Australian Privacy Foundation

http://www.privacy.org.au

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

28 October 2015

Jeanette Radcliffe
Secretary
Standing Committee On Community Affairs
Legislation Committee
Community.Affairs.Sen@aph.gov.au

Dear Ms Radcliffe

Re: Comments on the Health Legislation Amendment (eHealth) Bill 2015

This submission by the Australian Privacy Foundation (the APF) is in response to a request by the Standing Committee On Community Affairs for comments on the Health Legislation Amendment (eHealth) Bill 2015.

We are happy for the submission to be made public and we will be making it available on our website.

Standing of the Australian Privacy Foundation

The Australian Privacy Foundation (the APF) is the nation's premier civil society organization concerned with privacy.

Its membership includes lawyers, academics, information technology experts, health informatics fellows, communication policy analysts and non-specialists. It has been recognised through invitations to provide testimony in parliamentary inquiries and other consultations regarding data protection, along with participation in high-level international fora. A brief backgrounder is attached.

Background

It is our view that it is very important that Australia has a well understood and accepted national framework for EHR privacy, confidentiality, information security and access control, appropriate for clinical outcomes for public and private health.

If we fail in this objective (as there appears to be the potential for happening with the efforts of those promoting the PCEHR) we are at risk of both undermining confidence in the core confidentiality and trust at the heart of the clinical relationship, and also of jeopardising the integrity, accuracy and fitness for sensitive purposes of the information. This is especially true if too many conflicting external data-mining motives have been allowed to overwhelm the core secure and controlled clinical record keeping of traditional systems.

We also note that the PCEHR in particular, which plays an unresolved, partly redundant and potentially disruptive part in the EHR system, has been dogged by governance, security, accountability and trust issues due to its confused and conflicted strategic direction and attitude to patient consent and control. This personal health information area remains a live issue for all Australians.

This submission follows our submission [1] to the Federal Department of Health regarding the eHealth Bill and is an expansion of many of the concerns voiced in that document.

Summary of Comments

The APF has serious concerns about the woeful lack of control of access to information in the PCEHR and to information in the PCEHR that can be transferred to, and accessed by, associated systems.

We draw the attention of the committee to the observation that the PCEHR is being treated as a standalone IT system. This is manifestly untrue. The PCEHR is part of a complex, interacting health information ecosystem. Privacy issues need to be treated holistically, not in a piecemeal manner, as is the situation with the eHealth Bill.

Concerns about personal information security, privacy, confidentiality and governance of the fragmented national electronic health records system are as much about how the pieces interact, whether controls, protection and risk governance effectively deal with the interoperability, complexity and potential for breach and misuse inherent in the virtual system of which the PCEHR is part, as they are about the PCEHR itself, which would have little interest if it was truly standalone.

Data will flow into and out of the PCEHR; legislation that does not deal with these flows and provide protection for patient data across all systems is worse than useless. It might give the impression that patient data is being protected by the law when in fact it is not. This can give patients a false sense of comfort which is totally unfounded.

A fundamental issue with its past and perhaps future is the degree to which there is a coherent framework into which the PCEHR fits, as ad hoc, fragmented, isolated and uncoordinated control efforts will continue to be part of the problem.

We note also that in the absence of such a framework which all patients, clinicians, data administrators and risk assessors can put the EHR, and in the absence of efforts to understand its lack of popularity and utility, the focus on 'nudging' poorly informed citizens into it by reliance on the inherently poor 'Opt out' model is a matter of great concern, because these fundamentals are still not being addressed, the public relations aspects are the focus.

We observe that the Review of the Personally Controlled Electronic Health Record in December 2013 (December 2013 Review) [2] said that the utility of the PCEHR required attention and improving. The APF agrees with and supports this assertion. We also note that no attempt has been made to address this situation; all the focus has been on getting registration numbers up, not on improving health outcomes.

We have a number of recommendations

Recommendation 1: The PCEHR or its successor should never be made opt-out. The risks to personal privacy of a system with such sensitive and personal data should only be taken where the benefits of having a summary health system are significant and obvious. An opt-out approach would create a system with data on many, if not most Australians, which is of no health benefit at all. It would also remove the only measure that would provide an indication of the usefulness of the system as seen by health professionals and patients.

Recommendation 2: The access controls implemented in the PCEHR should be completely redesigned to reflect a "need to know" approach.

