Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

14 April 2016

Paul Madden
Deputy Secretary and Special Adviser
Strategic Health Systems and Information Management EE

Dear Paul

Re: draft National Digital Health Strategy for Australia, July 2016 – June 2019

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

Please find attached our comments on the National Digital Health Strategy.

We have circulated early drafts to the other recipients of the draft strategy; however the views expressed in the attached document are those of the Australian Privacy Foundation alone.

We hope that this circulation of the draft strategy will be the first of many. The development of a national strategy such as this deserves consultation amongst a wide and diverse audience.

Thank you for your consideration.

Yours sincerely

Dr Bernard Robertson-Dunn

On behalf of the Board
Australian Privacy Foundation
Chair Health Committee
bernard.robertson-dunn@privacy.org.au

Submission to the Department of Health on the draft National Digital Health Strategy.

Australian Privacy Foundation
Date 14 April 2016

Contact
Dr Bernard Robertson-Dunn
Chair Health Committee
bernard.robertson-dunn @privacy.org.au

1. Executive Summary

This response to the draft National Digital Health Strategy for Australia, July 2016 – June 2019 is predicated on our belief that all information systems containing personal data represent a potential risk to privacy. However, that risk may be worth taking if the value of the system to the individuals involved outweighs the risk.

Our primary concern is that the value and benefits of the My Health Record system to consumers have not yet been adequately demonstrated.

Furthermore, making the system opt-out means that a large proportion of the population will have a health record with little or no value and as such represents a significant and un-necessary risk.

With regard to the draft strategy document, we contend that, as a strategy, it is flawed for reasons we discuss below, but just as importantly, its scope is skewed to the My Health Record project, not a strategy for identifying useful outcomes and associated issues as well as integrating access and privacy controls across the national electronic health record space. The latter is what a digital strategy must address, with the My Health Record as a subset of the larger picture.

On the strategy document itself we have several comments to make:

There are no References to Earlier Initiatives

The strategy seems to have been developed without reference to earlier initiatives. We specifically refer to the previous National Strategy issued in 2008[1], the Royle Review[2] and the large body of feedback on the eHealth Legislation in June 2015[3]. A number of key participants in the health, informatics and privacy domains expressed some serious concerns about the system and the proposed opt-out trials which appear to have been completely ignored by the Department since then. The feedback certainly has not been referenced or incorporated into the draft strategy.

In addition, we also draw attention to the considerations by several Senate committees regarding the eHealth bill of 2015. The Parliamentary Joint Committee on Human Rights and the Senate Standing Committee for the Scrutiny of Bills each raised significant concerns about the bill, especially regarding the proposed change to opt-out. Not including references to these committees, the issues raised and the way the strategy has incorporated the views of these committees is a significant and unwise omission.

The Purpose and Audience are Unclear

The purpose of the strategy is unclear. At whom is it aimed? The Federal government and its agencies? State governments as managers of health care facilities? State run health care facilities? Private health care facilities? Software vendors? Hardware vendors?

We suggest that the purpose of the strategy be made very clear, along with how the stakeholders at whom the purpose is aimed will be involved in both finalising the strategy and delivering it.

Our advice is to ensure that the purpose is directly linked to ways in which health care is made more effective first and more efficient second.

The Document Lacks Flow, Coherence and Analysis

The various sections of the document do not form a coherent, logical flow of evidential information, analysis, conclusions and initiatives. The content of each of the sections bear little, if any relationship with the others.

In addition there is no relationship between Digital Health – a technology enabler - and the problems and challenges of information management. Furthermore, the aims and objectives of information management lie in the delivery of better health care.

Turning this around, the need to deliver better health care through improved information management should be the drivers of Digital Health. Technology may offer opportunities for better use of data but it needs to be shown explicitly that this will lead to improved health care without unwarranted risks to privacy and that unintended consequences are minimized and that an approach to dealing with them is in place.

What is mainly missing is the linkage through information management through to improved health care processes and outcomes. There are some references to Digital Health and improved administrative processes, but the high value outcomes are more likely to be achieved from better health care decisions – a phrase that occurs only once in the draft strategy and only then in the context of engaging the patient.

