills need to reflect community standards of accountability.
10. The APF asks to be informed of the total expenditure figure Government has invested thus far and will invest in the PCEHR system to July 2012.
11. The APF is concerned by the influence of the failed IHI implementation and the retention of local systems combined with the PCEHR overlay on quality patient care outcomes and clinician training and workload. Neither Bill specifies benchmarks or independent bodies to measure these factors as outcomes. We ask that the Bill be amended to specify such benchmarks and to ensure the information is publicly available rather than confidential or outside the scope of Freedom of Information requests to NEHTA, as often occurs at present.
12. The APF is concerned that the Bills do not embody informed consent arrangements and that citizens are not being advised by federal authorities about the breadth and depth of data Australian Governments hold, use, disseminate and data mine about individuals without consent.

13. The PCEHR system embedded in the Bills is a document viewing service and not a patient care system at all. The APF questions marketing efforts to convince patients and practitioners otherwise[2-4]. The APF therefore asks how the system, which cannot uniquely identify individuals and simply permits document transmission and viewing, will be used for patient care benefit at all.

14. The Bills still do not define the term "health provider". The APF wonder precisely who will and will not be able to use the PCEHR system; this includes summaries of patient care information via the Internet for those unable to directly connect to individual patient electronic health records.

15. The APF has been alarmed to note recent press reports suggesting the PCEHR system ought to be "opt out" rather than "opt-in". The reports, which quote many prominent Australians, suggest the proposed PCEHR system architecture enabled by the Bills, are not generally understood. If the PCEHR system is "opt out" then all health practitioners will be forced to register for the PCEHR system as health providers and citizens alongside individuals from the broader community. The current PCEHR system architecture cannot function as an "opt-out" system.

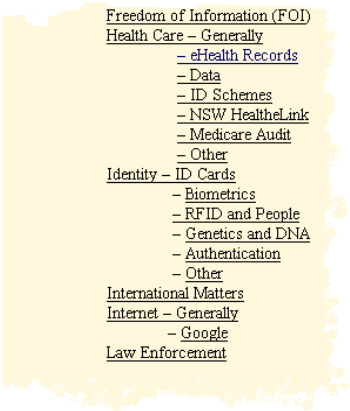
16. Finally, neither Bill details the eHealth services that will actually be achieved by July 2012. It is better to get this Government initiative right than to meet an arbitrary deadline. Everyone is a health consumer so getting a national eHealth system wrong would be very costly in terms of public perception of the Government and set our national eHealth agenda back several years. The Bills should refer to actual deliverables and benchmarks over and above simply enabling a PCEHR system experiment with clinicians and the broader community in living laboratories.

Section 2

Introduction

International experience has demonstrated that a systematic and transparent approach must be taken to privacy compliance in order to achieve a trustworthy PCEHR system upon which patients and health workers can rely [(1)]. The APF has made many attempts to communicate with the national E Health Transition Authority (NEHTA) and the Department of Health and Ageing (DoHA) in systematic and transparent ways over several years, as the partial screenshot from our website, below, illustrates. Despite claims to the contrary, effective consultation (i.e. meaningful two way communication) with consumer advocacy NGOs began to occur and then ceased in 2011 - that is for a period of less than a year, while Government plans to deliver a national PCEHR system have been in place for more than five years. In this context, the "the Personally Controlled Electronic Health Records Bill 2011" and "the Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011" are disappointing.

Selected APF Papers Sorted by Policy Topic



http://www.privacy.org.au/Papers/indexPolicies.html

Screenshot 1: Section of more than 2 e-pages of APF letters, submissions and papers sorted by "Health Care"

I have attached copies of pertinent APF policy documents and previous submissions regarding the PCEHR Draft Legislation, the PCEHR Concept of Operations and a letter to the Minister of Health, NEHTA and DOHA to this submission to avoid repeating APF feedback previously submitted to health authorities on the key issues [(2-5)]. The three submissions were made to the Department of Health and Ageing in 2011 and the letters to the Minister and other senior health authorities were also sent during 2011. All of these and further related documents are publicly available on the APF web site. Despite their exclusion from the body of this submission, matters raised therein are of vital importance. We request consideration of these papers as supplements to this submission.

This submission focuses on five key themes. They are poor governance, "Island Australia" standards, Government agent's immunity from responsibility, the quality of patient care and growing Government stewardship of centralized information about its citizens. Each topic is covered in a section listed below.

Governance

Neither of the Personally Controlled Electronic Health Records Bill 2011 and the Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011 (the Bills) outlines the governance framework which has informed their development let alone the PCEHR system development itself. Motherhood statements and general governance principles are documented without any form of operationalisation. The matter of governance, a concept at the heart of successful project planning, has been largely overlooked until late 2011. Governance concerns are at the core of initial project planning processes rather than a concept that can be retrofitted once a system has been designed.

1. The APF is concerned that reverse engineering of governance issues at the heart of the PCEHR system will adversely affect health professional and patient use of such.

The Bills enable the minister to make PCEHR rules, requires the Information Commissioner and the PCEHR System Operator to report annually and provides for a review of the first two years of the operation. However there is no indication in the extensive Bills of system benchmarks or ways governance success or failure of the system may be judged and no scientifically valid evidence is referenced either. For instance, all Australian were issued with an Individual Health Identifier (IHI) number, which links to personal and health information, in July 2010 and these have been downloaded in batches by various health professionals for local use. The local use includes saving the records to practice information systems and circulating them to colleagues, many of whom in turn save them to their own computerised information systems, mobile phones and computer tablets. The majority of patients, let alone health authorities and other health professionals, are unable to measure or control all locations where information about an individual is actually stored at present. Thus, effectiveness of the PCEHR system cannot be measured by IHI download rates or use in health settings because there are no valid boundaries for such enquiry.

Discussions with health authorities this year suggest that advisory bodies will be formed to evaluate the effectiveness of the PCEHR system after July 2012. We believe it is vital to include Non-Government funded citizen Organisation (NGO) representatives on these advisory bodies to avoid perceptions of a conflict of interest. Such appointments would also demonstrate Government confidence in the PCEHR system.

2. The APF believes that it is crucial that Non-Government funded citizen Organisations (NGOs) are offered permanent advisory roles on governance bodies that will probably be established post PCEHR system roll-out.

Governance is a key system benchmark yet thus far patients have been forced to rely upon press releases or Government-linked websites for all information about the privacy and security of the health information about themselves. Conversely Government health authorities are able to store, use, uncontrollably disseminate and access such data. Current IHI evidence is unreliable for governance research and assessment purposes, and no other performance benchmarks have been publicly revealed. Frankly, the IHI Bills and the current Bills before the Senate suggest that citizen expectations about their power to understand where health and personal information about them is stored no longer exists in Australia.

3. The APF maintains that the Bills require governance benchmarks so that citizens may verify PCEHR system performance, security and privacy functionality themselves, independently of Government agencies.

We are alarmed to understand that Government agencies, as specified in the Bills, will steward all information stored in one's PCEHR, one's IHI and all data from the Centrelink and Medicare megamerger. There is a history of poor governance in the context of managing Australian health data [(3)]. For example, in late 2011 the Federal Court found that Medicare had illegally merged patient health and personal data. Medicare also faced (and probably still does) a plethora of accusations about the way their investigations are handled [(6)]. The weakened frameworks will enable linked data storage of two or more discrete information systems storing personal and health information to be co-located in the same data base (see above). Yet the Government is working to diminish protections embedded in Professional Services Review legislation so Federal Court challenges to database mergers of indexed health information may not continue. [(6)] Such diminishment erodes citizen rights to privacy and security as a fundamental human right.

The heavily publicised audit proposals embedded in the Bills take no account of human factors or of the fact that current audit systems, upon which the proposed Bills rely, are dysfunctional. One simply needs to look at the evidence to see that health authorities either amend legislative frameworks to authorise presently illegal data hosting requirements (see above) or ignore these concerns completely, as per the following example. An attached submission outlines instances of where patient information stored in pharmacies dismally failed recent Australian National Audit Office (ANAO) audits yet DoHA failed to act because it had received no direct complaint made by an individual patient[(2-4)]. Individuals can only ever discover such a breach under the proposed PCEHR system Bills if the Government agency employee with whom they make such enquiries judges that it is appropriate to pass on the information. Anecdotally, we understand that health authorities have acted to ensure that news of such breaches is not publicly available[(20)]. We ask whether individuals enquiring about their own records will be subject to similar censorship. The Bills ensure that Government employees, as

public custodian of the data, are inextricably conflicted in the context of breach enquiries and Government plans to advance the PCEHR system.

Further, in APF experience, information breaches are often discovered months after occurrence and can foster litigation. The community expect DoHA and other Government agencies to control breaches, such as in the instance of the pharmacy example above, on their behalf rather than await individual complaints before taking action. Suggestions, as with changes to the Professional Services Review discussed above, magnify our concern as to the community's right of action

4. The APF is not comfortable as to the conflict of interest that Government employees must manage under the Bills should an individual citizen be concerned about unauthorised access to their IHI, PCEHR and associated data.

The Bills do not explain minimum terms, rights or responsibilities for individuals' and healthcare providers' participation in the PCEHR system. There are no complaints mechanisms embedded in the Bills. Individuals will not be able to directly access audit information about their PCEHR system records except via the Government and its agencies[6]. The APF is distressed to note that when Government agencies do not comply with robust legal governance frameworks it is the protection such frameworks offer to people that are weakened as a result, to the cost of their individual human rights.