Recommendation 3: Access controls should extend to systems that integrate with the PCEHR.

Recommendation 4: Every user who has access to health and personal data held in the PCEHR should have a unique user ID and password. They should also be identified to the system as to the health discipline(s) in which they work and access to the data in the PCEHR should be constrained to their health care service provision or, in the case of the patient, the understanding of those services.

Recommendation 5: The privacy and access control aspects of the eHealth legislation should be extended to the information in the systems with which the PCEHR integrates.

Recommendation 6: The access and use controls around the PCEHR should only be developed after and as part of the consultative development of a widely accepted national ehealth privacy and security framework, which situates it in its relation to all the other systems likely to interact with it, and ensures a continuity of control, auditing and governance across the whole EHR system. Anything less will prevent everyone from getting an informed understanding of the risks and the effectiveness of proposed controls, and thus will undermine the basis for any consent, opt in or opt out.

Recommendation 7: The utility and value to health professionals of the PCEHR should be significantly improved. This should be done in consultation with, and approval of, the various health professions and institutions. With a large amount of redesign, it might turn out to be useful - but right now it is an evidence free assertion.

Recommendation 8: It is recommended that the Department of Health engage the Australian Signals Directorate to conduct a Cyber Security analysis on the PCEHR. This would be to determine if the security and access controls implemented in the system, as well as the fact that the system is accessible from the internet is appropriate to the risk of potential attack by cyber criminals and terrorists as well as from state-organised cyber attack threats.

Recommendation 9: It is recommended that the Department of Health engage a suitable government body to conduct an analysis of the risks associated with the potential for data in the PCEHR in particular and health record systems in general to be used as the basis of fraud and identity theft.

Details of Submission

Opt-out

With reference to the proposal to make the system opt-out, we fail to see any benefit of having most Australian's personal and health data in a data base with such poor access controls as well as being attached to the internet. Most of the data that would be held in the PCEHR would have no practicable health value, but would represent a significant and dangerous risk.

We also draw the attention of the committee to the basic design requirement of the system which was to make it opt-in. If the government wishes to persist with this ill-advised initiative, it should, as a minimum, revisit the design of the system and ensure that all aspects of an opt-out system have been taken into account and the system modified appropriately. In our opinion this should include greatly improved access controls, as outlined above.

The introduction to December 2013 Review included this quote:

> *"As might be expected based on global experience, adoption and utilisation was slowly growing but appears to have plateaued despite increasing consumer registration (Figure 2). This level of utilisation is most likely the consequence of the issues raised by the stakeholders around the usability and clinical value of the PCEHR in this report."*

We find it interesting that the Department of Health has chosen to focus on the number of registrations rather than usability and clinical value. The Department has put significant effort into improving the registration process but does not appear to have attempted to address any of the usability and clinical value issues.

Our observation is that the registration rate is one measure of the usefulness of the system, albeit a poor one – the fact that the registration rate is low is a symptom of the un-usability of the PCEHR.

By forcing people to have an eHealth record, which for many has no apparent benefit in improving health outcomes, and using the ePIP program to insist that GPs input data into the system, the Department is removing the only measure of the system that provides any sort of feedback regarding its usefulness. They are not only addressing the symptom not the cause of poor uptake, but are ensuring that the measure of the Department's success – registration rates - is satisfactorily achieved.

It could be argued that the only reason an opt-out approach is being proposed is so that the bureaucrats can get a tick-in-the-box for something that does not actually measure anything useful in terms of health outcomes, meaningful use or in improving the efficiency and effectiveness of health care in Australia.

Some might very well think that is a valid argument, we couldn't possibly comment.

Recommendation re Opt-out

Recommendation 1: The PCEHR or its successor should never be made opt-out. The risks to personal privacy of a system with such sensitive and personal data should only be taken where the benefits of having a summary health system are significant and obvious. An opt-out approach would create a system with data on many, if not most Australians, which is of no health benefit at all. It would also

remove the only measure that would provide an indication of the usefulness of the system as seen by health professionals and patients.

Access Control

User Access

We observe that in most, if not all Federal Government IT environments, every user has a unique ID and password. Users are then granted access to specific applications on a “need-to-know” basis. Each user has had, at a minimum, a police check and usually has been vetted for security to Restricted.