The result is that, without a linkage to improved health care, the contents of Section 6 - Digital Health vision and Section 7 - Key strategic areas of focus lack justification and any explanation of why the particular objectives and initiatives have been selected and how they will achieve the vision.

This means that making an assessment of the value of the Vision, Objectives and Initiatives to Australians very difficult. It is our preference that a strategy as important as that driving eHealth in Australia should be based upon evidence, logic and analysis.

We recommend a cost/benefits analysis of the system should be undertaken to answer questions about the financial returns on the investments of the federal government, state governments, software vendors and medical practitioners.

With an estimated total cost over the first ten year period of the operation of the system of between $1.5-$2.0 billion, we are skeptical that improvements in health care that match that expenditure and which could be attributed to the system are achievable.

We would be interested in seeing the government's calculations and predictions as to when the financial benefits of the My Health Record system are expected to overtake the cost of the system.

Also missing in the draft strategy is any detailed analysis of capability or funding constraints or expectations. The draft strategy says that "government and the private sector is funding the development and delivery of local digital health systems", however, the strategy should be structured and predicated on the capability of the various parties and stakeholders to participate, not just state who will pay for it. Participation requires resources, both skills and financial. If the stakeholders do not have available the necessary resources, then the strategy needs to be tailored appropriately. A strategy that is not integrated into a known and agreed funding model is most likely to end up as shelf-ware or only partially implemented.

A National Electronic Health Record Privacy and Security Framework is Needed

A high priority for a strategy aimed at establishing trustworthy electronic health record systems (the My Health Record system is only one) for Australia should be elevating the issue of privacy, information security, confidentiality and access control. This means formulating a widely-accepted national framework to assist in dealing with these issues, solving the major problems in this area, clarifying how different schemes and protections fit together -- with an initial focus on secure, reliable clinical system intercommunication.

We suggest that the strategy be expanded to include such a framework.

As part of this framework, a priority should be to recognise the urgency to finally pass the long-overdue improvements to legal protection in this area, particularly what is often called the Tort of Privacy law, and the Data Breach Notification law. Without these laws, which are ready to go, the framework will lack necessary legal foundations to give confidence to patients and others that if something goes wrong, they will find out about it and could hold those responsible to account. At present neither is true.

Conclusion

In our opinion, the draft we have been asked to review is a start, however it requires major work before it could be seen as a useful document. The APF is more than willing to participate in its development.

We see the strategy as badly distorted by too much emphasis on the My Health Record, rather than the primary unresolved 'safe and easy communication' issues for the larger national eco-system of clinically relied-upon EHR systems, but we cover the MHR in some detail.

We are not convinced that the value of a national opt-out health database, paid for by the Federal Government, (which implies a strong degree of control) has been justified.

Neither are we convinced that the primary use of the database is to improve health care or efficiency.

The fact that the concerns about the usability, purpose and risks of the system raised by many institutions last year in the context of the eHealth bill have not been addressed has left the lasting impression that clinical support is not the driving force behind the government's intentions of the My Health Record project.

Background and context of the Strategy

Looking at the background and context, it is our opinion that that there are a number of areas that are missing.

1. There is no critical assessment of the National E-Health Strategy, 30th September, 2008[1]. Our view is that it is essential to look back at what was proposed, what happened and learn the lessons of the past seven or eight years. It is useful to understand what worked, what the obstacles turned out to be, what oversights or surprises turned out to cause serious impacts, and what could have been done better or differently.

   As an example, in the 2008 strategy, under 6.3.1 Connect and Communicate (1-3 years), it says:

   > In three years time, we will be able to measure the progress of the national E-Health Strategy for each of the key stakeholder groups as follows.
   >
   > Consumers
   >
   > - Consumers will begin to be able to be uniquely identified by the health sector through the rollout and initial adoption of the Unique Health Identifiers.
   > - Broadband connectivity is available to a vast majority of Australian consumers
   > - The national Consumer Health Portal has been implemented and consumers are beginning to use this as one of their primary online sources of health information to assist in management of their health care
   > - Consumers are seeing early releases of new E-Health solutions that allow them to begin interacting with care providers through online channels. Prescriptions are being transferred electronically for 10% of the population and 30% of pathology tests are being ordered electronically
   > - 20% of consumers of access to a limited form of electronic health record and 2-5% of consumers begin to access personal health information from initially available IEHR solutions.