5. The APF asks that minimum terms, rights and responsibilities for individuals' and healthcare providers' participation in the context of the PCEHR system are specified in the Bills.

Standards

International standards are a non-negotiable foundation of the complex PCEHR system. Standards define record formats (that is the range of fields to be populated by end-users), vocabulary and terminology, syntax, the seven machine layers for a health message to move between locations, hardware requirements and all the business processes at every point in the interoperability chain. Despite ongoing concerns expressed by the Medical Software Industry Association (MSIA) and the Australasian College of Health Informatics(ACHI) as well as consumer advocacy groups such as the APF as to the requirement for a single international standard to underpin the establishment of the national PCEHR system, NEHTA's Tiger Teams and other agencies such as the International Health Terminology Standards Development Organisation (IHTSIDO) have attempted to retrofit these to the PCEHR system architecture[7-9]. The Tiger Teams were initiated as a way to devise useful national eHealth standards[10]. As of November 2011, the Tiger Teams had not met, yet ostensibly managed to harmonise several very complex standards for an Australian EHR by month's end. This unseemly rush undermines community trust in the local and International standards that were allegedly harmonised without a governance framework. We wonder what other aspects of the project will have to be compromised like this to meet the 1 July 2012 deadline. The rushed mash-up of several different national and international standards ostensibly underpin the system, which could lead to medico legal liabilities and dangerous outcomes for patients.

The standards mash-up is potentially costly for clinicians in other ways too. Anecdotal evidence suggests not all health organisations, especially private practitioners and specialists, will opt-in to the system. Patient care will be based on this "mish-mash" of standards and computer operating systems that the evidence shows have not ever been able to exchange data effectively[1]. Indeed, we understand this issue remains vexed in the current PCEHR lead site settings. There are currently nine lead sites, or health care organisations, trialling the PCEHR system across Australia. The mash-up will diminish Data Confidentiality, Integrity and Availability (data-CIA) so that records stored in the PCEHR system will provide an unreliable basis for patient care, as occurred with the doomed Health Care Summary project in the UK [1]. Unlike the definition of data integrity expressed in the Security and Access Framework document, and presumably a foundation of the PCEHR system, data integrity actually incorporates the accuracy and completeness of information and processing methods and is not simply a measure of tamper-proof communication systems[11-12]. The Bills show no evidence of a common understanding of what is required to underpin a PCEHR system that patients and clinicians can trust.

This diversion from a single International standard will result in an "island Australia" PCEHR system. Australian industry, patients and health professionals will be confronted by a series of cascading costs and barriers as the direct result of the bridges planned between current systems and those required to use the PCEHR system [9]. Australian business will be unable to function competitively in an international setting whereby one standard applies locally and another applies overseas. Patients who choose to do so will not be able to link to their

supposed electronic health record (EHR) from other countries. Current multinational research and business entities working on ways to exchange health data between countries will be hampered. Suppliers of hardware and software are likely to face an inefficient and incompatible system that adversely impacts on return on investment (ROI) and, in terms of the domestic software industry, may even result in business failure if companies work to develop applications for Australian eHealth.

Proposed PCEHR system standards are likely to lead to increased costs for medical practitioners looking to bridge current practice software, which complies with an earlier data exchange standard, to new mash-up PCEHR system standards. The issue is magnified when, at a later stage, clinicians will have to upgrade systems once more to work to a single, effective International standard for global health information exchange. Even practitioners that do not opt into the PCEHR system in the first instance will be caught up in this concern.

Also, a patient may have registered for a PCEHR on 1 July 2012, but the health professional they consult may not yet be capable of entering data on to that patient's electronic record. The Bills do not contain any provision to address this very real and likely dilemma but the community will need to manage the issue through Government agencies post July 2012. This unwieldy process will be foisted on the Australian community regardless of the very real concerns outlined herein.

The Bills do not discuss standards for the exchange of information on mobile information and communication technology (ICT) platforms or cloud computing protocols. Anecdotal and research evidence indicates the application of these tools is pervasive in patient care settings for two reasons. Firstly, in public hospital settings, clinicians often avoid reliance on shared, computing equipment with applications that do not communicate with each other on the single machine let alone other computers in the same room or building[13]. Secondly, clinicians require evidence at the point of patient care. However the application of these tools place clinicians and the health organisations in a grey medico-legal situation that only litigation will clarify. This is an untenable situation that has been forced on clinicians and patients due to ongoing disregard of such useful tools in national eHealth Bills, both proposed and in existence.

6. The APF is concerned that the proposed PCEHR standards mash-up will trigger a cascade of costs and barriers that health practitioners, island-Australian software manufacturers and the community will be forced to suffer, while individual patients will suffer adverse health errors due to the resultant loss of data-CIA.

7. The APF asks whether the Australian Government, and so all tax payers, will bear the industry and health practice costs of failed PCEHR system standards implementation.

8. The APF requests information about what else, other than standards, will be compromised in order to meet the PCEHR system implementation deadline of July 2012.

Immunity from responsibility

The Bills ensure the Government and associated agencies are devoid of any responsibility for adverse health errors, stolen or misused data from centralised databases and practitioner ICT systems. As indicated in an earlier submission to DoHA, the move allows Government departments and contractors to continue conducting their living laboratory experiment, as represented by the PCEHR system Bills, without concomitant responsibility for their actions[2]. Based on feedback received via the community and mentioned in earlier submissions to NEHTA and DoHA, the pre PCEHR system implementation experiment depends on findings from research involving many unwilling patient-participants at the Lead Sites. The APF questions the approach of those who devised the Bills in a way that the National Health and Medical Research Council (NHMRC) has deemed as unethical[14].

Recently the former minister, the Honourable Nicola Roxon, attempted to address these concerns. However her statement to the press indicated that the Government has not changed its position, but has merely talked around the edges of a mismatch between community standards of responsibility and those held by the architects of the PCEHR system[15]. Yet we know that 85% of Australians are unhappy about carelessness with their data privacy and security; around half of these are prepared to litigate in instances of data breach[16]. A key finding from the recent Australian Law Reform Commission (ALRC) review of the national privacy regime highlighted the need to legislate a private cause of action where an individual has suffered a serious invasion of privacy[19]. Regardless, the Bills ensure the Government and employees of the Government cannot be held to account for their PCEHR and IHI system actions, while contractors may well not be liable either. If

Government and associated agencies and contractors require different provision arrangements from others then these need to be specifically articulated in the Bills. The blanket exemption for the Government and their agents totally disregards community standards of accountability.

9. The APF believes it is fundamentally important, in keeping with patients 'basic rights, that the absolution of jurisdictions and their agents are removed from the Bills. Misuse of the data must be subject to consequences, especially given many unwilling patient participants at Lead Sites. The right to litigation when unfairly impacted by another's action occurs with the general community and is supported by the recent ALRC review of Privacy laws[19]. The Bills need to reflect community standards of accountability.

Quality of patient care

The APF is concerned about the quality of patient care outcomes if the PCEHR system is founded on the IHI database. A recent security paper auspiced by NEHTA states that due to lack of confidence in the capacity of the IHI to uniquely identify patients, they will also be allocated parallel, service provider identifiers to ensure clinicians work on the right patient with the right information at the right place, at the right time [17]. Accordingly, the Government has authorised a system for mandatorily and uniquely numbering all citizens from birth to grave for one purpose, whereas the architects of the PCEHR propose to use the IHI for a contradictory purpose. The contrary purpose will magnify existing confusion in clinical settings where at least two identifiers will apply to every patient and may actually increase rates of adverse health error.

The IHI concern is exacerbated by new, machine-based, standard clinical terminologies Australian health workers will have to learn in order to use the PCEHR system at all. Along with medical and other health training requirements, Australian health workers must now learn a new discipline – the PCEHR system clinical terminology. Given ongoing reliance on local practice systems, reliable individual health records will depend upon the effective application of double language. Also, health workers will be forced to double-handle all patient care records in the context of unhelpful budgetary and productivity constraints[13]. One process will be used to care for patients and the other will be used to satisfy the machine requirements of PCEHR systems. The bi-lingual and double-handling nature of the proposed system in addition to the imposition of machine-based clinical terminology on time-poor health workers seems likely to foster data fragmentation and data-CIA errors, key concerns which the PCEHR system was ostensibly designed to address.

The adverse outcomes are particularly likely in the context of overwhelming eHealth workforce shortages across the sector. The shortage has fostered development of the Australian Health Workforce Institute (AHWI). Aside from research into the subject, the APF is not aware of any training endeavours actually initiated by the AHWI in the context of the shortage. While acknowledging the importance of research and development work, we would argue the reality of the PCEHR system and the lack of suitably qualified workforce are contraindicative issues that take precedence over academic research endeavours at present. Real patients and real clinicians will be relying on the PCEHR in real life from July 2012. Our analysis of Government expenditure to support the Australian health workforce shows this has been minimal and ineffective thus far. Anecdotally for instance, we understand that Australian medical students do not know what the PCEHR system is yet let alone clinical terminologies and neither are taught in any clinician training syllabus. This lack of knowledge and the workforce vacuum are bound to adversely impact on eHealth quality of care outcomes for many years to come.

