Australian Privacy Foundation

G.P.O. Box 1196
Sydney NSW 2001

enquiries@privacy.org.au

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

27 May 2014

Dear Minister Dutton,

Re: APF response to the findings of the Review of the Personally Controlled Electronic Health Record

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

Health records are an integral and essential part of any health care system. E-Health record systems offer the technical means to provide effective and efficient treatment of patients. Designing a useful e-health system to save lives, reduce hospitalisation and contain healthcare budgets means using technology to enhance clinician, institutional and patient trust in the source.

The findings of .the Review of the Personally Controlled Electronic Health Record (PCEHR), December 2013 has proven generally disappointing. Review findings offer clinician, institutional and legalistic perspectives rather than patient or citizen perspectives.

Fundamental management issues remain at the heart of a national e-health system and these must be resolved to meet the gap between end-user expectation and services the proposed national e-health system and the PCEHR or MyHR (My Health Record) can deliver. Finally, the APF concurs with Minister Dutton's comment while Shadow Minister, the PCEHR system, if it gains momentum, will continue to pour "good money after bad".

Experience with similar e-health megaprojects overseas (in particular the UK) that have experienced significant budget blowouts, major delays in implementation and low endorsement by stakeholders suggests that Government should think critically about claims made by PCEHR proponents in the Review.

The initial APF response is summarized below:

1. Findings allude to the need for transparency of the overall framework for privacy and security of the whole complex national medical e-records system, indicating a need for yet more bureaucratic frameworks to support this. A key contributor to the poor

output for so much input on the PCEHR/MyHR, and the trust deficit that appears to be manifesting now, was probably reluctance of health authorities to transparently negotiate and resolve the clinician and patient expectations around access, security and control along the way, and ensure that keeping everyone informed and satisfied with the choice being made was kept as a central priority. A lesson for next time, or for the e-health rescue mission on the horizon!

2. The review manages patient safety and clinical effectiveness as if these have no relationship to information security. This is **patently untrue**.

   E-Health information must address the basic tenets of information security to contain levels of unintended medical error and ensure both confidentiality and privacy. The tenets are data confidentiality, data integrity and data availability. Data is **confidential** when information is accessible only to those with the required level of authorisation, consistent with the trust placed by consumers in health service providers and the strong body of Australian law regarding the practitioner-patient relationship. Data **integrity** refers to the accuracy and completeness of information and processing methods. Data **availability** means that all authorised end users can obtain reliable information when and where it is required[1].

   Dutton review findings state that an individual's PCEHR/MyHR record "…may not contain accurate and reliable information about their health, but this should improve over time" (p31).

   This fact portends disastrous implications for patients, with no right to litigation involving the Crown or their agents. It also has the potential to impose substantial costs on the public and private health systems, which will carry the cost of harms due to defective information.

3. Many general practitioners and other clinicians currently use e-health software managed by other professionals. The application of this software is supports patient medical attention; utilization is generally restricted to a small set of end-users selected by, but excluding, the patient. The PCEHR/MyHR national system provides a summary of health information to registered clinicians. Patient rights to self-determination have been steam-rolled. These facts beg the following question - What benefit accrues to patients from registration in a national system that:

   - only provides a summary of health information, paid for by patients, to registered clinicians,
   - holds a rich database of 22 million personal records, more than 21 million of which are unlikely to be populated by health data.
   - is run and managed by the Federal government and
   - is exposed to the risks of the Internet?

4. The APF assumes the PCEHR/MyHR system is open because patients and health professionals require access to use it. But the system is designed on the assumption that end-users trust it based on the belief that health authorities have a beneficent outcome in mind. The governance framework has not been mapped nor described and there is no information about it that is publicly available. End-users are expected to trust the PCEHR/MyHR system, regardless of who manages it and how the MyHR system will change over successive governments. There is no information about the people or systems citizens are trusting. The APF maintains that "blind consent" is different from meaningful consent.

There is increasing recognition in international law and in emerging global e-health protocols (for example under the auspices of the OECD) that when dealing with health information there must be true consent. Instances of disregard of that consent have been highlighted by the APF in communication with the Office of the Australian Information Commissioner regarding the PCEHR and are likely to attract adverse comment from Europe, a key trading partner whose privacy regime is significantly in advance of Australia. Failure to address the concerns of consumers and other stakeholders will fundamentally erode support for PCEHR/MyHR in the same way as the Australia Card.

5. Notably, MyHR will be considered a dumping ground for information in much the same way as the PCEHR system has been (p.39 of Dutton review). According to Addendum 2 of the Review report (p.52), patient authored records will not ever be "seen" by registered clinicians and patients cannot ever "see" clinical notes. There is little exception to this and no information as to whether the patient can add data to these fields or not. At the same time the review report continues to rely on patients to update the validity of their records without transparency about information contained in the record. On one hand, patients are trusted to validate the records; while on the other hand, they cannot know what they are validating.
6. The report findings suggest transition to an 'opt-out' model for all Australians on their MyHR to be effective from a target date of 1st January 2015. This recommendation is subject to the completion of the minimum composite of linked Healthcare Identifier (HI) records, which are renowned for inaccuracy. The patient care errors first reported in reviews of the PCEHR will continue, as both systems will use the same flawed HI foundation.
7. The review findings point to a need for the establishment of clear standards for compliance for clinical users via a proposed Privacy and Security Committee populated by government funded organisations and groups. The APF argues non-government funded organisations must also have a place on this Committee. Their inclusion will among other benefits help to ensure that development is perceived as legitimate and is not captured by particular interests (especially IT solutions vendors) nor involve the closed circle that results in failed megaprojects and thence major embarrassment for governments.
8. Renaming the PCEHR to MyHR is simply an exercise in "arranging the deck chairs on the Titanic". There is nothing "Mine" about it; the record is about me but not mine. There was nothing personally controlled in the PCEHR system, and there will be nothing controlled by patients in the MyHR system.
9. The myGov web site, through which people will access the PCEHR/MyHR (p. 37), has already experienced a data breach debacle of mammoth proportions. The site managers have clearly demonstrated the government's inability to secure private information from the most basic threats, let alone from criminals[2]. This fact is supported by the findings of the Dutton Review, who point to community perceptions of NEHTA governance shortcomings and that governance has been "essentially non-existent" since handover of e-health to the Department of Health (formerly the Department of Health and Ageing) (p.79). Frankly, the APF is dismayed that the community is, in the first instance, being forced to "opt out" of a system that risks the privacy of all personal and health information and from which they can never delete records already been uploaded to the PCEHR/MyHR system by the Crown and its agents.