   It is common knowledge that in 2011 the last two points most certainly were not achieved and it is arguable that the third was not either. In fact none of these three have been achieved after close to eight years.

   A full analysis of the National Strategy of 2008, where it succeeded, where it did not and the reasons for each, would be a useful guide in developing the current strategy.

2. There is no mention of the review of the Personally Controlled Electronic Health Record system by Mr Richard Royle released in December 2013[2]. It is surprising that this Review has not been referenced. As with the National Strategy of 2008, the Review is both a source of evidence for the (somewhat disappointing) roll-out of the PCEHR from 2012, and the driver for major initiatives now and in the near future. These include: the opt-out trials, using a privacy-hostile

opt-out approach to consent, of the re-branded My Health Record; and perhaps subsequent changes to the My Health Record system and its (in our opinion, poorly-governed) interactions with other government data systems.

3. There is no mention of the published submissions to the Department of Health[3] last June regarding the proposed eHealth legislation. We raise this because there were a number of relevant submissions from a range of organisations critical to the conduct of health care in Australia.

   We particularly note the submissions from:

   - The Royal Australian and New Zealand College of Psychiatrists (ANZCP);
   - The Australasian College of Health Informatics (ACHI);
   - The Health Information Management Association of Australia (HIMAA)
   - The Australian Federation of AIDS Organisations; and
   - The Royal Australian College of General Practitioners (RACGP).

   This first submission is particularly important as it raises a number of privacy risks for patients with mental health issues and the lack of built-in protections in the system.

   The APF also made a substantial, evidence-based submission to the eHealth legislation review[4].

   All of these organisations expressed a range of significant and serious concerns about the Personally Controlled Electronic Health Record (as it was then) and the proposed opt-out trials.

   These issues go to heart of the My Health Record system, its usability and the real risks to patient privacy and security.

   It is our observation that few, if any of the concerns raised by these knowledgeable and experienced institutions have yet been addressed.

4. There is no mention of the opt-out trials of the registration of people into the My Health Record.

   The question of the resort to opt-out, a consumer- and privacy-hostile model of recruitment that would not be appropriate for any medical procedure or experiment, is a critical question to address. The failure to effectively persuade citizens of either the benefits or the safety of the earlier Personally Controlled Electronic Health Record was presumably behind the low take up rate for this government-controlled electronic health record, and the adoption of a scheme which puts the onus on individuals who do not want a record to try to prevent it being created. It is also troubling that the Attorney General's Department is involved, an agency whose focus is policing and national security not sensitive medical information.

   We contend that putting the responsibility to opt-out onto individuals is oppressive, especially when the aim of the My Health Record is clearly to link the record with many other records in government hands.

5. There is no mention of the concerns raised by The Parliamentary Joint Committee on Human Rights and the Senate Standing Committee for the Scrutiny of Bills.

   We quote from the report of the Parliamentary Joint Committee on Human Rights[5] page 72

2.85 The question raised by the committee was what is the reasoning or evidence that establishes that the objective behind the opt-out model is a legitimate objective; in that it seeks to address a pressing or substantial concern. In relation to this, the committee notes the minister's response that under the current rates of participation for My Health Records, healthcare providers generally lack any incentive to adopt and contribute to the system, thereby limiting the usefulness of the system. The minister also notes that currently roughly two-thirds of healthcare providers use paper based records and increased registration with, and use of, the My Health Record system would encourage the use of healthcare providers to use electronic records for their patients in the My Health Record system. The minister also states that increased use of the My Health Record system will deliver cost benefits to the healthcare system, which will occur more quickly under an opt-out model than the current opt-in model.

2.86 Reducing costs to the healthcare system is likely to be a legitimate objective for the purposes of international human rights law. However, the committee notes that the minister's response does not provide any evidence to demonstrate that increasing numbers of persons registered on the My Health Record system would in fact reduce healthcare costs.

