**Australian
Privacy
Foundation**

5 September 2018

Submission to the Senate Inquiry into My Health Record

Table of Contents

**Australian
Privacy
Foundation**

1 Background

This submission is the distillation of contributions from members of the Australian Privacy Foundation. It is informed by experience in privacy, security, public sector administration, large scale government Information Systems development, medical science, health care practice and law.

The primary author of this document is Dr Bernard Robertson-Dunn who can be contacted at Bernard.Robertson-Dunn@privacy.org.au

Further information regarding My Health Record, ADHA's opt-out initiative and the APF's response is available here: https://privacy.org.au/campaigns/myhr/

2 Key Points

2.1   Overall

My Health Record is a major and unnecessary risk to privacy. It has little or no benefit to the average Australian; its costs and risks are significant and deliberately understated by the ADHA.

The government is inserting itself into the relationship between patient and health provider and as such is distorting the balance of trust that is essential for effective health care.

This nor any other government can guarantee that they will not change the legislation in the future to enable it to sell patient data, link data or misuse health data.

My Health Record does not meet the needs of either health professionals or patients. It is primarily a secondary, summary system - and even then it is totally reliant on patients and GPs uploading that data. It is has features (such as patient control) that severely diminish its utility for both sets of users. It reduces the efficiency of health workers, especially GPs, requires a significant investment in time and effort from patients to input and manage data and is of little value to most Australians.

The cost of running My Health Record after opt-out is implemented is estimated at over $1billion per annum; approximately three times the government's claimed (but unjustified) benefits. This is in addition to the more than $2billion the system has cost so far.

As a centralised, national, government owned and controlled database of personal and private data connected to a many thousands of other, less well protected privately operated and controlled systems, it is open to abuse and misuse.

For those patients who require access to their medical records there are simpler, safer and cheaper methods of achieving this.

For those patients for whom immediate access to important medical data may be of benefit e.g. to indicate to emergency workers that they have unusual or critical care requirements, there are simpler, more reliable and safer methods of achieving this objective.

There are existing apps that deliver much more to patients than My Health Record ever can. For example, see the information on NPS MedicineWise in the section "Alternatives for people/patients to access their health data", below)

My Health Record is a non-real-time system, which makes it unsuitable for applications such as prescription monitoring. This has been recognised by the states who are developing and implementing their own prescription monitoring systems. It is also highly probable that having multiple systems with different data regarding prescriptions and medications could cause confusion and delays in providing treatment.

My Health Record is a non-high availability system which makes it un-reliable and unsuitable in times of critical, high volume medical emergencies. Systems that are local to the point-of-care are far more suitable and reliable.

Legislation does not and cannot protect the security and privacy of the data, all it can do is to punish those who actually get caught.

My Health Record is an unreliable, potentially inaccurate, usually incomplete and misleading historical medical record of a patient's interaction with the health care system. Digital Health should enable a reduced workload on health providers, facilitate better data acquisition at the point and time of care to support more effective and efficient medical decision making. My Health Record increases the workload of, and is of no benefit to, the majority of health providers at the point-of-care.

My Health Record will disenfranchise approximately 25% of all Australians who do not have the skills, technology or ability to manage their records

The Government has failed to properly inform all Australians of the move to opt-out, has only provided minimal information on My Health Record, claimed unjustified benefits and nothing about the significant costs and risks of the system.

The ADHA is currently planning to completely re-design and re-implement My Health Record; after more than six years and a cost of over $2billion. This is an implied admission that it has not achieved the outcomes that were claimed for it when originally approved. There is no indication that the ADHA or the Department of Health have learned the most obvious lesson from its failure – that the basic premise that a secondary, summary, government owned non-point-of-care system is totally unsuitable to today's modern health care system, never mind provide a platform for the long-term future of patient centric medicine.

2.2   Patient's Perspective

From a patient's perspective, My Health Record is not integrated with systems that support their health providers. A patient's experience with the health care system is much more than just a summary of their historical medical records. For example when dealing with their GP, a patient may wish to make use of appointment booking and online repeat prescription ordering facilities.

The government makes many claims as to the benefits for patients of the My Health Record, yet fails to inform patients of their role in inputting data and keeping it up to date, of the costs and the risks of the system.

There are many alternatives to My Health Record that are cheaper, simpler, better and which do not involve giving health data to the government.

The Federal Government's Health Care Homes initiative has as a mandatory condition that patients have a My Health Record, or be eligible and willing to have one. [1]

GP and former AMA president Dr Kerryn Phelps claims that the demand for patients to sign up to the national health database to access Health Care Homes support is unethical [2]. "I have massive ethical concerns about that, particularly given the concerns around privacy and security of My Health Record. It is discriminatory and it should be removed," she said

There is no guarantee that the government will not widen the scope of service that mandate My Health Record to include all Medicare/ Centrelink/ Welfare services.