An analysis of electronic practice has recently commenced based research networks in NSW. The analysis suggests there is evidence to support ideas about increased rates of patient care error when clinicians depend upon eHealth systems without valid and reliable data quality assurance mechanisms "and suffer an interoperability problem where information aggregated from diverse systems may be misinterpreted because of different meanings and contexts for care"[18, 21]. The report suggests "routinely collected electronic health care data [is] aggregated into large databases [that] are increasingly being mined, linked and used for audit, continuous quality improvement in clinical care, health service planning, epidemiological study and evaluation research"[18]. That is, the databases are not simply being used to improve patient care outcomes but also provide a fertile source of information for health administration, planning and research. The PCEHR overlay seems likely to amplify concerns linking error to data quality concerns. The mixture of uses may hamper the reliability of care information stored on the systems. The findings of researchers' investigations seem to suggest a plausible relationship between increased reliance of clinicians on some eHealth systems for patient care and adverse health effects.

After spending untold amounts of tax payer funds, Australian health care is likely to prove as dysfunctional post PCEHR system implementation and with as many "rail gauge" issues as occurred previously.

10. The APF asks to be informed of the total expenditure figure Government has invested thus far and will invest in the PCEHR system to July 2012.

11. The APF is concerned by the influence of the failed IHI implementation and the retention of local systems combined with the PCEHR overlay on quality patient care outcomes and clinician training and workload. Neither Bill specifies benchmarks or independent bodies to measure these factors as outcomes. We ask that the Bill be amended to specify such benchmarks and to ensure the information is publicly available rather than confidential or outside the scope of Freedom of Information requests to NEHTA, as often occurs at present.

Government stewardship of centralized information

The APF has noticed a trend towards increased Government stewardship of centrally managed and often co-located identified or identifiable information about all Australian citizens. Our concern about the mega-merger of Medicare and Centrelink data is exacerbated when one considers PCEHR records that are linked to the Medical Benefits Scheme, the Pharmaceutical Benefits Scheme, organ donor and childhood immunisation register. As our submission suggests, Government spokespersons have agitated for weaker privacy legal frameworks to enable linked data storage of two or more discrete information systems storing personal and health information to be co-located in the same data base too (see Governance, above).The APF therefore enquires about the existence of informed consent arrangements in the Bills to underpin such mega-mergers of information and about mechanisms to publicise the details of the centralisation to Australian citizens.

12. The APF is concerned that the Bills do not embody informed consent arrangements and that citizens are not being advised by federal authorities about the breadth and depth of data Australian Governments hold, use, disseminate and data mine about individuals without consent.

Miscellaneous and conclusion

13. The PCEHR system embedded in the Bills is a document viewing service and not a patient care system at all. The APF questions marketing efforts to convince patients and practitioners otherwise[2-4]. The APF therefore asks how the system, which cannot uniquely identify individuals and simply permits document transmission and viewing, will be used for patient care benefit at all.

14. The Bills still do not define the term "health provider". The APF wonder precisely who will and will not be able to use the PCEHR system; this includes summaries of patient care information via the Internet for those unable to directly connect to individual patient electronic health records.

15. The APF has been alarmed to note recent press reports suggesting the PCEHR system ought to be "opt out" rather than "opt-in". The reports, which quote many prominent Australians, suggest the proposed PCEHR system architecture enabled by the Bills, are not generally understood. If the PCEHR system is "opt out" then all health practitioners will be forced to register for the PCEHR system as health professionals and citizens alongside individuals from the broader community. The current PCEHR system architecture cannot function as an "opt-out" system.

16. Finally, neither Bill details the eHealth services that will actually be achieved by July 2012. It is better to get this Government initiative right than to meet an arbitrary deadline. Everyone is a health consumer so getting a national eHealth system wrong would be very costly in terms of public perception of the Government and set our national eHealth agenda back several years. The Bills should refer to actual deliverables and benchmarks over and above simply enabling a PCEHR system experiment with clinicians and the broader community in living laboratories.

References

1. Jolly, R. (2011) The e health revolution—easier said than done; Research Paper no. 3 2011–12. Parliamentary Library, Parliament of Australia. http://www.aph.gov.au/library/pubs/rp/2011-12/12rp03.htm
2. The PCEHR Draft Legislation, Submission to Dept of Health and Ageing (27 Oct 2011). http://www.privacy.org.au/Papers/DoHA-PCEHRBills-111027.pdf

3. The PCEHR Concept of Operations, Submission to NEHTA (30 May 2011). http://www.privacy.org.au/Papers/NEHTA-ConOps-110530.pdf
4. The PCEHR Concept of Operations - Addendum, Submission to NEHTA (7 Jun 2011). http://www.privacy.org.au/Papers/NEHTA-ConOps-Add-110607.pdf
5. eHealth – Consumer Consultation and Project Governance, Letter to DoHA (18 Apr 2011). http://www.privacy.org.au/Papers/PCEHR-DoHA-Ltr-110417.pdf
6. Dearne, K. Senate calls for delicate Medicare merger. The Australian, November 1 2011.
7. Medical Software Industry Association (MSIA) Submission on Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system 7th June 2011 http://www.yourhealth.gov.au/internet/yourhealth/blog.nsf/3BB39556BFEE97C2CA2578D9001E9106/$FILE/Medical%20Software%20Industry%20Association%20submission.pdf
8. Australasian College of Health Informatics (ACHI) (2011) Response to Request for Comment on the Draft PCEHR Concept of Operations, Original May 2011 (V1.0), Updated June 2011 (V1.2) http://www.achi.org.au/docs/ACHI_Response-PCEHR_ConOps_V1.2.pdf
9. National E-Health Transition Authority (NEHTA) PCEHR Standards. http://www.nehta.gov.au/ehealth-implementation/pcehr-standards
10. Gidden, J. (2011) NEHTA rounds up tiger teams. http://ehealthspace.org/news/nehta-rounds-tiger-teams
11. National E-Health Transition Authority (NEHTA) (2011) NESAF Release 3 Business Blueprint (S1131) Version 3.0 — 20111130 Final. National E-Health Transition Authority Ltd, ACT, Australia
12. Cheong, I. (1996). Privacy and security of personal health information. Journal of Informatics in Primary Care, 15-19.
13. Fernando, J. & Dawson, L. (2009) The health information system security threat lifecycle: An informatics theory. International Journal of Medical Informatics 78(12)
14. National Health and Medical Research Council (NHMRC) Guidelines for research involving humans. http://www.nhmrc.gov.au/health-ethics/human-research-ethics
15. Dearne, K (2011) Australian Privacy Foundation slams e-health liability law. The Australian, November 1.
16. Colley, A. (2011) Unforgiving Aussies are willing to act on privacy breaches. The Australian, November 8.
17. National E-Health Transition Authority (NEHTA) (2010) NEHTA Security and Access Framework, http://www.nehta.gov.au/component/ docman/doc_download/877-securityand-access-framework)
18. Liaw, S-T., Harris, M., Zwar, N., Powell-Davies, G., Comino, E., Dennis, S., Bunker, J., & Jalaludin, B. (2011) The UNSW electronic Practice Based Research Network. http://notes.med.unsw.edu.au/CPHCEWeb.nsf/page/UNSW+EPBRN
19. Australian Law Reform Commission (ALRC) Privacy law and practice; ALRC Report 108. http://www.alrc.gov.au/inquiries/privacy
20. National E-Health Transition Authority (NEHTA) (2010) Healthcare Identifiers service implementation approach http://www.nehta.gov.au/connecting-australia/healthcare-identifiers
21. Liaw, S.T (2011) Decision support systems: A general practice research journey. Australian Family Physician Vol. 40, No. 9, September

Australian Privacy Foundation

.

enquiries@privacy.org.au

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

APF feedback about the exposure draft PCEHR Bill 2011 (PCEHR Draft Bill) and exposure draft PCEHR (Consequential Amendments) Bill 2011

October 27 2011

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. I write as Chair of the Health Sub Committee of the APF. Our response to your request for community feedback on the "Exposure Draft PCEHR Bill 2011 (PCEHR Draft Bill) and exposure draft PCEHR (Consequential Amendments) Bill 2011" is detailed below.

The APF submission does not explicitly respond to all concerns as these have been addressed in several previous PCEHR draft system submissions and in our policy documents (1-5). The policy documents are attached for your information. Therefore the focus of this submission is simply to add new analysis of key privacy issues from the individual citizen's perspective.

We reiterate our position that it is completely unacceptable for any critical privacy protections to be in delegated legislation.

All protections must be in statutes, in order to ensure that they have been considered and directly expressed by the Parliament. Delegating them to statutory instruments makes them appear unimportant. It also risks them never being delivered, and enables the protections to be readily compromised by subsequent amendments that can be processed without publicity and without consideration by the Committee process or the Parliament.

In short, the credibility of such protections as are being proposed is shot to ribbons by the failure to put them high on the agenda. The Department is greatly undermining its own scheme by its intransigence on this matter alone.

Regardless, any statement in either Bill suggesting that consumers can directly review their own health information is misleading. Such statements will seriously erode consumer trust in the system once they have direct experience of such. Research findings indicate the lack of patient trust in an electronic health system has dire consequences for clinician trust in and the effectiveness of such schemes (6, 7). Logically then, misleading information contained in the Bills will erode the effectiveness of the Australian PCEHR system.

As all previous submissions suggest, APF concerns centre on 4 major themes: lack of definition, lack of evidence to support assumptions made in the Bills, quality of care and ineffective legislative issues. We are concerned that without any real-life, duplicatable evidence the notion of social value pervading the Bills presupposes a potentially dangerous scientific validity i.e. that there is privacy versus quality-of-health-care pendulum and that to get good health care one must swing the pendulum against privacy. This is simply not the case and moreover, in the context of the PCEHR Draft Bill and Consequential Amendments Bill, is seriously damaging to the quality of patient health care outcomes more generally.