2.87 However, even assuming that the opt-out model would result in increased use of the My Health Record system by healthcare professionals, and thus reduce healthcare costs, the committee remains concerned that the means to achieve this increased usage may not be proportionate to the objective sought to be achieved. In particular, no information is provided by the minister as to why the current opt-in model has not succeeded, and whether there are other methods available to ensure more people voluntarily decide to include their health records on the My Health Record system. This is relevant to the question of whether there are other less rights restrictive ways to achieve the same aim.

2.88 The minister's response states that people in the initial trial locations will be notified by letter that their personal health information will be automatically uploaded on the national register. However, no detail is provided as to whether this will provide sufficient detail to people to allow them to be fully aware of their rights to opt-out of the system. The committee reiterates that the bill itself does not set out any safeguards to ensure that healthcare recipients are given reasonable notice or a reasonable amount of time to decide whether to opt-out.

2.89 The committee also notes the minister's statement that the move to automatically upload everyone's personal health records onto the national database is 'likely to improve privacy' for individuals, as it will decrease reliance on paper records. However, it is not apparent that including all personal health data on a centralised national database would better protect privacy – information on government databases also run the risk of being inappropriately accessed, and including more personal information that can be accessed by more people is not likely to improve the right to privacy for individuals.

These are major and significant concerns raised by an important and knowledgeable body. To ignore them in developing and formulating a National Digital Health Strategy is most unwise.

6. There is no check-point assessment of the cost/benefit of the Personally Controlled Electronic Health Record/My Health Record initiative after nearly four years of operation.

The Department of Health should have a good idea of how much has been spent and what the plans are for the next five years. It also should be possible to estimate the cost to the health industry of implementing and maintaining the My Health Record component of their compliant systems and the ongoing costs of managing health information.

This would give an estimate of the total cost of the My Health Record system up until the end of the strategy planning period.

For benefits, we suggest that a bottom up approach is preferable to the previously use, but hard to defend, assumption that IT applied to heath will return similar benefits. Health care is not like manufacturing.

A useful approach to benefit analysis could be to define (say) ten use case scenarios, and for each say how many times each is expected to occur per year and then estimate the reduction in health care costs of that scenario that can be attributed to the existence and use of the My Health Record.

All this analysis should be in support of a cost/benefits analysis of the system which we believe should be undertaken to answer questions about the financial returns on the investments of the federal government, state governments, software vendors and medical practitioners.

With an estimated total cost over the first ten year period of the operation of the system of between $1.5-$2.0 billion, we are skeptical that improvements in health care that match that expenditure and which could be attributed to the system are achievable.

The only really important measure of the system is the number of times health records have been downloaded and used as part of health care episodes. These numbers could then be used as the basis for further work to understand any subsequent reduction in health care costs of the whole system over time.

Our suggestion is that the general principle should be that a cost plus risk versus benefit analysis should be a part of progress review of existing major initiatives like the My Health Record, and a clear articulation of the claimed or hoped for benefits should be possible after four years, with initial estimates and actuals to compare with; and that on the cost side, it is important to identify risks, and risks projected onto others, as factors to take into account.

We acknowledge and understand that governance of deciding whether benefits now and in future outweigh costs and risks now and in future is a major and difficult topic. Proper identification of prospective and historical factors which should be taken into account in a cost plus risk versus benefit assessment for electronic health records in general is not a well-resolved process. However, it is important that this requirement to identify the proper basis for an assessment should feature in the strategy.

7. We note that the Internet of Things has a mention in section 5, The need for a National Digital Health Strategy: “The Internet of Things offers real potential to have a major influence on revolutionising healthcare delivery.” The next mention is in the glossary.

   If the Internet of Things offers real potential, it would seem logical to include it in the strategy. Medical devices are covered, but the concept and issues of The Internet of Things is much greater than just devices. Issues of public safety, privacy and security are already major areas of concern and will grow over the time frame of the strategy.