2.3   Health Provider's Perspectives

Responses to a Medical Journal of Australia poll "My Health Record: staying in or opting out?" shows that 70% of their readers will opt-out.

18% of respondents to a Medical Journal of Australia poll agreed with the statement "My Health Record will improve patient outcomes".

The government has failed miserably to engage with, and obtain the support of, the most critical segment of the community involved in Health Care – health providers. These are the people who are required to input data into the system and who are expected to make use of the data. Their

privacy is also at risk. There is no recognition or legislated protection afforded to all the health professionals who may be identified via a patient's My Health Record.

GPs are not convinced that the government has a) demonstrated that the system has any benefit to them b) that they government has fully informed them of the costs risks and other aspects of the system that will impact their ability to provide effective and efficient health care to patients.

Use of the My Health Record is not supportive of efficient workflows and will cost many GPs significant unpaid time and effort.

2.4   Changes to the Legislation

These do not go far enough.

The first change to "remove the ability of the My Health Record System Operator to disclose health information in My Health Records to law enforcement agencies and government agencies without an order by a judicial officer or the healthcare recipient's consent;" treats the ADHA, a government agency, as a special case. The ADHA, the System Operator, has access to all the data in My Health Record. This is a paradox that can only be resolved by the government not holding health information in My Health Records.

Notwithstanding the first change, the second change to "require the System Operator to permanently delete health information stored in the National Repositories Service for a person if they have cancelled their registration with the My Health Record system – that is, they have cancelled their My Health Record" does not address the issue of deleted or updated documents in a current My Health Record being hidden, but not visible to patients. These documents should also be deleted.

2.5   The future of Health Care

My Health Record does nothing to address the real problems facing the health care industry. These include reducing the siloed nature of the health care system, facilitating the journey of a patient through the system, focusing on and moving toward patient centric care, not on processes or data, advances in treatment that address the causes of illness and health conditions rather than a statistical, risk based approach that is predicated on correlation and symptoms.

My Health Record is a dumb document management system with little clinically useful data and is an IT relic of the past.

2.6   Alternative to My Health Record

The UK's Summary Care Record has similar health care objectives to My Health Record (see below for more details) without the distorting effects of patient control or dependencies. The SCR does not require giving patient health data to the government; automatically collects data from GP's systems and can only be accessed by health providers. It has clear, focused boundaries and benefits at much lower cost and risk.

2.7   Recommendations

The move to opt-out should be halted at the end of the period in which Australians can inform the government that they do not wish to be registered for a My Health Record.

A proper review of the system, its objectives, risks, implementation, impact on Australian health care, value, projected costs over the next 100 years and alternative approaches should be conducted by a body independent of the ADHA, the Department of Health, or any other participant with a vested interest in its outcome.

It is the informed opinion of the APF that the only sensible outcome of such a review is likely to be to abandon the system.

**Australian
Privacy
Foundation**

3 Additional Information

3.1 Support for eHealth

We do not question the goals of eHealth or even of Health and Medical Records, it is the means by which the government is attempting to achieve those goals that we take issue with. The consequences, both intended and unintended are significant, are not fully understood by the government and most certainly have not been communicated to the Australian People.

Health care could and should be made more effective and efficient. Those patients who want access to their health records should be able to get it. However, there are better, safer and cheaper ways of achieving these objectives without first giving the data to the government. It is un-necessary and has major negative consequences.

It needs to be remembered that medical and health recordkeeping are essentially administrative tasks. Recordkeeping is neither necessary nor sufficient for good health care.

Sharing health data with your trusted health care professionals is a good thing. Giving it to the government is quite another; you never know what they will do with it and you don't know what policies a future government may enact.

My Health Record is the wrong solution to the wrong problem

The problem is not historical record keeping; the problem is better health care decisions. This requires a wide range of quality, current, accurate, detailed information at the time and point of care; not old historical, potentially inaccurate, summary data that is costly to acquire and manage.

Quality information comes from improved diagnostic tools and protocols; it comes from advances in science and engineering, not blind adoption of technology and a reliance on the patient.

Improvements in health care will come from systemic changes to the health care system as a whole, from better access to patient data at the point and time of care and from treatment that addresses an individual's condition rather than the current risk reduction approach prevalent in much of today's clinical medicine.

eHealth, or more accurately, automation supported by information systems and dynamic analytical tools, has much to offer. Better document management of historical data is a costly distraction from the main game. My Health Record does not even offer better document management.

