



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>
Secretary@privacy.org.au
<http://www.privacy.org.au/About/Contacts.html>

24 June 2015

Department of Health,
MDP 1003,
GPO Box 9848, CANBERRA ACT 2601

Dear Department of Health

Re: Feedback on the PCEHR/IHI Legislation Discussion Paper

This submission by the Australian Privacy Foundation (the APF) responds to the request by the Department of Health for comments on the Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper.

It follows previous APF feedback about the Draft Concept of Operations [1] and the addendum [2].

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.

We also draw you attention to the work the Foundation has done previously in this area.

APF policy Statements are available at <https://www.privacy.org.au/Papers/PS.html>

Work we undertook in 2009 on 'eHealth Data and Health Identifiers' is particularly relevant to the issues under discussion and is available at <https://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf>

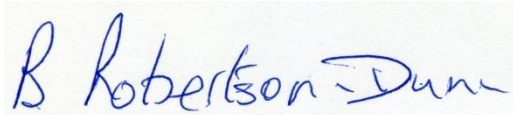
We also have an index of 48 prior submissions on eHealth matters, at:
<https://www.privacy.org.au/Papers/indexPolicies.html#eH>

This submission is informed by a detailed awareness of data protection and privacy law, major Information System development and the health information environment in Australia.

APF's approach to assessing privacy issues surrounding health care and associated Information Systems is based primarily on publicly available evidence. This submission complies with that approach.

Thank you for your consideration.

Yours sincerely

A handwritten signature in blue ink that reads "B Robertson-Dunn". The signature is written in a cursive style and is positioned above a horizontal line.

Dr Bernard Robertson-Dunn
Chair, Health Committee, for the APF Board
Bernard.Robertson-Dunn@privacy.org.au

Summary and Conclusions

The Australian Privacy Foundation has a number of very serious concerns with the PCEHR, the proposed changes to the system and its enabling legislation.

These can be summarised as follows:

1. The value of the PCEHR, as only one eHealth system in Australia, has not been demonstrated. The PCEHR has been implemented such that it replicates current health care practices and therefore offers limited functionality. The opportunity to enable better and more effective and efficient work processes has been missed;
2. The documentation available on the websites of NEHTA and the Health Department is old, inconsistent, incomplete and does not adequately describe the fundamental drivers and requirements of eHealth care or the way in which these have been architected and designed into the system; and
3. The risks to privacy of a high value repository of every Australian's identity and health data are not matched by the minimal value and benefits inherent in the PCEHR. Moving to an opt-out model is not justified and will only increase that risk. A major factor is the poor legislative protection afforded to health information in Australia which, in our opinion, has led to a lack of trust that the risks are, or will be, adequately managed.

With respect to the proposed move to opt-out, we believe that there is a strong possibility that there will be a realisation amongst the population at large that the PCEHR is actually a thinly disguised national identity number attached to some health information, none of which can be relied upon because there is no way to medico-legally trust the information contained. However the identity data will be seen as very useful to the government, especially when cross-matched against internet and telecommunications metadata and other government databases.

Based upon our many concerns, we do not believe that the proposed changes to the system or the legislation will achieve any significant improvement in use by the health community.

We contend that the government has only two alternatives: either decommission the system as soon as possible, or completely re-architect the system such that it is able to support major changes to existing health care work practices and is much better and more closely integrated with existing health record systems.

Overall Response

The PCEHR was commissioned in July 2012. It has been subject to a brief, six week review (the Royle Review) which was completed in December 2013 and released to the public in May 2014 [3].

We have examined the publicly available information on the PCEHR, the Royle Review and the proposed legislative changes. As a result of this review, we have a number of concerns and questions regarding the PCEHR.

Our primary concern is that we can find no reliable and compelling evidence that demonstrates that the PCEHR as it exists today, or as it will become if the proposed changes are implemented, can deliver the type or level of value and benefits that justify the risks to privacy of a high value repository of every Australian's identity and health data.

We are also concerned that many of the publicly available documents are very old and should have been updated, as promised in the documents themselves. It also appears from comments made at public briefings that the Department of Health has available a number of documents that should have been made available, including several Privacy Impact Assessments. We are also concerned that the documentation that is available is incomplete, inconsistent and does not appear to conform to Information System development best practice.