   We recommend a careful approach to integrating internet technology enabled devices into hospital and pathology systems. Furthermore, allowing smartphone and other user devices to interoperate directly with the My Health Record is a direction that has enormous potential security and privacy risks. As with the My Health Record system itself, we do not believe that the value and benefit to Australian patients and consumers has been demonstrated. We cannot assess the risks of such initiatives because there has been no information provided as to their architecture, designs or security features. We suggest that these should be widely circulated among specialist disciplines for comment and feedback before any firm initiatives undertaken.

In addition to the above observations concerning those matters we believe are missing from the strategy, putting section 9, "National foundational digital health capabilities" at the end makes little sense. This section should be an input into the strategy itself and therefore should be moved toward the front of the document and be integrated into the narrative.

3. Digital Health Vision and Objectives:

The draft strategy has this as the Vision of Digital Health:

> The individual is placed at the centre of healthcare. Individuals and their healthcare providers are supported through the availability of up-to-date, accurate and reliable health information about the individual's health. Digital health solutions will enable a safe, high quality and more cost effective health system for all Australians.

We do not understand why these statements have been chosen as a Vision for a National Strategy for Digital Health. They are difficult to relate to anything in the document either before or after.

In a strategy document such as this one, the vision should be the cornerstone of the whole document. It should be clear why it has been selected, and the strategy should explain the value and benefits of the vision. In addition, the strategy should discuss the problems and challenges of achieving the vision followed by initiatives that deliver the vision with clear linkages to the vision.

There also needs to be a discussion on the issue of resources required to implement the strategy. Evidence should be obtained as to the capability and funding constraints of the stakeholders who are required to participate in, and implement the strategy. Participation requires resources, both skills and financial. If the stakeholders do not have available the necessary resources, then the strategy needs to be tailored appropriately. The strategy should also make clear the resource expectations that are inherent in the strategy, specifically those on which the objectives and initiatives are based. In our view it is not sufficient to simply say "government and the private sector is funding the development and delivery of local digital health systems and this strategy can be used as a guide for both the health and technology sectors in the planning of activities to ensure that local digital health solutions are developed to enable information interoperability at both the local and national level". There is no point in having a strategy if it can't be funded.

The Digital Health Vision is followed by a set of objectives that, like the vision, have no obvious or logical relationship with anything mentioned previously in the draft strategy.

There is no discussion of options, no rationale for the objectives, no analysis of the value of the objectives, no discussion of potential problems or challenges that will need to be addressed in achieving these objective, no identification of the stakeholders and their capability to participate in achieving these objectives, no high level plan, no high level timeframe, no cost estimates or constraints.

In our opinion, a strategy document should discuss all these issues before identifying specific initiatives. That way the initiatives can be assessed in the context of the objectives.

As they stand, in our opinion, the Digital Health Vision and the Objectives are statements of motherhood, lacking in context, logic, or any indication of the value to the government, consumers or the health industry.

An important way to ensure that the strategy's Digital Health Vision and Objectives are well formed is to articulate the different interests of the main stakeholders, with patient and citizen interests foremost. This is to counter the observed dominance of large institutional interests in the health care area. This approach should include both positive interests in what the stakeholder wants to happen, and negative interests in what to avoid, what existing benefits they seek to preserve from potential disruption.

The priorities that drive the Digital Health Vision and Objectives should not just be those of the government or the "health system" but the whole ecosystem, with patient interest's foremost, and acknowledgement of potential conflicts of interest with other players like governments, clinicians, other health sector service providers, and parasitic internet intermediaries like global marketing companies like Facebook and Google.

4. Key strategic areas of focus

This section commences with:

> "The strategy comprises seven key strategic areas of focus. These seven areas of focus have been determined based upon an assessment of the current health system challenges, undertaking an analysis of the likely changes to healthcare delivery in the next ten years, and undertaking an alignment to the current health system priorities."

The details of the assessment need to be included in order to make clear why the areas have been selected and the implications to the rest of the strategy.

5. Need for a national agreed privacy and security framework for health record access

We reiterate past concerns that the My Health Record system needs to have an overarching national framework for electronic Health Record privacy, personal info security, confidentiality and patient-respectful access control, covering the principles on which all Australian electronic Health Record systems, and all interconnections between them and with third parties, should be based. There appears to be no public and understandable document of this type.