3.2 Why should the government have access to an individual's health data?

This question goes to the heart of the My Health Record System. When designing the PCEHR the designers had a choice. Either link existing health care systems, improve the exchange of health data between them and do not store data in the process, or build a centralised, government owned and controlled database that collects copies of health data from other systems. The designers chose the approach that gives patient data to the government. Why it chose this approach has never been made clear.

The UK tried building a nationwide, centralised database similar to that of My Health Record that automatically extracted data from GP systems. After this initiative failed to gain public acceptance it was halted and a review of data sharing was conducted by Dame Fiona Caldicott. This and the government's response resulted in a set of principles (see section "The UK Experience" below)

The most relevant of these principles is number 4, "Access to personal confidential data should be on a strict need-to-know basis":

> *Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.*

The Australian Federal government has no need-to-know an individual's personal confidential health or medical data. Unlike the UK NHS it does not deliver health care services. In Australia the Federal government is entitled to acquire, analyse and utilise aggregated, population level data to develop funding and regulatory policies. It has no need for personal health data.

The government may claim that My Health Record data will not be shared with government agencies, but it cannot be disputed that the ADHA, as the System Operator, has unfettered, unlogged access to an individual's personal confidential data.

The only way for the Australian people to be confident that the government cannot possibly access and/or misuse their personal confidential data is for the government not to collect it in the first place.

3.3   Medical, Health and Patient Data

Medical Records, Health Records and Patient Records are different concepts and have different uses.

1. When a GP or specialist interacts with a patient, the health provider needs to keep track of that interaction: history, test results, diagnoses, treatment plans, etc. This is a Medical Record and it is primarily for the benefit of the health provider. It is in their language and is part of the on-going process of patient medical treatment. It is not a health record; it is a record of treatment.

2. Hospitals need to monitor the status and progress of the patients they are treating. When the patient is discharged, most if not all responsibility is transferred to someone else. That transfer should be accompanied by an appropriate hand-over. The old data is virtually useless. The patient has (hopefully) recovered, hospital data is of little value without the wider context of the health data held by other health providers. Like GP records, hospital records are also Medical Records.

3. Patient or Health Records are usually defined as medical records with additional, non-medical data that provide additional information and a wider context.

   As an article in the New Yorker put it:

   > *"We have at least four kinds of information that matter to your health and well-being over time: information about the state of your internal systems (from your imaging and lab-test results, your genome sequencing); the state of your living conditions (your housing, community, economic, and environmental circumstances); the state of the care you receive (what your practitioners have done and how well they did it, what medications and other treatments they have provided); and the state of your behaviors (your patterns of sleep, exercise, stress, eating, sexual activity, adherence to treatments). The potential of this information is so enormous it is almost scary."* [3]

   My Health Record is not a Medical Record, is not a Health Record nor is it a Patient Record.

3.4   Benefits

The government claims that: "My Health Record is an online summary of your key health information" and "Your health information in one place". However, the government's own statements make it clear that it will start off empty, will not contain your medical history or older tests and you need to be involved in the collection of your health data from people already have it.

> *"What to expect when logging into My Health Record for the first time*
>
> *The first time you log into your My Health Record there may be little or no information in it. There may be up to two years' worth of Medicare information such as doctor visits under the Medicare Benefits Schedule (MBS), as well as your Pharmaceutical Benefits Scheme (PBS) claims history. If you choose, you can remove this information after you log in.*

Information will be added after you visit your GP, nurse or pharmacist. You can add your personal health information and notes straight away." [4]

and

"Your previous medical history such as older tests and medical reports will not be available within your new My Health Record" [5]

If you don't see your GP and/or your GP does not spend a significant amount of time discussing with you the costs and risks of heaving a My Health Record, you will not have one, or you will have one with no medically useful data in it. The government's claims that uploading a Shared Health Summary should only take a few minutes and involves just a couple of mouse clicks, fails to acknowledge the AMA's guidelines for managing the PCEHR/My Health Record, a document of 27 pages.

One of the major goals of My Health Record was to reduce fragmentation of health data by facilitating better access to a patient's health data for the benefit of both the patient and their doctors. In this it fails miserably. My Health Record is a summary system it will not contain historical data or test results and requires patients and their GPs to add data.

No realistic figures have been released by the government that demonstrate benefits to patients or the health care system.

The ADHA sporadically releases statistics on registrations and uploads of documents to My Health Record [6]. They have not released any data on the number of times a My Health Record has been downloaded and used in an emergency situation (for example) or how it has reduced the cost of health care.

Of the 6 million registrations for My Health Record only about 20% have a Shared Health Record. So far this year approximately 640,000 Shared Health Summaries have been uploaded. This implies than fewer than 11% of Shared Health Summaries are current.