New and specific concerns

New and specific concerns with the Bills are as follows:

1. The legislation does not contain an adequate definition of "health provider".

   The APF asks that the term "health provider" is properly and adequately defined in the legislation.

2. The legislation excludes any discussion of new and emerging technologies, such as cloud computing, smart phones and tablets. These may pose privacy or security risks to an individual's health and personal information or clinical files. Patients and their clinicians need to feel confident applying such innovations to health care data. This is not the case at present.

   The APF maintains that the legislation must specify guidelines or standards to enable the application of new and emerging technology to the PCEHR system.

3. The legislation permits health services to download PCEHR system data and store it on their own clinical information services. Researchers will be able to apply to human ethics committees to override consent using Section 95 and 95A of Australian Privacy Law to obtain PCEHR data directly from health service systems rather than from the Department of Health and Ageing (DOHA) or its agencies (8). This is of particular concern given the Public Interest Determinations (PIDs) 11 and 11A that currently permit the collection and use of contact details of genetic relatives to enable disclosure of genetic information. Recent moves to renew temporary PIDs10 and 10A that permit the collection by health service providers of third party health information that

is relevant to a patient's family or social medical histories, without the third party's consent, are also concerning (9). The megamerger of Centrelink, Medicare and DHS without a privacy impact assessment exacerbates matters (10). Data exchanges of this nature will not manifest in the proposed technical audits of PCEHR system records. The community will have no ability to know of or control access to their PCEHR data.

The APF requests that legislative guidelines be incorporated into the Bills to control researcher access to PCEHR system data stored on health services' clinical information systems for secondary purposes without consumer knowledge or consent.

4. No Government can be sued or prosecuted for any harm or damage resulting from the Legislation and its implementation. No employee of these jurisdictions can be sued or prosecuted for any harm or damage resulting from the Legislation and its implementation. The APF believes that all sanctions for data breach contained in the draft Bills absolve all governments and their agents from any responsibility for personal or clinical information.

The APF believes that absolution of all Governments and their agents from responsibility from data breach should be removed from the draft Bills. It is unacceptable to absolve government jurisdictions from accountability to the community.

5. The APF asks for detail of the circumstances of deliberate data breach and asks precisely how this might occur in the context of an ordinary (not eminent) citizen's PCEHR system data.

The APF asks that deliberate acts of PCEHR system data breach are defined in the draft Bills.

6. No health service, or health professional or clinician can be sued or prosecuted for any harm or damage resulting from the Legislation and its implementation if government authorities decide no deliberate data breach occurred. Penalties outlined in the Bill are therefore unenforceable and so are irrelevant.

The APF asks for penalty details in the context of unintentional breaches of community information linked by the PCEHR system. Such penalties would include, but not be limited to, compensation to the aggrieved parties, the availability of class action in the case of major breaches to lower costs to individual plaintiffs, and to assure means are put in place to reduce the re-occurrence of breaches in the future. The latter measure would be binding upon the breaching agent.

7. Which body or organisation will be held into account in the instance of dangerous or malicious hacks of centralised databases, such as the Individual Health Identifier database, that are linked by the PCEHR system? If one accidentally kills someone on the road or accidentally walks out of a

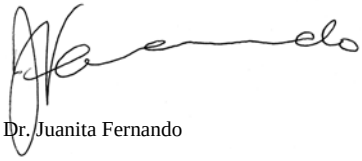
shop without paying for goods, one must still face consequences. The same is true of breaches to health data.

The APF maintains that all breaches of health data, regardless of their nature or context, must be subject to consequences for those involved in the breach.

8. **Finally, the APF supports the submission made by David More regarding all governance issues and other relevant matters**.

Our clear impression is that health authorities remain "rearranging deckchairs on the Titanic" rather than grappling with the real life privacy and security issues generated from all of our previous submissions and questions regarding the PCEHR system ConOps and supporting legislation.

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 the 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. Telstra security exonerated in mailing list error ITWire Jul 7, 2011 5:04 PM (15 hours ago) http://www.itnews.com.au/News/262961,telstra-security-exonerated-in-mailing-list-error.aspx
2. Brettingham-Moore, C. "Pharmacy-held data security questioned." Medical Observer, June 4 2010.
3. "Smartcards to give patients records control". ABC News. !2 July 2011. http://www.abc.net.au/stories/2011/07/12/3267328.htm
4. Wilcox, AB., Yueh-Hsia Chen & Hripcsak, G. "Minimizing electronic health record patient-note mismatches" JAMIA 2011;18:511-514 doi:10.1136/amiajnl-2010-000068
5. Hilvert, J. "Commissioner eyes tough e-health privacy laws". Jul 14, 2011. http://www.itnews.com.au/News/263561,commissioner-eyes-tough-e-health-privacy-laws.aspx
6. Senate Official Hansard http://www.aph.gov.au/hansard/senate/ dailys/ds150310.pdf
7. Fernando, J. & Dawson, L. (2009) The health information system security threat lifecycle: An informatics theory. International Journal of Medical Informatics 78(12)
8. More, D. "I Think I Have Now Worked Out Why The PCEHR is A Fundamentally Flawed Idea! See If You Agree". July14 Australian Health Information Technology Blog, Thursday, July 14, 2011 http://aushealthit.blogspot.com/
9. Greenhalgh T, Stramer K, Bratan T, Byrne E, Russell J, Hinder S, Potts H. The Devil's in the Detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace programmes. London: University College London; 2010.
10. East, M. 'AHPRA owes doctors an apology, inquiry finds', australiandoctor.com.au, 3 June 2011, http://www.australiandoctor.com.au/news/2f/0c070f2f.asp
11. Security and Access Framework http://www.nehta.gov.au/component/docman/doc_download/877-security-and-access-framework

Australian Privacy Foundation

.

enquiries@privacy.org.au

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

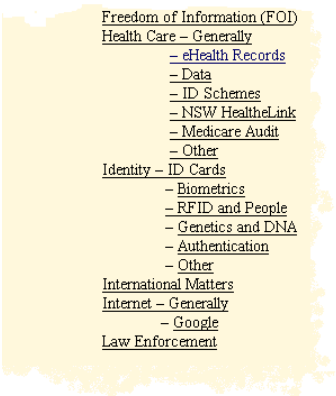
APF feedback about the Draft Concept of Operations (ConOps): Relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) system.

30 May 2011

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. I write as Chair of the Health Sub Committee of the APF. I refer to "the Draft Concept of Operations (ConOps): relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) system".

Experts have long indicated that a systematic and transparent approach must be taken to privacy compliance in order to achieve a trustworthy PCEHR system upon which Australians can rely (1). The APF has made many attempts to communicate with NEHTA and the Department of Health and Ageing in systematic and transparent ways over several years, as the partial screenshot from our website illustrates. Despite claims to the contrary, effective consultation (i.e. meaningful two way communication) with consumer advocacy NGOs began to occur in 2011. In this context, the "Draft ConOps: relating to the introduction of a PCEHR system" is disappointing.

Selected APF Papers Sorted by Policy Topic
http://www.privacy.org.au/Papers/indexPolicies.html



Screenshot 1: Section of more than 2 e-pages of APF letters, submissions and papers sorted by "Health Care"

This submission comprises 2 sections. Section 1 outlines fundamental problems with the National E-Health Transitional Authorities' (NEHTA's) approach to the ConOps. Section 2 details key deficiencies of the proposals contained within the Draft.

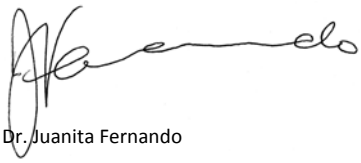
The APF submission does not explicitly respond to all concerns although we do raise several broad issues that may concern other stakeholders. The primary focus is to analyse privacy issues from the individual citizen's perspective. Our clear impression is that health authorities are resisting the need to embrace the broader informed community with anything but public relations projects; we await continued and meaningful consultation.

The APF is disconcerted by the lack of a governance framework in the draft ConOps. Work on the framework will occur throughout the third quarter of 2011, after enabling legislation has been introduced to Parliament (2). Key questions need a response prior to introducing the legislation. These concern:

1. Who will hold what type of health and personal information?
2. Who will be authorised to send, read, write, print, download and otherwise access the information? How will such authorisation occur?
3. How will data quality be assured?
4. How will private information be protected?
5. What evidence suggests the draft PCEHR system will make a difference to community concerns about answers to these questions?
6. Who is ultimately responsible and accountable for the draft PCEHR system?

The draft ConOps and accompanying Consumer Booklet do not explicitly address community unease about the baseline of all information government authorities may hold on citizens although many of these may be indexed in future system builds, as illustrated in Figure 1. The draft PCEHR system is unlikely to improve community health outcomes although, as the figure does show, it looks likely to prove useful to government agencies, insurers and researchers.