Our view is that this draft document does NOT rise to the challenge of setting out a comprehensive, high level strategy and framework for electronic Health Records dealing with these most important unresolved issues: privacy, personal information security, confidentiality and patient-respectful access control. And we draw your attention to medical opinions that are opposed to any form of patient control. This is a critical issue that needs to be resolved via consultation and co-operation with the medical community, the ultimate users of the system. Its importance is such that if it cannot be satisfactorily resolved, it is unlikely that My Health Record, in any incarnation will be used to any meaningful extent.

Further, we maintain that the generic system interaction level issues between the various stakeholders are not adequately considered. We have no time here to comprehensively address all the missing connectivity aspects in need of guidance, but they would be a necessary foundation for such an electronic Health Record framework. This would need to be widely understood, consulted upon and agreed, in particular by the patient and civil society stakeholders who will carry the risk of breaches and misuse.

6. Missing legal protections

We note also that patients and the Australian community still, after many years of viable recommendations being on the table, do not have the benefit of laws covering the following matters which would offer protection in relation to electronic health records:

- A private legal right action to redress serious intrusions of privacy, as recommended by two ALRC reviews but ignored by three governments;
- A mandatory data breach disclosure notification law, a promised condition for passing the communications data retention law in 2015 but still not in place; and
- A comprehensive update of medical and health information provisions of the Privacy Act, as recommended by ALRC (but ignored in favour of fragmented, uncoordinated and privacy-hostile laws like those for the IHI and PCEHR/MHR).

Taken together, this lack of action to implement protections taken for granted elsewhere seems to demonstrate an active hostility to giving Australians effective legal protection of their privacy and personal information security interests. It also leaves patients, their families and the broader community exposed to the potential harms and risks of electronic and online health records being misused without the essential legal remedies enjoyed in other, more privacy-respectful countries.

Any policy progress in the electronic health record or digital medical data area will be illusory until these necessary and overdue protections are finally in place. Until then, patients (and others) may be well advised to remain conscious that basically 'you are on your own' if anything goes wrong with the sensitive information in electronic health records.

7. Initiatives

A strategy should be a composite set of integrated, interconnected, logical ideas, options and rationales. It should be possible to map each initiative, its benefits and measures through a chain of arguments through to the overall purpose of the strategy.

We respectfully suggest that the current strategy document does not match this expectation.

It is difficult to assess the suitability and appropriateness of the proposed initiatives and the claimed benefits primarily because there is no explanation of how an initiative will achieve an objective and how the benefits will be delivered.

An initiative is a solution to a problem or challenge. These have not been identified or described.

As an example, taking the first initiative and the objective it is supposed to support:

> Objective 1. Provide individuals with electronic access to the information needed to better manage and control their personal health outcomes, maintain health and wellbeing, improve health literacy, and enable them to capture and securely share that information.
>
> Initiative 1. S1.1 Software vendors in partnership with consumers, healthcare providers and organisations will design and implement digital health solutions aimed at delivering person centred care.

This description is lacking in many details, including: that it does not explain how it will enable some or all of the objective to be achieved; it has no owner; it has no cost estimates: there are no guides to what the digital health solutions might be or even should be in order to integrate with the overall strategy and other initiatives; there is no priority allocated to it.

The case studies are interesting anecdotal examples of activities, but they lack hard data and need to be related much more tightly to the initiatives and objectives. Most of the statements in the case studies are just descriptive; they do not provide insights or lessons which future actions can leverage.

It is our recommendation that the initiative should be presented in a common framework.

For each initiative there needs to be:

1. The objective(s) it is intended to achieve;
2. A description of the benefits and value to be delivered, along with meaningful measures of them;
3. How delivering the initiative will achieve the objective(s). This needs a level of detail more than just a statement that it will achieve it or them;
4. A description of the initiative that would allow a high level costing to be completed; an owner to be allocated; stakeholders and other parties identified; challenges and difficulties outlined, along with how they will be overcome;
5. A description of the capabilities of the various parties who will be required to deliver the initiative;
6. An assessment of the risks associated with the initiative, including the risk that the initiative may have flaws or not achieve its intended outcomes.