With an Information System and its use, Privacy is not an absolute; it is a trade-off between the value and benefits of that system and the risks of implementing and using that system. Therefore our concerns fall into three categories:

1. The claims of the value and benefits of eHealth records in general and the PCEHR in particular;
2. The availability of documentary evidence as to the full nature of the requirements and high level architecture and design decisions that underpin the system; and
3. The risks to privacy created by, and associated with, the PCEHR.

We will deal with our concerns and questions with respect to the existing implementation of the PCEHR first, followed by the proposed changes.

Current State

Concerns about claims as to the value of eHealth records

The Royle report says:

"The Panel finds that an electronic health record remains a critical part of the future Health infrastructure for Australia and with the recommended changes in the PCEHR will help accelerate the potential benefits identified by the 2008 eHealth Strategic Plan to provide more effective and efficient healthcare for all Australians."

In our reading of the 2008 eHealth Strategic Plan, we suggest that the benefits are not clear and the evidence behind the conclusions is not available. For example, the report says:

The tangible benefits associated with E-Health are difficult to accurately quantify due to the poor quality of baseline Australian health care system information and the very close, and often blurred, relationship between E-Health and broader health sector reform initiatives. However, there is a growing amount of local and international research available to highlight the potentially important role E-Health may play in delivering Australian citizens a higher quality, safer, more equitable and more efficient health system.

In our opinion this is a highly qualified statement of support for eHealth, let alone eHealth records, and the report contains no substantial evidence that backs this statement.

Concerns about claims as to the value of the PCEHR

In the Royle Review is the statement "Booz and Company estimate that over \$A7 billion in direct costs could be saved (in Australia) annually by digitizing the healthcare sector and that those cost savings would also reflect substantial improvements in the customer experience with millions of hospital visits and admissions avoided each year".

Slide 13 in the publicly available Booz and Company presentation is an estimate that adopting the PCEHR would achieve benefits of \$400million annually by the year 2020. We note that slide 13 in this presentation this statistic is specifically highlighted as referring to the PCEHR and that this highlight is missing from the version of the slide included in the Royle review. We also note that the figure of \$400million attributed to the PCEHR is never mentioned in the Royle review.

We are concerned that the review has based its conclusions on the false assumption that the PCEHR itself would achieve benefits of over \$7billion per year. Even if the authors of the report have not made this assumption, they certainly have not clearly identified the true estimate of the benefit of the PCEHR as predicted by Booz and Company.

It is also of concern that it is unclear if the authors have assumed that the PCEHR is the only eHealth record in Australia. If they have, then they have failed to incorporate potential savings from the other eHealth records currently available and planned for Australia. In either case the evidence for the value of the PCEHR is uncertain and unreliable.

We would like to point out that we are not alone in questioning the use and role of the PCEHR. We draw attention to Dr David More's Blog [4] and to comments made by Dr Edwin Kryus [5] on 22 June 2015 on the hurdles that will need to be overcome if eHealth is to succeed.

Concerns about the way the PCEHR is being marketed to Australians

We are concerned that the public are only being told about the potential benefits of the PCEHR. As with any Information System, and especially with those that contain personal identity and health information, there are risks and other non-financial costs. We contend that these potential costs of having an eHealth record must be identified and given equal prominence as the claimed benefits in order to permit Australians to make an informed choice regarding participating in the PCEHR system.

Concerns about the PCEHR as an IT system and its development

There is much evidence that many, if not most, large scale IT projects either fail or do not achieve their intended objective. The most often cited reason is associated with poor, missing or changing requirements. In standard and best practice Information Systems development, requirements are identified in a series of steps and in a particular order. There are many approaches to Information Systems development; however they all start with a “model of use”. This is usually developed during a “Business Architecture” phase in which issues, including the following are defined, documented, analysed and addressed:

- The purpose and value of the system;
- The users of the system;
- How the system is to be used;
- Ways in which existing processes may be automated, improved, replaced and managed;
- The usability of the system;
- What interactions with other systems need to be included and the nature of those interactions;
- What information should be included in the system and the way that information flows through the system and is processed by the system;
- Legislative and other requirements and constraints; and
- Non-functional requirements such as security, privacy, availability, performance, locations, interfaces, support, development etc.

None of these are technical issues, but they do provide the basis for the solution. These issues should be addressed through consultation and agreement with those who would use and derive value in the system. If this did occur, there is no evidence of the outcomes or how they have been translated into the architecture and design of the system.