This is contrasted with the PCEHR, which allows anonymous users, without any form of police or security check to access the system. The default access controls on the PCEHR are such that an approved institution can allow its employees to access a patient’s health information, if required to deliver health care to that patient. In addition, access is granted to the full and complete range of health and personal information held on a patient stored in the PCEHR. Access is logged, but only at the institution level.

This means, for instance, that if a patient goes to see a dentist and there are potential health issues if undergoing dental treatment and the patient grants access, then the dentist, their nurses as well as ancillary and administrative staff all have full access to a patient’s health record. This can include aspects of the patient’s health care that have no relevance to the practice of dentistry, such a mental health issues.

If this description is correct, and in the absence of any explanation for this recipe for data breach and misuse, and of a widely understood and accepted framework for EHR security and privacy controls, this gross departure from fundamental IT security, integrity and governance principles is quite alarming. It should alone cause a pause in further development to enable the implications to be audited and remedied at a fundamental architectural and design philosophy level.

We draw the attention of the committee to the fact that that medical and health records are classified in the Privacy Act as "sensitive" personal information, warranting a higher standard of protection than many other routine data items. To not have strict, individually accountable and auditable access control down to the data item level, with permissions from the patient working at this level and auditing supporting full review of inappropriate disclosure, 'sharing' and improper use, is not acceptable as the basis for any health record system let alone one that is called 'personally controlled'. Control by the patient is only feasible if every use and every user is identified and under granular logging, auditing and review and applies to all health record systems, not just the “umbrella” system that is the PCEHR.

We note that there are provisions in the system that allow a patient to limit access to certain documents. We believe that this is a crude access control mechanism in that it works at the document level, not health content (i.e. a document may contain only some information that a patient wishes to keep confidential but the whole document must be restricted). In addition, it is cumbersome to implement and in many cases patients do not have the capability, capacity to exercise these controls. These might include those undergoing treatment in hospital or who have mental health issues that impact their ability to function appropriately.

We would also like to draw the committee's attention to Section 70 of the eHealth Act 2102. [3]

This says, in part:

> *(1) The System Operator is authorised to use or disclose health information included in a consumer's PCEHR if the System Operator reasonably believes that the use or disclosure is reasonably necessary for one or more of the following things done by, or on behalf of, an enforcement body:*
>
> - *the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;*
> - *the enforcement of laws relating to the confiscation of the proceeds of crime;*
> - *the protection of the public revenue;*
> - *the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;*
> - *the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.*

This allows access to patient data, outside even the trivial access controls that exist in the PCEHR system. These accesses are not logged for the patient to see.

The only requirement is that "*System Operator reasonably believes that the use or disclosure is reasonably necessary ...*"

This requirement is likely to be essentially unreviewable, because it is easy to create a reasonable belief and hard to disprove it - especially when there is no statutory tort, something that is recommended by the ALRC, on which to sue.

It is our opinion that this clause is far too vague and gives the System Operator too much latitude in what and to whom they can divulge patient data.

We also maintain that using medical records as input to issues of revenue protection or crime, professional discipline or any law imposing a fine is a massive breach of medical confidentiality, and should only occur, if at all, as a result of a case by case court order or search warrant, with the presumption against, except in the most serious and overwhelmingly necessary cases.

This whole proposal to let enforcement bodies access personal medical and health data sets up a complete breach of medical confidentiality. It allows for access by essentially unreviewable bureaucratic whim on a systemic basis, rather than cautious case by case exception in extreme circumstances.

No wonder the proponents are seeking to use 'Opt -out' - there is no obvious reason why a patient, properly advised, would accept such a model voluntarily. It does fit however with the current obsession with trying to break or 'disrupt' privacy rights in the name of uncontrolled sharing into 'Big Data' systems which are little more than fishing expeditions and indiscriminate mass surveillance systems.

We maintain that the lack of access control to a patient's health record and the lack of appropriate partitioning of health and personal information in the PCEHR is such that the system represents a real and high risk to the privacy of Australians who choose to participate in the system.

It is assumed that those who have chosen to participate in the PCEHR can see some sort of benefit in having a centralised database of their personal information and some of their health data accessible over the internet and by anonymous users with no police or other checks.

The APF is not the only institution with concerns regarding poor access controls.