Yours sincerely



Dr. Juanita Fernando

Chair, Health Sub Committee
Australian Privacy Foundation

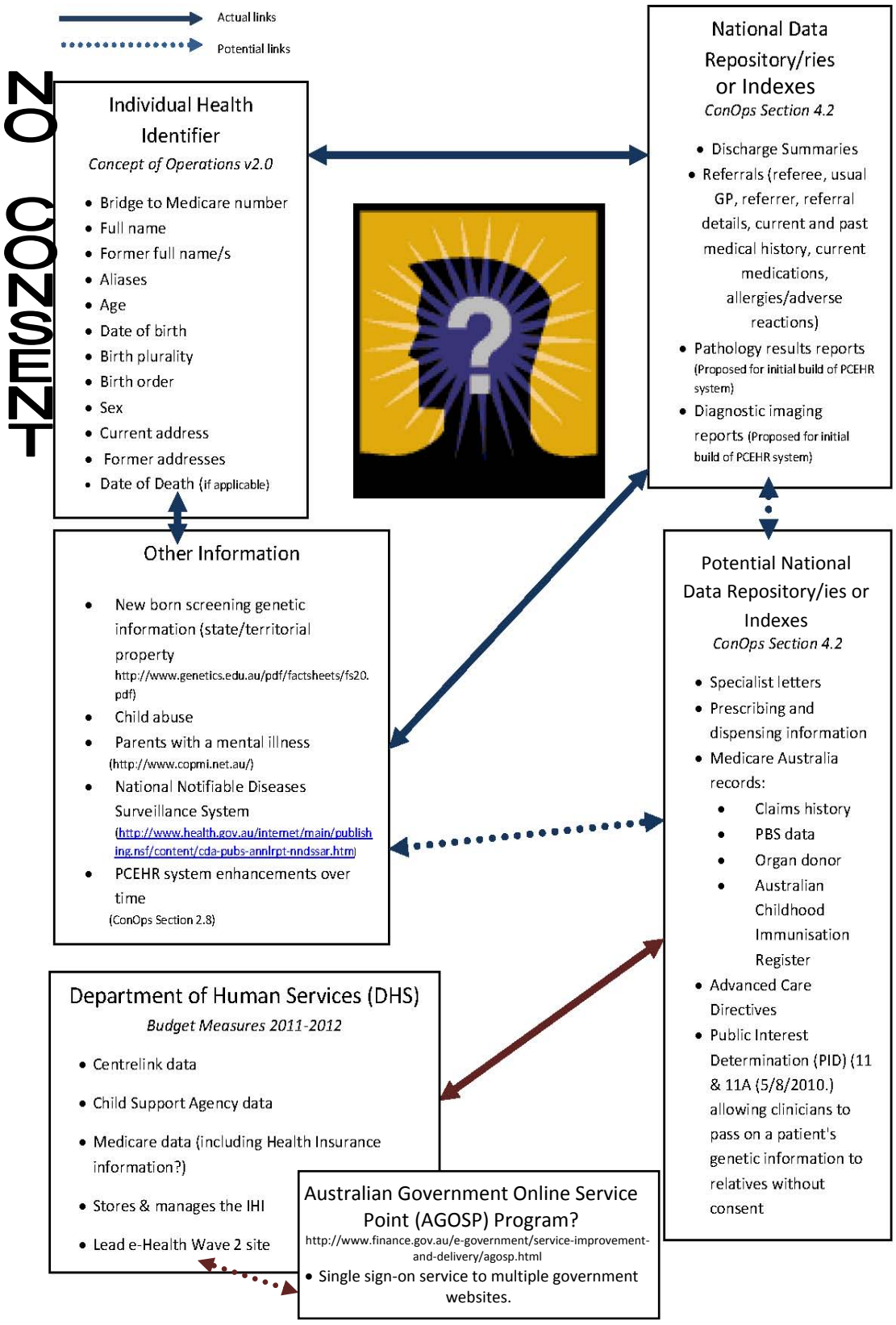
Dr Fernando is in Medicine, Nursing & Health Sciences
Monash University 03 9905 8537 or 0408 131 535
mailto:Juanita.Fernando@monash.edu

Dr Fernando is a 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. NHHRC, "A healthier future for all Australians - Final Report June 2009" (http://www.health.gov.au/internet/nhhrc/publishing.nsf/Content/nhhrc-report)
2. Draft Concept of Operations relating to the introduction of a personally controlled electronic health record (PCEHR) system. Consumer, Healthcare, Provider, ICT Industry, and Policy Consultation Report January to April 2011, NEHTA.

Figure 1: Identified information about citizens held and/or indexed by Australian government health authorities in PCEHR system May 2011.



Section 1: The ConOps approach

The lack of a coherent governance framework in the document lies at the heart of the APF submission on the draft ConOps. The development of such a framework would address the key privacy issues that are likely to influence individual enrolments into the system. It would also provide an opportunity to depoliticize various stakeholder discussions about the PCEHR system. Our health authorities seem to have learned nothing from the largely unsuccessful British national electronic health record system (1). Plans to design our PCEHR system without embedding it into a plain-English and transparent governance framework need urgent reassessment if we hope to create safer, more efficient and sustainable health care services for all Australians.

These governance shortcomings indicate that the draft PCEHR ConOps does not achieve our understanding of the key aim of a Concept of Operations document. A Concept of Operations is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system (3). The PCEHR ConOps does not achieve this aim and stakeholders are not made aware of prospective system characteristics that will inform the outcomes they actually need from an electronic health record. The ConOps is confusing to read and obscures important issues. Document sections and sub-sections are supported by important information embedded in figures and tables only and by a bewildering multitude of cross-references to other parts of the same document. Rather than an informative Concept of Operations document, the draft PCEHR ConOps is excessively complex and seems intelligible only to "insiders".

The ConOps seems to prime Australians to re-set their expectations as to the deliverables funded by their investment of the $467 million in the PCEHR system. We are very concerned where patient control and consent will actually start and stop in relation to using the initial build of the PCEHR system. Government control of all personal and health information about citizens, some of this consensual, is depicted in. "*Figure 1: Identified information about citizens held and/or indexed by Australian government health authorities in the PCEHR system May 2011*". The APF is disturbed by the breadth and depth of information about individuals the PCEHR system plans to store or index without a clear governance framework upon which to base informed consent processes.

We can't see how the draft ConOps resembles or relates to the PCEHR system described in the National E-Health Strategy (2). The ConOps indicates that the range of citizen data stored in the PCEHR system may expand in unknown ways using unspecified methods for future undefined refinements. We have no access information about actual PCEHR pilot project plans, protocols, data models or evaluations. The draft ConOps for the PCEHR system signals an even more confusing era of access to private citizen information by clinicians, health organisations and many authorities than at present. While some attention is paid to clinical governance matters in isolation, such as accreditation, the overall governance framework for the PCEHR system and e-health nationally has not been devised. Work on an overarching governance framework, rather than the much needed detailed plan, will occur during a few months in late 2011, after enabling legislation has been introduced to Parliament. In short the Draft ConOps seems to be hastily conceived in such as way as to meet the scheduled implementation date of July 2012 rather than to inform stakeholders about how the system will function in real life.

REFERENCES

1. iHealthBeat, "Audit Slams British EHR Program for Being Largely Unsuccessful" http://www.ihealthbeat.org/articles/2011/5/18/audit-slams-british-ehr-program-for-being-largely-unsuccessful.aspx
2. National E-Health Strategy, http://www.health.gov.au/internet/main/publishing.nsf/content/national+Ehealth+strategy
3. Concept of Operations, http://en.wikipedia.org/wiki/Concept_of_Operations
4. Draft Concept of Operations relating to the introduction of a personally controlled electronic health record (PCEHR) system. Consumer, Healthcare, Provider, ICT Industry, and Policy Consultation Report January to April 2011, NEHTA.

Section 2: Privacy issues

This section lists the important elements overlooked or euphemized by the draft ConOps.

1. *Enabling legislation*

   At a recent Roundtable meeting in Melbourne, the APF asked for further information about the national repository service, including potential data sources, from both private and public health organisations, and enabling legislation to support the repositories. NEHTA has advised that:

   > "*Legislative issues relating to repositories are currently being assessed by Australian governments (i.e. Commonwealth and States and Territories). Proposed legislative approaches to these issues will be the subject of public consultation." (12)*

   The APF and other stakeholders were advised that a legislative issues paper is due in June 2011, with four week turn-around for comment. The exposure draft of legislation to support the creation of the PCEHR, the national repository service and consequential legislative amendments by July 2012 is scheduled for August to September2011. At least one public meeting will be scheduled before the PCEHR system legislation is introduced to Parliament, scheduled around October 2011. Consumer feedback will be drawn from patients at lead e-health implementation sites to inform PCEHR system design. State and federal law harmonization will not occur in time for initial PCEHR system build. **While not directly related to the draft ConOps document, the APF maintains the rushed implementation schedule and lack of access to hard data will impede the ability of individuals and organisations to provide meaningful, reflective and considered feedback to health authorities.**

2. *System governance*

   Evidently, "*the PCEHR long term governance framework will be agreed and in place through the last quarter of 2011/2012*" (13). Plans to design a governance framework after enabling legislation has been introduced to Parliament are disturbing. We raised the urgent need for an inclusive, formal and long-term governance framework for consultation at the recent Four Corners Roundtable in Sydney (5). The draft ConOps describes an advanced state of the PCEHR system design, lead sites are already working with the system (in the context of patient care) and the legislative implementation schedule is proceeding rapidly. The health authorities will spend only a few months devising the governance framework for a system that hopes to change the face of Australian healthcare forever. The community are unlikely to have faith in, or trust, the PCEHR system without a methodical, well planned governance framework at its heart. **In line with the APF's Policy Statement, the PCEHR system is not likely to attain key aims stated in the draft ConOps unless a detailed, formal governance framework that includes representation from NGO consumer advocacy groups occurs before the draft system and consequential amendment bills are tabled in Parliament**.