10. There are many unresolved challenges to be addressed before the community is forcibly enrolled in the PCEHR/MyHR system. Yet there are no plans to let consumers/patients know the answers to all their questions, including forcible enrolment so that they know what will happen next, how it will happen and how their privacy will be protected. They are entitled know what future governments may do with their data, including actions as occurred in the UK recently when the National Health Service offered Big Data harvested from the national e-health scheme about patients for sale to drug, insurance companies and others.[3]

11. The APF is alarmed to note that Review findings indicate private sector involvement in the MyHR system without clearly expanding upon this generality (p15). As pointed out by Greenleaf[1] (2010) *No legislation should ever allow a national identification system to be operated by the private sector. A fortiori, no legislation should allow such a step to occur without the full scrutiny of the legislative process. That the government is proposing that the control of the future health records of all Australians could be privatised at all, let alone without full Parliamentary scrutiny, is likely to greatly upset many Australians. It is the type of 'try on' that was found all through the Access Card legislation, and is now being trotted out again in the hope that no one will notice*[4].

12. Australians have already voted with their feet on the national e-health system. Despite the plethora of assisted registration processes in public hospitals and Centrelink offices across the country in 2013, the PCEHR has a history of consistently poor take up. The Dutton report findings clearly indicate that direct federal cost savings underpin the "opt out" function (pp.8-11 and 28). An informed community has chosen **not** to join the PCEHR system; they see no value in it.

    Individual self-determination doesn't seem important to health authorities, who are more worried about billions of dollars poured into the ill-conceived PCEHR than they are about patient welfare. In response to the failed PCEHR, the report findings recommend citizens be compelled to opt-out of the rebranded MyHR system, in the hope that the community won't notice for some time. Clinician or other health/welfare authorities will be paid to "tout" the system to patients (p28) damaging the trust bond needed to provide useful healthcare.

    Clinicians will be employed by the government to pass private citizen information on to the federal government. I find this business and marketing practice both patronising and questionable in a democratic country like Australia. (p.39)

13. As occurred with the introduction of the Health Identifier, the Dutton review resurrects the old Australia Card spectre. "Opt in" measures, rather than "Opt out" ones at least offer the community an opportunity to exercise their human right to self-determination.

    The Dutton report findings suggest transition to an 'opt-out' model should be effective from a target date of 1st January 2015. This recommendation is subject to the completion of the minimum composite of linked Healthcare Identifier (HI) records based on Medicare numbers, which are renowned for inaccuracy. As per usual, health authorities are rushing toward an implementation date without trials or a transparent governance framework. Patient care errors have been regularly reported in government reviews of the PCEHR (not publicly available) and will continue, as the rebranded PCEHR, now MyHR (My Health Record) will use the same flawed HI foundation. Please refer to the APF policy I have attached to this email and some excellent work written by Graham Greenleaf [3-4] about the HI number: At the time of

writing, Greenleaf's work concerns the HI but I believe it holds up in the context of PCEHR/MyHR "opt out" provisions.

The APF maintains that a well-balanced thought process has been absent in arriving at the report finding

Yours sincerely

Chair, Health Sub Committee
Australian Privacy Foundation

Dr Fernando is in Medicine, Nursing & Health Sciences, Monash University
Phone: 03 9905 8537 or 0408 131 535
Mailto:juanita.fernando@med.monash.edu.au
Contact Details for the APF and its Board Members are at:
http://www.privacy.org.au/About/Contacts.html

References:

1. Fernando, J. & Dawson, L. The Natural Hospital Environment: A Socio-Technical-Material perspective. *International Journal of Medical Informatics*, 83 (2014): 140-158
2. Grubb, B. (2014) Revealed: serious flaws in myGov site exposed millions of Australians' private informa[illegible] *SMH*, May 15. http://www.smh.com.au/it-p[illegible]serious-flaws-in-mygov-site-exposed-millions-of-australians-p[illegible]40515-zrczw.html
3. Ramesh, R. (2014) NHS pat[illegible]ailable for sale to drug and insurance firms; The Guardian. 20 January. http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy
4. Greenleaf[1], G. (2010) *A National ID system to put health privacy at risk*: Submission to the Community Affairs Legislation Committee Inquiry into Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010', March. http://cyberlawcentre.org/ipp/publications/2010_HI-CLPC-sub59-1003.pdf or http://www2.austlii.edu.au/~graham/publications/2010/CyberLPC_submission2.
5. Greenleaf[2], G. (2010) *Comparisons between the 'Australia Card' (1986-87), 'Access Card' (2006-07) and Individual Health Identifier (2009-) proposals as identification systems,* draft of March (appended to Health Identifiers submission in March 2010, above). http://cyberlawcentre.org/ipp/publications/2010_draft_IHI_OzCard_comparison_table.pdf or http://www2.austlii.edu.au/~graham/publications/2010/IHI_comparison2.pdf

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