Once all the initiatives have been properly justified and analysed, there should be a further analysis of any interdependencies and associated risks at that level.

The needs, wished for benefits, and risks to be avoided that underpin the initiatives need to be developed and agreed with multiple stakeholders.

Furthermore, the drivers for, and the development of, the initiatives should be the main focus on the strategy. If you don't pick the right problem and address the associated challenges, initiatives may offer solutions that are not relevant or do not work.

Starting from a particular assumed "problem" can however imply the scope of its solution. So it's important to explicitly identify the range of potential problems that could be addressed; to develop this understanding in a logical progression from context, interests and values, with feedback from those affected; and to base the final priorities for the problems to actually target on an open comparison between all potentially relevant problems, with patient and clinician interests uppermost. The solutions, the features of the privacy and security framework, and particular initiatives will then follow more coherently.

8. Consultation Process

In our opinion and experience consultation, with the Department of Health has been largely one of "we talk, the Department does not listen".

This is borne out by the apparent lack of interest in the submissions made to the department regarding the eHealth Legislation last year. Some serious issues were raised by many knowledgeable and experienced bodies but there is no evidence that any have been addressed. This is a major concern and we trust that a better outcome will result from this current exercise.

9. Conclusion

For a strategy intended to deliver something as important as improved health care, it needs to be crystal clear why it is being undertaken and how it will achieve its objectives. It should provide a high degree of confidence that it has been well thought through, is credible and achievable and that most, if not all, potential difficulties have been identified and mitigated against.

It should also be fully integrated into previous initiatives, feedback and current thinking in the domain of interest.

A strategy should comprise a context, an overall vision, a discussion of potential objectives including challenges and problems expected to be encountered, a set of objectives that will achieve the vision and why they have been selected; a set of initiatives that, when implemented will meet the challenges and solve the problems

Our view is that the draft strategy requires a significant amount of work to bring it up to the standard expected of such a critical document.

In doing this reworking, one related element needs urgent attention. A key element for a strategy aimed at establishing a trustworthy electronic health record system for Australia should be elevating the issue of privacy, information security, confidentiality and access control to the forefront. This means formulating a widely-accepted national framework to assist in dealing with these issues, solving the major problems in this area, clarifying how different schemes and protections fit together -- with an initial focus on secure, reliable clinical system intercommunication.

There is probably more long term value and greater benefit in this focus than in a focus on an expensive government-controlled duplicate health record system which is not designed to meet the critical challenges of clinical practice. A system which has been developed before such a national electronic Health Record data protection framework is in place, and which puts the needs of third parties above those of patients and their clinicians.

We encourage the work to develop such a framework and to fill in the other missing elements of a strategy to be taken up as a priority, but for it to be done properly. We look forward to contributing to a review of the next version, one which at least lays out the bones of an integrated, widely-agreed national electronic Health Record privacy and security framework, builds more on the work done already by others, and provides the depth and analysis missing in this draft of the Strategy.

10. References

[1] National E-Health Strategy, 30th September, 2008
http://ozhealthithistory.wikispaces.com/file/view/National%20E-Health%20Strategy%20REPORT%20-%20Final%20Release%20300908%20v1.pdf

[2] *Review of the Personally Controlled Electronic Health Record*
Richard Royle, Released December 2013
https://health.gov.au/internet/main/publishing.nsf/Content/17BF043A41D470A9CA257E13000C9322/$File/FINAL-Review-of-PCEHR-December-2013.pdf

[3] eHealth Submissions 2015
https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/consultation-submissions/

[4] APF submission to the eHealth legislation review
https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/consultation-submissions/$FILE/060%20-%20Australian%20Privacy%20Foundation.PDF

[5] Parliamentary Joint Committee on Human Rights
Human rights scrutiny report
Thirty-second report of the 44th Parliament
https://avn.org.au/wp-content/uploads/2016/03/Joint-Parliamentary-Committee-into-Human-Rights-Final-Report-on-Adult-Register-Bills-01-December-2015.pdf

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/