We have examined the publicly available documents, specifically the Concept of Operations [6] and the PCEHR High Level Architecture [7] and can find no evidence that any form of “model of use” has been developed or a business architecture phase conducted.

It is not possible that a business architecture phase could have been conducted and that an appropriate model of use could have been developed because that would have required engagement with a significant number of stakeholders and would have been a very public exercise. No published evidence is available to show such engagement has happened.

If a major change in practice – opt-out instead of opt-in – is to be proposed, then the model of use has changed and will require a proper Business Architecture phase to be conducted.

We do note that in some of the documents available on the NEHTA website, a Business Architecture is mentioned, but the documentation on the NEHTA and the Health Department is inconsistent,

incomplete and does not adequately provide a clear and detailed description of what the system is supposed to do, why it does it, what the options and/or trade-offs are.

Our concern is that the PCEHR has been developed without regard to best practice and that there is no publicly available documentation of key requirements, architecture and design, most specifically as these apply to issues of privacy.

Concerns about understanding how the PCEHR will realise claimed values and benefits

The Personally Controlled Electronic Health Records Act 2012 [9] says:

The object of this Act is to enable the establishment and operation of a voluntary national system for the provision of access to health information relating to consumers of healthcare, to:

- a. help overcome the fragmentation of health information; and
- b. improve the availability and quality of health information; and
- c. reduce the occurrence of adverse medical events and the duplication of treatment; and
- d. improve the coordination and quality of healthcare provided to consumers by different healthcare providers.

With respect to these particular objectives, we are concerned that:

1. There is no documentation that identifies how the PCEHR will achieve these objectives;
2. There are no defined measures of these objectives;
3. No analysis has been published regarding the extent to which these objectives may have been achieved; and
4. 'Opt-out' is no longer a basis on 'voluntary' participation as the de facto standard of operation.

Of greater concern is the apparent lack of understanding in the whole eHealth initiative that the best use of health information systems is to develop new and better ways of delivering health care.

To return to the Royle review, we point out the presentation states that:

Technology alone is not the problem: this is about changes to ways of working and using new tools.

In other words, many of the benefits come from changes to work practices. However, the Review, under the section on Design ... contains the statement that:

Greater flexibility / user customisation required to suit individual clinician work practices.

This is exactly the opposite of the Booz and Company report conclusion that says that work practices should change, not that technology should be flexible enough to support existing work practices.

We also highlight that the 2008 eHealth Strategic Plan Recommendation R3 says:

Encourage health care participants to adopt and use high priority E-Health solutions and modify their work practices to support these solutions.

In other words, both documents are saying that the benefits from an Information System come from doing things differently and better. This is standard advice when implementing an Information System: don't automate what you do now, change the way you do things.

The PCEHR is essentially just a document repository. Our concern is that there is no evidence that the PCEHR supports better ways for health professionals to change or improve their work practices. Neither is there evidence that improving usability will achieve this.

As already stated, in the review of the PCEHR in 2014 most of the concerns and subsequent recommendations are about the “value proposition” and “usability”. It is our contention that the lack of a business architecture phase in the development of the eHealth record initiative is responsible for these shortcomings as well as the issues we see in addressing privacy. Further information about the importance of business architecture is included below.

Concerns about responsibility for data quality and accuracy

We are concerned that issues regarding the responsibility for data accuracy and data quality in the PCEHR have not been adequately addressed and/or clearly communicated to all involved in the use of the system.

There are multiple major issues that do not appear to have been identified or completely resolved, these include:

- Defining responsibilities for accuracy of health information in the system;
- How errors are to be corrected and who is responsible for the correction and what are acceptable response times for correction;
- The medical and legal status of incorrect, invalid or unwanted health information in a patient’s record that has been created as part of the opt-out process, but which has not been seen or validated by the patient;
- How disputes are to be resolved;
- Any form of risk assessment on security, privacy or other requirements; and
- Highlighting in the health record that certain information may be in dispute or of dubious, quality.

Concerns about the risks to privacy of the existing PCEHR

The IHI and PCEHR have what is probably the most complete and valuable identity and personal information on Australians. This makes it of high value to people wanting to obtain unlawful access. The risks associated with the IHI and PCEHR must be worth the value and benefit to the nation and to individuals. Our concerns regarding the validity of the claims of value and benefit are detailed elsewhere in this paper, however, we also have concerns regarding the treatment that privacy requirements and issues have been given within the IHI and PCEHR.