3. *Trial methods and outcomes*

   We are surprised to note that the scheduled implementation date evidently takes precedence over establishing the solid governance framework that ought to have been decided before the IHI and other PCEHR system building blocks were established. A key outcome from the Melbourne roundtable indicates several matters fundamental to ensuring a practical PCEHR system are currently under discussion. Important information about patient and clinician analyses of the system at lead sites will not be publicly available. The APF and other organisations and individuals will be denied access to real data to inform decisions about PCEHR system analyses. **The APF is concerned that keeping information about fundamental matters from the public domain will hamper community trust in the PCEHR system and may actually jeopardise the entirety of Australian national e-health efforts.**

4. *National repository service*

   The national repository service referred to throughout the ConOps is not explicitly discussed in the document. The current draft may be interpreted to indicate the repositories will store information about the community without their consent. The APF put this question to NEHTA at the Melbourne Roundtable and has been formally advised:

"*The PCEHR National Repositories will only hold information on behalf of the PCEHR System in relation to enrolled individuals*" (12).

We suggest this matter be more clearly addressed in future iterations of the ConOps, brochures and material designed to support community enrolments into the PCEHR system.

5. *Data fragmentation and extra work*

On the one hand the ConOps indicates that PCEHRs will address data fragmentation as a business driver. Data fragmentation is linked with adverse health outcomes and refers to silos of de-contextualised information that is stored in a variety of locations fostering uncoordinated decision-making processes (1). On the other hand the draft states the PCEHR system will not replace existing fragmented health information and communication (ICT) systems. Evidently it will impose additional layers on existing local and Territory and State based health information infrastructure. Recent comment from an Australian Medical Association (AMA) representative at the Clinician-Consumer Roundtable meeting in Melbourne suggested that workflow issues have not been considered in the draft ConOps. The representative said that if the PCEHR system added to time constraints between doctor and patient (i.e. if a clinician is forced to see fewer patients per work shift due to PCEHR system demands) then doctors won't use the system at all (12). The imposition of additional work is unlikely to be embraced by clinicians, especially those in private practice, so that – as experienced in the UK – many clinicians may ultimately ignore the system completely and health information will remain as fragmented as it was previously (2).**In the absence of workflow information in the draft ConOps, the APF maintains that models describing the PCEHR system in the context of clinical workflow and patient care outcomes should be urgently addressed by NEHTA prior to the initial system build.**

A review of the Con Ops shows the PCEHR is not intended to replace local patient identifiers and practice records and so ensure the right treatment is given to the right patient at the right time (3**).** Local health services will continue to rely on same, fragmented combination of information technology used presently. **The APF submits that the ConOps needs to state how the introduction of a parallel system will end data fragmentation and ensure the right treatment is given to the right patient at the right time.**

6. *Personal control*

Section 3.2.1 of the draft ConOps indicates that patients will be able to view all elements in their PCEHR and can tailor clinician views according to authorisation. Section 2.8 of the draft and recent stakeholder meetings suggests much of this control will occur during future refinements scheduled at unspecified points of time (12). Unless people have some control of data on entry, they are being treated as 'dumb terminals' themselves. Equally, the quality of the 'original' data in this context is unchecked and therefore unverified: it is dangerous to assume that existing data is accurate when establishing an entirely new data regime. **The ConOps should explain in plain-English what level of personal control consumers will actually have in the initial build of the PCEHR, that is, as of July 2012.**

7. *Error correction*

Error correction, enquiry and complaints arrangements outlined in the Draft ConOps are very dangerous to the health and wellbeing of the Australian community. The arrangements are manual and depend upon the individual affected reporting their concerns to a PCEHR Operator. The Operator will then initiate an enquiry and redress these accordingly. What medico-legal processes have been established to manage situations such as when the patient record on the PCEHR system conflicts with the local record or when an error is stored on the system and there is no local record at all? This question is particularly significant in emergency situations and when patient care depends upon the Consolidated View of a record in the system. Information indexed through the PCEHR system may not ever provide a reliable information source for patient care. **The APF suggests that a mechanism to warn clinicians about potential human error embedded into the PCEHR system must be clearly outlined in the ConOps and needs to occur prior to July 2012.**

8. *List of implementations for initial PCEHR build*

The document makes no coherent statement as to what Australians can expect from the initial build of the PCEHR system. Neither does it guarantee to incorporate all of the ideas the draft contains.

However section 9 does refer to "evidence-based implementations" as an important step in an ongoing evaluation process. Logically, proposed system enhancements will be informed by these evaluations. Health authorities ought not to change the PCEHR system as desired without reference to due process or open and transparent debate. NGO consumer groups must be involved in developing the metrics to inform Key Performance Indicators (KPI) that will be applied to the evaluations. This is especially important to those evaluations assessing the qualitative and quantitative realisation of benefits around better healthcare and improved satisfaction of individuals receiving healthcare.

The APF asked NEHTA about NGO consumer group involvement in devising the KPI metrics applied to ongoing system evaluations at the recent Melbourne meeting (12). The formal response we received was as follows:

> *"The Benefits Partner will be involved in the Change and Adoption consultation activities and will be consulting with end users to assess the benefits and evaluation criteria".*

The response does not answer the question adequately. NGO consumer group involvement in devising the KPI metrics should be added to the tender document that potential Benefits Partners will address.

The ConOps should:

1. **Itemise the benefit individuals can expect to receive from the PCEHR as of July 2012 and**
2. **Embed NGO consumer group consultation processes in the Benefits Partner tender document discussing proposed enhancements to the system.**

9. *"PCEHR" or "the PCEHR system"*

Terms "PCEHR" and "the PCEHR system" seem to be used interchangeably throughout the ConOps. Is there a distinction between the terms – i.e. does PCEHR refer to a singular record not attached to the mooted system or is this simple a consistency error? **Terms need to be harmonized throughout the ConOps or, if we are referring to two unique terms, each must be operationalized accordingly**.

10. *Health insurance*

According to briefings received at the Four Corners Roundtable held in Sydney recently, health insurers will be able to ask patients whether or not they have enrolled in the PCEHR system and vary premiums accordingly (5). Is this the case? If so, we feel such arrangement need to be manifest in the draft ConOps. **The APF believes the draft must clearly inform the community of this matter so that individuals can decide whether this decision contravenes the spirit of government moves to ensure health care insurers will not use any PCEHR system information for the management of claims or to determine eligibility.**

11. *Pseudonyms and Medicare benefits*

Hansard shows the government believes pseudonymous care will not impose a requirement that healthcare providers use an IHI when providing healthcare services, nor will identifiers be required for claiming healthcare benefits (4). Anecdotally, we understand that some patients have been denied a Medicare benefit because they used a pseudonym to obtain health care. Pseudonymous care is the only option open to many people wanting to protect identities for the purpose of their health and wellbeing (e.g. battered wives). Many of these people need the rebate in order to afford clinical care in the first instance. Pseudonymous care is totally different to anonymous care, as reiterated at the Melbourne meeting (12).Evidently a patient can apply to the Individual Health Identifier (IHI) Service Operator for a pseudonym and is then provided with a new identifier linking to the actual IHI. How will this process relate to claims for healthcare benefits? No information about the process of obtaining a pseudonym or healthcare benefits for pseudonymous care is currently available in the ConOps document. **We believe it is very important for the draft ConOps to be revised in order to show how the management of pseudonymous care will function with regard to the IHI, the PCEHR and claims for healthcare benefits.**

12. *Genetic data and storage*

The draft makes no reference as to whether genetic data is managed in the same way as other key health information about individuals. We believe newborn babies will automatically be opted into the PCEHR without parental consent (5). The information stored about newborns in the PCEHR is likely to comprise genetic information from the "heel prick" test. There are radically different, existing rules

throughout Australian States and Territories as to the storage of (and access to) "heel prick" data: the draft appears to assume that all such individual rules will be overridden by the first build of the PCEHR system. However we have learned that processes to harmonise the existing privacy rules throughout Australia will not occur before July 2012 (12). **We submit that the draft ConOps should explain to the community the way genetic data will be managed in the initial PCEHR system build.**

Also, genetic profiling is increasingly influencing Australian health care outcomes, as supported by a recent Public Interest Determination (6). The issue of whether genetic data should be stored in an individual's health record or indexed via national repositories to personalise medicine is already being discussed in the peer reviewed literature. **The issues of overridden consent in some instances and genetic data storage overall are factors that must be discussed in the ConOps so that all Australians may reflect on potential risks in the context of information stored in the PCEHR system.**

13. *Length of data storage*

Several speakers at the Four Corners Roundtable in Sydney stated that information will be stored in the PCEHR system for 110 years (5). What will occur to the stored data after this period? **The APF is surprised the ConOps neither mentions the arrangement nor discusses data disposal measures.**

14. *Access rules*

The document also does not explicitly outline everyone who will have access to the stored data, under what rules. This is particularly confusing with regard to emergency access. Information we received during several stakeholder meetings have explained there will be no way to override exclude lists or the lack of a PCEHR enrolment on the one hand, yet the Draft ConOps takes a contradictory position (5). We understand that legislative concerns with regard to emergency access provisions are still being discussed, but this cannot be comprehended by anyone reading the draft. **The APF believes that the community requires a clear explanation of emergency rules in the context of clinician access to the PCEHR system before the initial build is decided.**