As an example we draw attention to the submission by the Australian Association of Social Workers [4] which contains this paragraph:

> *PCEHR, privacy and family violence*
>
> *While the AASW supports the proposed changes to privacy and security, we still have further questions about how the PCEHR deals with issues of confidentiality for individuals who seek anonymous or confidential care. We have particular concerns in regards to how the system acknowledges the dynamics and complexities of family violence as those experiencing abuse may be forced, through coercion, to give perpetrators access to their record resulting in care ceasing to be confidential. This could contribute to an escalation of abuse and potentially deter individuals from seeking support from their healthcare provider as they no longer have the assurance of confidentiality.*

The Royal Australian and New Zealand College of Psychiatrists submission [4] also raised a number of points, such as in these paragraphs:

> *Another concern is the kind of information stored in the PCEHR. If particularly sensitive information to do with sexual health, trauma or mental health is recorded in the PCEHR, the patient may feel it necessary to disclose this information to some health practitioners and not to others. For example, if patients have received medical treatment following a sexual assault, they may deem this relevant information for the psychiatrist but they may feel disclosure to their podiatrist is unnecessary and invasive. Will there be levels of access depending on the sensitivity of information and its appropriateness to different parties? Will there also be any provision for hand-written records to be kept in parallel to record sensitive information or detailed records made during the interview with a patient or will clinicians be expected to operate in a paperless system, thus losing much useful detailed history? This detail is not only useful for clinicians assessing patients at a subsequent time but also for the preparation of medico-legal and other reports.*
>
> *With respect to medico-legal and privacy issues, there are concerns around the potential for information to be inappropriately accessed and used. For example, there is a growing trend for solicitors to issue subpoenas of broad scope to obtain sensitive health information, often to be used in family law proceedings to 'dig up dirt' on estranged spouses. The PCEHR, being a centralised location for much of the patient's health information, leaves patients particularly vulnerable with regards to this matter. RANZCP members have also raised concerns about insurance companies gaining access to health records and misusing this information in ways that are detrimental and unfair to the individual.*
>
> *The RANZCP also wishes to emphasise an important issue in relation to mental health diagnoses under the PCEHR system. Mental health diagnoses are often less clear cut than their physical health equivalents. Diagnoses can change as more information becomes available, research in the field develops or courses of treatment are found to be more or less effective. Therefore, a change in a patient's mental health diagnosis is a common occurrence and - if previous diagnoses are not*

critically reviewed - it can and does result in many years of unnecessary treatment and stigmatisation of the patients concerned. Consequently, the RANZCP considers that more information is required as to how the issue of a changing diagnosis will be reflected in a PCEHR. If a diagnosis is made by one practitioner and then reviewed, changed or removed by another, for example, how will this show up? Are there measures in place to avoid stigmatisation of an individual due to an incorrect diagnosis? Any PEHCR system would need to be flexible enough to allow easy correction of mislabelling and adjustments made as the result of new information coming to light or a change in presentation.

It is clear that the access controls incorporated in the PCEHR, as it currently exists, means that it is totally unsuitable for use by the health profession in Australia.

Extraction of data into other systems

We also draw the committee's attention to the fact that many, if not most institutions will access the PCEHR through their primary health care systems.

This means that it is potentially possible for these other systems to extract some or all of a patient's health data and store that data in a local system, a system that would not be subject to any of the provisions of the eHealth Bill (other than generic privacy requirements) or have access logged such that the user could see if their health record had been read or downloaded.

The data that could be transferred into one of these local systems could include the full health record, including data that was of no relevance to the nature of the health care provided by that institution.

It is proposed that the access controls in the PCEHR should be extended to control the documents and data that can be downloaded.

Recommendations re Access Controls

Recommendation 2: The access controls implemented in the PCEHR should be completely redesigned to reflect a "need to know" approach.

Recommendation 3: Access controls should extend to systems that integrate with the PCEHR.

Recommendation 4: Every user who has access to health and personal data held in the PCEHR should have a unique user ID and password. They should also be identified to the system as to the health discipline(s) in which they work and access to the data in the PCEHR should be constrained to their health care service provision or, in the case of the patient, the understanding of those services.

Recommendation 5: The privacy and access control aspects of the eHealth legislation should be extended to the information in the systems with which the PCEHR integrates.