We note that the IHI is not publicly available, however experience shows that this does not prevent it from being attacked.

We are concerned that only one Privacy Impact Assessment (2011) [9] (PIA) has been conducted and made publicly available. We understand that other PIAs have been conducted as the system has been modified, but are not aware of any being made public.

We also have concerns that the Privacy Impact Assessment was conducted before the new Australian Privacy Principles (APPs) replaced the National Privacy Principles (NPPs) for organisations from 12 March 2014. There is no evidence that a PIA has been conducted that addresses these principles or that any changes have been made to the system that incorporates necessary changes.

There are a large number of exclusions in the Privacy Impact Assessment of 2011; however we wish to highlight two.

The first is that the PIA is based only on the Concept of Operations, a very high level document, lacking in detail and which was prepared before any architecture or design work. There are many aspects to the protection of privacy, and decisions occur at many points during the system development process. In our opinion it is not reasonable to assume that all aspects of privacy could be identified and dealt with at a single point of time in a single 'state of play'.

Secondly the PIA:

- does not assess the proposed PCEHR System with respect to compliance with the proposed Australian Privacy Principles (APPs). This assessment has focused on the existing state of privacy regulation in Australia at the time of the original planning and implementation; and
- does not assess privacy risks by reference to the enacted APPs.

We are concerned that there is no documented set of privacy requirements, no explanations of how those requirements have been incorporated in the architecture and design of the PCEHR and no publicly available PIA of the system as it currently exists.

Proposed Changes

Concerns about the scope and nature of the changes

There are many changes planned for the PCEHR, its governance and enabling legislation.

The planned changes in usability and legislation will have a direct impact on the user requirements and its architecture and design. In addition the opt-out trial will also be conducted during these changes.

Our major concern is that there is no "big picture" that shows what initiatives are planned, how they relate to each other and how they relate to other systems, including the other health record systems already in use and planned for at the state and local level be they public or private providers.

What is not clear at all from the Legislation Discussion Paper or any of the public briefings is what, if any, changes are to be made to the system either in terms of usability or in support of better health outcomes.

It is essential that privacy issues be included in the requirements and subsequent architectures and designs of all of these initiatives, and that evidence that they have been properly addressed should be available for scrutiny.

Concerns about risks to privacy

Changing to an opt-out, implied consent model will have consequences to the risk profile of the PCEHR program.

It can be argued that implied consent is not an intrinsically fair model, since it creates perverse incentives to leave people in the dark about things which might have implications for their whole family or community, for their whole lives.

There needs to be evidence that the risks associated with this new model have been identified and suitably addressed.

It should be noted that addressing risks in the system is likely to impact the fundamental requirements, the architecture, the design and the way in which users need to be informed and educated. Our concern is that the changes being considered to the PCEHR are being conducted in a piecemeal manner if not a vacuum of understanding or consideration of those risks.

We also have reservations about the potential reaction of the broader community if and when a full move to opt-out is begun. It is quite possible that undertaking the trials will not achieve a proper understanding of the reaction to a system that could be perceived by at least some to be a thinly disguised national identity number attached to some health information, none of which can be relied upon because of a lack of trust in the accuracy of the data, its completeness and its standing with regard to issues such as legal liability.

We suggest that the identity data contained in the IHI/PCEHR will be seen as very useful to the government, especially when cross-matched against internet and telecommunications metadata and other government databases such as those operated by the ATO, Immigration and Medicare, as well as a range of law enforcement agencies.

Concerns about fragmented legislation with respect to the protection of privacy of health information

We observe that privacy protection of health information is manifested in three acts – the Privacy Act (1988), Healthcare Identifiers Act 2010 and the Personally Controlled Electronic Health Records Act 2012.

We are concerned the legislative protection of privacy information has been fragmented across multiple acts and that each has a different focus. The Privacy Act (1988) is technology neutral, the Healthcare Identifiers Act 2010 covers a service currently being provided by the Chief Executive Officer of Medicare Australia and the Personally Controlled Electronic Health Records Act 2012 covers a particular implementation of an Information Technology system that is the responsibility of the Secretary of the Department of Health.

This legislation is not only fragmented, but it does not cover equally all health record systems in use in Australia. The interactions between the different health record systems can result in anomalies and discrepancies along with unclear protection and responsibilities.

We strongly suggest that legislative protection of health information should be made independent of any particular service, technology or Information Technology System.