The Con Ops suggests authorised representatives of an HPI-O, who may view a record, will not be identified on the system. The draft system will also permit patient information to be downloaded and printed by HPI-O staff. The document also states that health organisations will be responsible to pass protective obligations through all inter-connecting system parts along with the data. Yet evidence suggests no such responsibility may apply in real life situations, as the following example indicates. Serious information breaches were reported to the Department of Health and Ageing in the context of Medicare Australia's administration of the PBS link in pharmacies last year. The pharmacies evidently took no action. The Department argued the breaches were not their concern and took no action either (11). **The APF maintain that technical audit arrangements outlined in the draft document make no reference to human factors and are unacceptable at this stage.**

15. *The IHI*

The Individual Health Identifier (IHI) is the bridge that links information to the PCEHR system and the national repositories. According to Hansard records, the IHI was passed to replace the allocation of patient identifiers by each service provider (7). We now know this is not the case and that parallel identifiers will be allocated to patients along with the IHI as means of ensuring patient identification (8). Accordingly, the government has authorised a system for mandatorily and uniquely numbering all citizens from birth to grave for one purpose, whereas the architects of the PCEHR propose to use the IHI for a contradictory purpose. The contrary purpose will magnify existing confusion in clinical settings and may actually increase rates of adverse health error. **We submit that the matter of compulsory numbering for all Australians must be returned to Parliament for review in light of this function creep to ensure the health safety of all Australians.**

16. *NHHRC report*

The PCEHR system, as currently designed, distorts findings from the National Health and Hospitals Reform Commission Report, June 2009, as to recommendations about the development of personally controlled health care records (9). The PCEHR Con Ops distorts the report findings beyond recognition. **We urge health authorities to revisit the NHHRC report with a view to implementing the Report's PCEHR system recommendations therein.**

17. *Consumer booklet*

The consumer booklet should be at the heart of the process of engaging the broader public with the PCEHR system; but this is not the case. The booklet should explain as clearly as possible, with text and simple diagrams, to consumers how PCEHR system information will be diced, controlled, moved around and used, at a big picture level. By contrast with the existing glossy consumer booklet, health authorities have an obligation to create such a document in order to enable a much broader understanding of the big picture of the proposed PCEHR system and its assumptions and risks. The structure of the national PCEHR system's governing model for access and use needs to be addressed in the booklet (and the ConOps), as do issues of whether all protective obligations pass through all inter-connecting system parts along with the data. The identity of the single role that is responsible for compliance and breaches should be identified too. **The APF maintains that the consumer booklet should be revised so it is made clear enough for everyone to grasp the essential parameters, rules and roles being proposed in the ConOps.**

REFERENCES

1. Fernando, J., & Dawson, L. (2009). 'The health information system security threat lifecycle: An informatics theory', Int. J. Med. Inform., pp. 815-826
2. Greenhalgh T, Stramer K, Bratan T, Byrne E, Russell J, Potts HWW. Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study. BMJ. 2010;340.
3. E-Health: Healthcare Identifiers Service http://www.health.gov.au/internet/main/publishing.nsf/ Content/pacd-ehealth-consultation
4. Senate Official Hansard http://www.aph.gov.au/hansard/senate/ dailys/ds150310.pdf
5. Four Corners Roundtable http://newsletter.nehta.gov.au/industry-brief/industry-brief-archive/archive/view/listid-4-industry-ezine/mailid-66-industry-brief-special-bulletin-march-2011
6. PID 11 and 11A._ Regarding the collection and use of contact details of genetic relatives to enable disclosure of genetic information without consent, dated 5 August 2010.)
7. The second reading of the Healthcare Identifiers Bill 2010 and the Healthcare Identifiers [Consequential Amendments] Bill 2010, Thursday June 24.
8. (NEHTA Security and Access Framework, http://www.nehta.gov.au/component/ docman/doc_download/877-security-and-access-framework)
9. A healthier future for all Australians - Final Report June 2009 http://www.health.gov.au/internet/nhhrc/publishing.nsf/Content/nhhrc-report).
10. Consultation Process re PCEHR, Further Letters to NEHTA Clinical Lead re PCEHR Process Matters, and to NEHTA CIO re PCEHR Design Issues. APF. (15 Nov 2010) http://www.privacy.org.au/Papers/NEHTA-PCEHR-Process-101115.pdf)
11. Brettingham-Moore, C. "Pharmacy-held data security questioned." Medical Observer, June 4 2010.
12. Consumer and Clinician Roundtable, NEHTA, Melbourne, May 25 2011.
13. Draft Concept of Operations relating to the introduction of a personally controlled electronic health record (PCEHR) system. Consumer, Healthcare, Provider, ICT Industry, and Policy Consultation Report January to April 2011, NEHTA.

Australian Privacy Foundation

.

enquiries@privacy.org.au

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

Addendum to the

APF feedback about the Draft Concept of Operations (ConOps): Relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) system. (May 30 2011)

5 June 2011

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

Thank you for extending the consultation period for submissions about the "the Draft Concept of Operations (ConOps): relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) system". We refer to an article published in the Australian newspaper "PCEHR technical details to be released" on Friday June 3 2011 and provide the following addendum to APF feedback (Section 1 and Section 2) about the draft ConOps document (1).

Section 1

Last week, the Australian newspaper reported on comments from National E-Health Transition Authority (NEHTA) chief executive Peter Fleming to suggest funding would be needed beyond 2012. NEHTA staff understand they will be required for "the long term", and in about two months, the board will review the business case for the funding (1). The draft ConOps does not outline system deliverables due by July 2012. The APF believe it is important for health authorities to outline in the ConOps the actual deliverables that will be funded by their investment of the $467 million in the PCEHR system.

Section 2

4. National Repository Service

The community should be able to understand the precise nature of the National Repository Service (NRS) and the way it will function to improve their health in the context of the PCEHR system. At a recent Roundtable

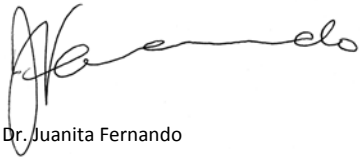
meeting in Melbourne, the APF was advised the NRS will index information from conformant repositories around the country (potentially tens of thousands) to inform the PCEHR system and that it will also house unnamed records with no other logical "home" (2). Mr Fleming recently suggested the NRS will be an indexing service so that clinicians or patients can obtain specific information (1). We are bewildered by various descriptions of the NRS, including the descriptions outlined in the draft ConOps text or embedded in illustrations. **The APF believes that, for the integrity of the ConOps process, it is mandatory that the exact nature and function of the NRS be clarified before the next iteration of the ConOps in order to inform community trust in national e-health frameworks.**

15. The IHI

When the APF attended a consumer roundtable meeting held in Melbourne earlier this year we were advised by health authorities that the IHI had not been used in a "live" environment due to concerns about patient safety (3). Mr Fleming is quoted in the recent newspaper report as saying that Tasmania has gone "live" with its IHI implementation in the acute care sector. Logically, we assume that concerns about the use of an IHI in the context of patient safety have been resolved over the last few months. However, neither we nor any other NGO to our knowledge has received relevant information on how concerns were/are bring managed. **The APF maintains that information about the application of the IHI to patient safety should be made publicly available to resolve community concerns about the number.**

We are glad to contribute this addendum to our submission on the draft ConOps for a PCEHR system.

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 is a 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. Dearne, K. "PCEHR details soon to be released." the Australian IT June 3 2011 http://www.theaustralian.com.au/australian-it/government/pcehr-technical-details-to-be-released/story-fn4htb9o-1226068848051
2. Consumer and Clinician Roundtable, NEHTA, Melbourne, May 25 2011.
3. Consumer Roundtable, NEHTA, Melbourne, February 9 2011

Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

17 April 2011

The Hon Nicola Roxon MP
Minister for Health and Ageing

Dear Minister

Re: eHealth – Consumer Consultation and Project Governance

I refer to the APF's letters to you dated 3 March and 7 March.

We note that, despite our request, you have failed to address this as a matter of urgency, and that you have not even responded within the 4-6 weeks that your office indicated at the time.

Your Department and NEHTA have both continued to actively avoid engagement with consumer advocacy organisations.

As you are well aware, the vast majority of consumers are ill-equipped to cope with the complexities of eHealth, and need representative and advocacy organisations to act on their behalf. You have chosen to prioritise a late and purely nominal consultation process with the general public over engagement with consumer advocacy organisations. Your actions make clear that you accord very low importance to the views of consumer organisations. Your statement that "We will work with all parties to ensure that a strong governance framework is in place [and] that governance will include consumers" therefore seems to have been at best a 'non-core promise'.

By withholding the ConOps document from consumer advocacy organisations for 9-12 months, and then making it available only when it was too late to reflect consumers' concerns, you have avoided the insights that the experienced people involved in those organisations would have offered.

Your behaviour makes clear that it was pointless for the APF to spend so much effort making constructive contributions to these projects. Instead it is necessary for us to invest our energies in making sure that the public understands that your Government's eHealth initiative is being devised in a manner hostile to the interests of consumers, and favourable above all to government agencies, insurers and researchers.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

Policy Position
eHealth Data and Health Identifiers

28 August 2009

http://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf

This document builds on the APF's submissions over the last two decades, and particularly during the last three years, in order to consolidate APF's policy position. It presents a concise statement of general Principles and specific Criteria to support the assessment of proposals for eHealth initiatives and eHealth regulatory measures.