Recommendation 6: The access and use controls around the PCEHR should only be developed after, and as part of, the consultative development of a widely accepted national ehealth privacy and security framework, which situates it in its relation to all the other systems likely to interact with it, and ensures a continuity of control, auditing and governance across the whole EHR system. Anything less will prevent everyone from getting an informed understanding of the risks and the effectiveness of proposed controls, and thus will undermine the basis for any consent, opt in or opt out.

These recommendations mean that:

- Data in the Health Record system should be classified according to the needs of health care disciplines. The granularity of this access control should be agreed with the various health professions and institutes.
- Every user who has access to data in the PCEHR should be identified to the system and that access should reflect the health care needs of that user. Logging of access should be associated with that user.
- When local systems interact with the PCEHR they should have a similar level of "need-to-know" access control. This should be designed and implemented in such a way that it prevents, for example, a dentist's system from access health data that is clearly not appropriate for that health care practice or capturing and storing some or all of a complete record in local systems.
- When data is extracted from the PCEHR it should be subject to the same individual user based access controls and logging. This means that, when a user in a health care institution accesses data that is stored in a patient's PCEHR record, that access should controlled and logged as though the access was through the PCEHR itself. Logs reflecting this access generated in the local system should be transmitted to the PCEHR for incorporation into the PCEHR audit logs.
- All requirements and design features should be developed by, and in collaboration with, health care professionals, designers of local systems that interact with the PCEHR, as well as representatives of privacy, security and consumer bodies.

Value and Utility

In addition to serious reservations regarding access control, we also have concerns regarding the use and value of the system itself.

We draw the committee's attention to documentation on the NEHTA website [6] which makes it clear that:

- *The PCEHR System is intended to complement and not replace existing clinical information systems*
- *The PCEHR is not a replacement for normal sharing of information between an individual and their healthcare provider*

In other words, the PCEHR is a simple database of a subset of patient data with pointers to data in other repositories. It is not intended to play a major part in health decision making – other systems have been designed and implemented for that purpose and these will achieve that objective.

What the PCEHR does do is draw together into a single repository a significant amount of data, and pointers to data, that are currently held in far more secure repositories and whose access controls are far more stringent than that of the PCEHR.

It should be stressed that the PCEHR is not the only health record system in operation in Australia; in fact, it is one of the least useful. Hospitals, GPs, specialists etc., all have their own systems, tailored for their needs and appropriately partitioned as to content and requirements of the health professional user.

The only reasonable uses we can see for a system like the PCEHR are:

1. On the occasions when a patient visits a new health carer.

Most patients see the same health professional each time they require treatment. Most Australians have no need for a health record, if they do, they can create a new one. Having a pre-populated health record may save a few minutes time but the number of times this occurs each year in Australia is probably quite small. To our knowledge this metric has never been measured or published.

Our opinion is that a lot of money has been spent and a considerable risk to patient privacy has been created on a system that has limited usefulness.

2. To act as a clearing house for health data.

Our understanding of how the whole eHealth system (as opposed to just the PCEHR) will work is this:

> Most health institutions will have other, local systems that their health carers use to support their health decision making. These systems will suck data out of the PCEHR into the local system. This means all the provisions in the eHealth Bill re privacy, audit logs and control will disappear.
>
> The people obtaining the benefit will be the down-loaders, not the up-loaders. The up-loaders, apart from automated systems associated with tests, are unlikely to get much benefit. A GP, who has their own eHealth record system, is highly unlikely to benefit, but probably shoulders most of the effort.
>
> The health benefits will come from using the local system, not the PCEHR itself, which is just a glorified store and forward messaging system that keeps the messages and calls them a Health Record.
>
> There are better and more efficient ways of delivering a health information messaging hub without putting patient's health information at risk.

We also have concerns about the thought that has gone into the design of the system. It is a fundamental tenet in the development of automated information systems that all exceptions, special cases and errors need to be identified and appropriately handled. When people are given a task they can be told what the “normal” procedures are and to see their supervisor if any problems arise or something is out of the ordinary. This simplistic approach is not sufficient when dealing with Information Systems. Every contingency must be planned for and the system must be able to cope with any eventuality.

As evidenced by the quotes above, in the context of access control, it is patently obvious that this level of analysis and design has not underpinned the development of the PCEHR.