We refer the Department to the example set by the USA with its HIPAA which contains both privacy and security rules. To quote The American Health Information Management Association [10]:

The privacy rule covers all protected health information (PHI) in an organization, the security rule is narrower in scope, with the focus solely on electronic PHI (E PHI). Section 164.530 of the privacy rule requires "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The security rule complements the privacy rule by establishing the baseline for securing electronic health information for covered entities both in transit and at rest.

The security rule is based on three principles: comprehensiveness, scalability, and technology neutrality. It addresses all aspects of security, does not require specific technology to achieve effective implementation, and can be implemented effectively by organizations of any type and size.

Concerns about appropriate legislative protection of privacy of health information

A number of issues have been identified by various commentators [11] [12] regarding the scope and effectiveness of the current legislation as it applies to privacy of health information. These include:

1. In the legislation covering the IHI, the service operator should be a constitutionally entrenched authority (instead of the Medicare CEO);
2. The extent of technology neutrality within current legislation needs to be reviewed and provide binding technology guidelines to those utilising PCEHR. In particular, guidelines surrounding audit trails, encryption and sever security absent from current legislation;
3. The length of storage of health data by the PCEHR should be reviewed. It is currently set at 30 years after death or 130 years if date of death is unknown, which is excessive when compared to state health records legislation;
4. The managers of the system should not be determined according to the PCEHR regulations, this creates uncertainty regarding who may control PCEHR in the future; and
5. There needs to be clarity within legislation regarding who owns the health data and what is meant by “ownership” in this context. The Privacy Act 1988 (Cth) is arguably inconsistent with the principles of ownership stipulated in the High Court case of *Breen v Williams*. That is, the rights of patients to access and amend their file and further, the collection of data for health statistics is incompatible with physician ownership.

These concerns are not limited to Australia, the USA faces similar issues. For example in this paper Top 3 issues facing patient privacy [13] the issues raised are:

1. Legislative gaps;
2. A lack of trust; and
3. A lack of patient control.

These are familiar issues to us in Australia and seem to be common in many other countries.

Our concern is that there are multiple issues in the legislation that affect privacy of health information and which, in our opinion, require urgent attention. These issues will become more important if and when the PCEHR becomes opt-out.

References

- [1] 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, <https://www.privacy.org.au/Papers/NEHTA-ConOps-110530.pdf>
- [2] Addendum to APF feedback dated 5 June 2011 <https://www.privacy.org.au/Papers/NEHTA-ConOps-Add-110607.pdf>
- [3] Review of the Personally Controlled Electronic Health Record. <http://health.gov.au/internet/main/publishing.nsf/Content/ehealth-record>
- [4] Dr David More's Blog <http://aushealthit.blogspot.com.au/>
- [5] Dr Edwin Kruys <https://www.mja.com.au/insight/2015/23/edwin-kruys-e-health-hurdles>
- [6] PCEHR Concept of Operations [http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/CA2579B40081777ECA2578F800194110/\\$File/PCEHR-Concept-of-Operations-1-0-5.pdf](http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/CA2579B40081777ECA2578F800194110/$File/PCEHR-Concept-of-Operations-1-0-5.pdf)
- [7] PCEHR High Level System Architecture
Registration required
<https://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1001-2011/NEHTA-1002-2011>
- [8] Personally Controlled Electronic Health Records Act 2012 <https://www.comlaw.gov.au/Details/C2012A00063>
- [9] PCEHR Privacy Impact Assessment <http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/pcehr-legals-pia-toc>
- [10] The American Health Information Management Association
A HIPAA Security Overview (Updated)
Available on the AHIMA website
- [11] E-health Records: How and Why the Law Must Change to Promote Better Privacy in Healthcare <http://www.slideshare.net/informa0z/bianca-phillips-swin>
- [12] The e-health records cloud: how and why the law must change to promote better privacy in healthcare; Bianca Phillips and David Genziuk
Privacy Law Bulletin, LexisNexis 2014 (Vol 11 No 1).
- [13] Top 3 issues facing patient privacy <http://www.govhealthit.com/news/top-3-issues-facing-patient-privacy>

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>

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) <http://www.privacy.org.au/About/Formation.html>
- Credit Reporting (1988-90) <http://www.privacy.org.au/Campaigns/CreditRpting/>
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) <http://www.privacy.org.au/Campaigns/Media/>