The first page contains headlines only, and the subsequent pages provide further explanation.

General Principles

1 **Health care must be universally accessible.**

2 **The health care sector is by its nature dispersed.**

3 **Personal health care data is inherently sensitive.**

4 **The primary purpose of personal health care data is personal health care.**

5 **Other purposes of personal health care data are secondary, or tertiary.**

6 **Patients must be recognised as the key stakeholder.**

7 **Health information systems are vital to personal health care.**

8 **Health carers make limited and focussed use of patient data.**

9 **Data consolidation is inherently risky.**

10 **Privacy impact assessment is essential.**

Specific Criteria

1 **The health care sector must remain a federation of islands.**

2 **Consolidated health records must be the exception not the norm.**

3 **Identifiers must be at the level of individual applications.**

4 **Pseudo-identifiers must be widely-used.**

5 **Anonymity and persistent pseudonyms must be actively supported.**

6 **All accesses must be subject to controls.**

7 **All accesses of a sensitive nature must be monitored.**

8 **Personal data access must be based primarily on personal consent.**

9 **Additional authorised accesses must be subject to pre- and post-controls.**

10 **Emergency access must be subject to post-controls.**

11 **Personal data quality and security must be assured.**

12 **Personal access and correction rights must be clear, and facilitated.**

General Principles

1 **Health care must be universally accessible**. Access to health care must not be conditional on access to health care data or on demonstration of the person's status (such as residency rights or level of insurance)

2 **The health care sector is by its nature dispersed**. Health care is provided by thousands of organisations and individual professionals, each with a considerable degree of self-responsibility. The sector is far too large, and far too complex to be centrally planned. Instead it must be managed as a large, complex and highly de-coupled system of autonomous entities, each of which is subject to regulation by law, Standards and Codes

3 **Personal health care data is inherently sensitive**. Many individuals have serious concerns about the handling of at least some categories of health care data about themselves. Their willingness to divulge important information is important to their health care, but is dependent on them having confidence about how that information will be managed

4 **The primary purpose of personal health care data is personal health care**. The protection of the individual person is the primary function of personal health care data and systems that process it. The key users of that data are health care professionals

5 **Other purposes of personal health care data are secondary, or tertiary**. Public health is important, but is a secondary purpose. Administration, insurance, accounting, research, etc. are neither primary nor secondary but tertiary uses. The tail of health and public health administration and research must not be permitted to wag the dog of personal health care

6 **Patients must be recognised as the key stakeholder**. Government agencies and corporations must directly involve people, at least through representatives of and advocates for their interests, in the analysis, design, construction, integration, testing and implementation of health information systems

7 **Health information systems are vital to personal health care**. People want systems to deliver quality of service, but also to be trustworthy, transparent and respectful of their needs and values. In the absence of trust, the quality of data collection will be greatly reduced

8 **Health carers make limited and focussed use of patient data**. Health care professionals do not need or want access to their patients' complete health records, but rather access to small quantities of relevant information of assured quality. This requires effective but controlled inter-operability among health care data systems, and effective but controlled communications among health care professionals. Calls for a general-purpose national health record are for the benefit of tertiary users (administration, insurance, accounting, research, etc.), not for the benefit of personal health care

9 **Data consolidation is inherently risky**. Physically and even virtually centralised records create serious and unjustified risks. Services can be undermined by single points of failure; health care data isn't universally understandable but depends on context; consolidation produces a 'honey pot' that attracts break-ins and unauthorised secondary uses and creates the additional risk of identity theft; and diseconomies of scale and scope exceed economies

10 **Privacy impact assessment is essential**. Proposals relating to personal health care data and health care information systems must be subject to PIA processes, including prior publication of information, consultation with affected people and their representatives and advocates, and publication of the outcomes of the study. Designs for systems and associated business processes must be based on the results of the PIA, and implementations must be rejected if they fail to embody the required features

Specific Criteria

1 **The health care sector must remain a federation of islands**. The health care sector must be conceived as islands that inter-communicate, not as elements of a whole. Health care information systems must be conceived as independent services and supporting databases that inter-operate, not as part of a virtually centralised database managed by the State. Coordinating bodies must negotiate and facilitate inter-operability, not impose central schemes

2 **Consolidated health records must be the exception not the norm**. A small proportion of the population may benefit from linkage of data from multiple sources, primarily patients with chronic and/or complex conditions. Those patients must be the subject of consent-based, specific-purpose data consolidation. This activity must not apply to people generally

3 **Identifiers must be at the level of individual applications**. Each of the large number of dispersed health care information systems must use its own identifier for people. A system-wide or national identifier might serve the needs of tertiary users of personal data, but does little for the primary purpose of personal care, and it creates unnecessary risks for individuals

4 **Pseudo-identifiers must be widely-used**. Particularly when personal data moves between organisations, the maximum practicable use must be made of one-time-use and other forms of pseudo-identifiers, in order to keep people's identities separate from the data itself, and minimise the risk of personal health care data escaping and being abused

5 **Anonymity and persistent pseudonyms must be actively supported**. Anonymity is vital in particular circumstances such as ensuring that people are treated for sexually transmitted diseases. Persistent pseudonyms are vital in particular circumstances such as for protected witnesses, victims of domestic violence, and celebrities and notorieties who have reason to be concerned about such threats as stalking, kidnapping and extortion

6 **All accesses must be subject to controls**. Access to personal data must be subject to controls commensurate with the circumstances, including the sensitivity of the data and the potential for access and abuse of access. This requires identification of the category of person and in many cases of the individual who accesses the data, and authentication of the category or individual identity. However, the barriers to access and the strength of authentication must balance the important value of personal privacy and effective and efficient access by health care professionals

7 **All accesses of a sensitive nature must be monitored**. Non-routine accesses and accesses to particularly sensitive data must be detected, recorded, and subject to analysis, reporting, sanctions and enforcement

8 **Personal data access must be based primarily on personal consent**. The primary basis for access to personal data is approval by the person concerned. Consent may be express or implied, and may be written, verbal or non-verbal, depending on the circumstances. All accesses based on consent must be detected, recorded and subject to analysis, reporting, investigation, sanctions and enforcement

9 **Additional authorised accesses must be subject to pre- and post-controls**. All accesses that are not based on personal consent must be the subject of explicit legal authority that has been subject to prior public justification. All such accesses must be detected, recorded and subject to analysis, reporting. investigation, sanctions and enforcement

10 **Emergency access must be subject to post-controls**. Health care professionals (but only health care professionals) must have the practical capacity to access data in apparent violation of the personal consent principle, but must only do so where they reasonably believe that it is necessary to prevent harm to some person. All such accesses must be detected, recorded, reported and subject to analysis, investigation, sanctions and enforcement

11 **Personal data quality and security must be assured**. Data must be of a quality appropriate to its uses, and retained only as long as it remains relevant. Personal data in storage, in transit, and in use, must be subject to security controls commensurate with its sensitivity, and with the circumstances

12 **Personal access and correction rights must be clear, and facilitated**. Each person must have access to data about themselves, and access must be facilitated by any organisation that holds data that can be associated with them. Where appropriate, the access may be intermediated, in order to avoid misunderstandings and misinterpretation of the data. Where data is not of appropriate quality, the person must be able to achieve corrections to it

Australian Privacy Foundation

Policy Position

Protections Against eHealth Data Breaches

28 August 2009

http://www.privacy.org.au/Papers/eHealth-DataBreach-090828.pdf

Personal health data is by its nature highly sensitive, so unauthorised access and disclosure is of even greater concern than it is with other categories of data. Irrespective of what laws and norms might apply to data breaches generally, it is vital that clear and effective protections exist for personal health care data. The APF has accordingly adopted the following policy on the matter.

A **data breach** occurs when personal health care data is exposed to an unauthorised person, and there is a reasonable likelihood of actual or perceived harm to an interest of the person to whom the data relates.

1. **An organisation that handles personal health care data must**:

   (a) take such steps to prevent, detect and enable the investigation of data breaches as are commensurate with the circumstances

   (b) conduct staff training with regard to security, privacy and e-health

   (c) subject health care data systems to a programme of audits of security measures

   (d) when health care data systems are in the process of being created, and when such systems are being materially changed, conduct a Privacy Impact Assessment (PIA), in order to ensure that appropriate data protections are designed into the systems, and to demonstrate publicly that this is the case

2. **Where gounds exist for suspecting that a data breach may have occurred, the organisation responsible must**:

   (a) investigate

   (b) if a data breach is found to have occurred, take the further steps detailed below

   (c) document the outcomes

   (d) publish information about the outcomes, at an appropriate level of detail

3. **Where a data breach has occurred, the organisation responsible must**:

   (a) promptly advise affected individuals (and/or their next of kin or carers)

   (b) provide an explanation and apology to affected individuals

   (c) where material harm has occurred, provide appropriate restitution

   (d) publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information

   (e) advise the Office of the Federal Privacy Commissioner

4. **Where a serious data breach has occurred, the Office of the Federal Privacy Commissioner must**:

   (a) review the outcomes of any investigation undertaken by the responsible organisation

   (b) where any doubt exists about the quality, conduct its own independent investigation

   (c) publish the results of the review and/or investigation

   (d) add the details of the data breach to a publicly available register, including any decision made as the result of the investigation, in order to ensure that information is available to support informed public debate about protections for personal health care data

5. **Where a data breach occurs that results in material harm**, the affected individuals must have recourse to remedies, both under the Privacy Act and through a statutory cause of action