In the December 2013 Review, it was noted that poor utility was a major factor in the low level of uptake of the PCEHR. We are unaware of any initiatives to identify what is required to increase the usability of the PCEHR or to actually implement improvements in the system

We also note that recommendations in the December 2013 Review included these:

> *31. Immediately update the MyHR strategy to actively enable decentralisation of information across multiple data repositories, with information being linked using the Healthcare Identifier (HI).*

The MyHR be updated to act not only as a data repository, but also an information exchange and providing important linkages to third party data repositories and information where it is stored.

32. Reset the policy standards and frameworks necessary to enable interoperability, in a decentralised model, plus commercial models that ensure providers can generate an acceptable return on the investments made in shared infrastructure.

33. Prepare a business case that defines appropriate methods of compensation for investment should be investigated that include one-off costs and/or transaction fee services for clinical access to records associated with integration of existing data sets into the MyHR.

There is no evidence that these recommendations from the December 2013 Review are even being considered, never mind implemented. They represent significant changes to the architecture and design of eHealth systems in Australia yet they do not seem to have received any funding.

Recommendation re Utility

Recommendation 7: The utility and value to health professionals of the PCEHR should be significantly improved. This should be done in consultation with, and approval of, the various health professions and institutions. It should also be based upon a thorough analysis of health decision making processes and practical evidence that it will work. The design so far exhibits all the characteristics of an IT driven development with technologists "knowing best" and ignoring the input and participation of the health profession and the software industry that is required to develop commercial systems that interact with it.

Cyber Security and Fraud

Cyber Security

There have been reports in the media recently [7, 8] that Australia is at an increased threat of cyber attacks.

David Irvine, former ASIO director general, has warned that jihadists could soon be capable of launching destructive cyber attacks, urging more should be done to build a "cyber secure country".

He is quoted as saying that,

"While terrorist organisations had not yet shown sophisticated cyber attack capabilities, Australia should be prepared for the worst.

We must anticipate, given the sophistication that they have already demonstrated in using the internet for propaganda and other reasons, that they could well develop destructive attack capabilities in the near future.

Cyber attack threats went beyond government information to include 'personal and commercial' data."

We strongly recommend that an independent assessment be conducted, preferably by the Australian Signals Directorate, or equivalent government security body, of the design and implementation of the system. It should also include the risk to national security of having personal and health data on all Australians in a system with poor access controls, accessible by anonymous, un-vetted users and which is accessible via the internet.

Fraud and identity theft

We also note that in evidence given to a Senate estimates committee recently and as reported in the media [9]

It is reported that:

> *Hundreds of Australians could have had their identity stolen as part of a scam targeting the Medicare system, Senate estimates has heard.*
>
> *There have been 369 cases of potential identity theft in the two years to June 2015, prompting the establishment of a police strike force to investigate whether the personal information of customers had been accessed and altered to obtain the sham payments*

In addition, other reports claim that in Australia, healthcare records are a major target for hackers – with fully populated medical records sold to fraudsters for up to A$1,000 each [10]. The reports says:

> *Carl Leonard, principal security analyst for Websense, said healthcare around the world is now experiencing 340% more attacks than the average industry sector. He said that, in 2014, there was a phenomenal 600% increase in the number of attacks launched against hospitals – and Australia is no exception.*
>
> *He said: "Healthcare offers a very complete dataset that can be used for identity theft or fraud. It holds very up-to-date contact information so you can send targeted mails, and use the information and repurpose it for identity theft"'*
>
> *Leonard said the challenge for the healthcare sector is to balance its desire to use electronic records to deliver improved patient care against the need to properly protect that information, without making it more difficult for medical professionals to access.*
>
> *While Australia's adoption of electronic health records is still patchy, Leonard said organisations needed to properly protect that data.*
>
> *"Even if only 10% of the population has an electronic health record, that is still incredibly valuable to an attacker."*
>
> *Leonard said: "A vulnerability exists because of the relatively new nature of health records and because of the environment they operate, where the physician needs to access the record easily."*
>
> *"Right now it's a perfect storm."*

In view of the attractiveness of the data in a health record system and the very real potential for the data to become the target for fraud and other criminal activity, it is strongly recommended that an independent assessment be conducted as to the risks of identity based crimes, along the same lines as that for Cyber Security. Given the integration of the PCEHR into the overall health record environment in Australia, the scope should be all health record systems, not just the PCEHR.

Recommendations re Cyber Security and Fraud

These assessments should be conducted and the results reviewed before the Senate passes legislation to make the system opt-out. The Terms of Reference should be made public, along with the results of the assessments to ensure that Australians can have confidence that the system is a safe and secure as possible.

Recommendation 8: It is recommended that the Department of Health engage the Australian Signals Directorate to conduct a Cyber Security analysis on the PCEHR. This would be to determine if the security and access controls implemented in the system, as well as the fact that the system is accessible from the internet is appropriate to the risk of potential attack by cyber criminals and terrorists as well as from state-organised cyber attack threats.

Recommendation 9: It is recommended that the Department of Health engage a suitable government body to conduct an analysis of the risks associated with the potential for data in the PCEHR in particular and health record systems in general to be used as the basis of fraud and identity theft.

Final Observation

We note that the December 2013 Review said:

> *A common theme was that the stakeholders' views were often sought and obtained, but in many instances these views (including those from Clinical leads and reference groups) perceived to be either overruled by the Commonwealth or lost in the NEHTA process.*
>
> > *"it remains perplexing that the output from all of these consultations were largely ignored by Government and by NEHTA in recent times".*
> >
> > *Quote – The Royal College of Pathologists of Australia Submission*

The APF supports this observation and notes that there appears to have been no changes made to the eHealth Bill as a result of the 137 submissions made to the Department of Health.

We look forward to a welcome change in this behaviour by the Senate Committee, which now has a chance to identify the fundamental issues with the PCEHR, in particular, and the whole eHealth environment in general. We contend that this is a better approach than focussing on mechanisms to 'put lipstick on a pig' and manipulatively 'nudge' uninformed patients into a poorly governed system that is at present neither ready, safe nor necessary for their health or their clinician's needs.

Thank you for giving us the opportunity to comment on the proposed amendments to the Health Legislation Amendment (eHealth) Bill 2015.

Yours sincerely

Dr Bernard Robertson-Dunn
Chair, Health Committee
On behalf of the board of the APF

References

1. Submission by the APF to the Department of Health re the eHealth Bill
Available at:
http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/consultation-submissions
Submisssion 60

2. Review of the Personally Controlled Electronic Health Record in December 2013
http://www.health.gov.au/internet/ministers/publishing.nsf/Content/B4B0EBCF8DAAC9B1CA257C49007B3117/$File/PD028.pdf

3. Personally Controlled Electronic Health Records Act 2012
https://www.comlaw.gov.au/Details/C2012A00063

4. Submission by the Australian Association of Social Workers to the eHealth Bill
Available at:
http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/consultation-submissions
Submission 58

5. Submission by The Royal Australian and New Zealand College of Psychiatrists (PDF 100 KB) to the eHealth Bill
Available at:
http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/consultation-submissions
Submission 079

6. Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) System
Edition: September 2011 Release, Date: 12 Sept 2011, NEHTA Version Number: 0.14.18
http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/CA2579B40081777ECA2578F800194110/$File/PCEHR-Concept-of-Operations-1-0-5.pdf

7. Beware ISIS cyber threat, says former ASIO chief David Irvine
The Australian, October 27, 2015
http://www.theaustralian.com.au/in-depth/terror/beware-isis-cyber-threat-says-former-asio-chief-david-irvine/story-fnpdbcmu-1227583279273?sv=bc039cc1f385a2178f0fdae0e28a8f4

8. Former ASIO boss David Irvine warns of 'destructive' cyber attacks by jihadists
ABC Online, October 27, 2015
http://www.abc.net.au/news/2015-10-26/former-asio-boss-warns-jihadists-could-soon-launch-cyber-attacks/6886448

9. Hundreds could be victim of identity theft scam targeting Medicare system, estimates hears
ABC Online, 22 October 2015
http://www.abc.net.au/news/2015-10-22/estimates-hears-of-scam-targeting-medicare-system/6878234

10. Hackers target Australian health sector, selling records for A$1,000
Computer Weekly
http://www.computerweekly.com/news/4500254986/Hackers-target-Australian-health-sector-selling-records-for-A1000

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

• Policies	http://www.privacy.org.au/Papers/
• Resources	http://www.privacy.org.au/Resources/
• Media	http://www.privacy.org.au/Media/
• Current Board Members	http://www.privacy.org.au/About/Contacts.html
• Patron and Advisory Panel	http://www.privacy.org.au/About/AdvisoryPanel.html