There is a page on the ADHA website with the title of Benefits Realisation. [7]

It poses the question:

"How are benefits realised?"

and provides an answer:

Technology drives positive changes to the way people work. These positive changes in behaviour (e.g., changing the process to complete a task or changing the tools to support a process) are what drive benefits realisation. For the My Health Record system, these elements include:

uploading of information to the My Health Record system from clinical information systems

a larger proportion of Australians with a My Health Record

healthcare organisations being connected to the My Health Record system to allow viewing and use of the information in the system

supporting clinicians and individuals to understand how to view information in the My Health Record system.

The implementation of the above elements in combination with positive changes in behaviour of both clinicians and individuals drives benefits realisation.

This statement is meaningless and nowhere is justified. It is classic motherhood and has more in common with cargo cult culture than hard-nosed, evidence based analysis.

Technology is a powerful tool, if used appropriately. It might deliver benefits but always comes at a cost. Nowhere on the ADHA website is there any justification for the claimed benefits or what the compromises and trade-offs are in delivering the claimed benefits.

Similarly, nowhere on the ADHA website is any discussion of the costs and risks of My Health Record.

Neither is there any data on real, concrete benefits to patients and/or health care providers that have been achieved in the six years the system has been in operation.

All My Health Record has done is increase fragmentation and put Australian's health data at security and privacy risk with minimal, if any benefits, to the majority of Australians, either patients of health providers.

The only viable conclusion is that My Health Record has little benefit to anyone and of no benefit at all to most Australians

3.5 Costs

The review of the PCEHR in 2013 [8] that resulted in the transition to opt-out, estimated that a summary health data system could have a benefit of $400m/year if everyone had one.

There was no mention in the report of the cost of transitioning to and maintaining an opt-out, summary health data system. This has been a feature of the whole health record initiative. There has been no published estimate of the costs of maintaining and using the PCEHR / My Health Record.

A quick analysis gives an indication of the some of the expected major costs of My Health Record. Based upon published government statistics (e.g. there are over 400,000 GP visits per day), it is estimated that, if everyone had a health record and it takes 3 minutes to keep up to date after every GP consultation, the cost would be between $500m and $1billion. That is just the GP data entry costs.

Including other costs such as those of GPs reading and interpreting My Health Record data, hospitals, specialists, pharmacists, the ADHA etc, suggest that the existence and use of My Health Record will be between $1 and $2 billion per year – effectively for ever. This is in addition to the cost so far of My Health Record and the transition to opt-out which is estimated at well over $2.5 billion.

Furthermore, the ADHA has a project underway to "re-platform" My Health Record. According to the material distributed to prospective vendors, it is to be a complete re-development of the system. It is unlikely to cost much less than the original system, in part because it will now need to address the transition cost of migrating the system and its data to the new solution.

For this enormous cost to be sustainable, My Health Record would need to deliver significant improvements in the efficiency and effectiveness of health care. It would also need to replace existing systems by being more comprehensive, more reliable and more complete.

Unfortunately, it is the nature of health care that it is essential that doctors be supported by local systems that could cope with emergencies (e.g. epidemics, bio-security/hazard incidents etc) and the potential failure of communications and power that are characteristic of centralised systems such as My Health Record. This requirement means that the most sensible and safest approach is to provide support systems that are co-located at the point of care. The obvious conclusion is that My Health Record can never replace local systems; it can only ever be a second level, support system not a front line, critical clinical system.

In other words no matter how much is spent on My Health Record, it will always be an additional cost to the government and the health care industry, not a mechanism for reducing costs or improving efficiency of health care.

3.6   Is My Health Record useful for research?

An argument has been put forward for using My Health Record data for research. This is naïve and suggests a worrying misunderstanding of the nature of the data in My Health Record and of much better sources of research data.

My Health Record contains, at best only selected summary or test data with no context. It can also be distorted by the patient through hiding data or prohibiting certain data from being uploaded. If the experience of the last six years is any guide, most will probably be empty.

More useful data is in the systems used by health providers.

3.7   Emergency Use

It is claimed by the government that My Health Record will be invaluable when a patient is involved in an emergency. This is a dubious claim with no justification and has never been seriously examined.

There are other approaches that have been available for many years and which offer obvious benefits over an IT system like My Health Record. These include but are not limited to the MedicAlert system.

Their website says:

> *MedicAlert is more than an ID*
>
> *When you become a member, you'll also receive a secure electronic health record that you can update to include any new or relevant medical information.*
>
> *This can then be accessed by emergency personnel and health professionals at any time via our lifesaving 24/7 Emergency Response Service. Our trained professionals will provide vital information about your health, medical history or current conditions, ensuring that you're treated quickly and efficiently or returned home safely to loved ones. [9]*

[The APF does not endorse and has no connection or arrangement with MedicAlert system and is reliant on their website for information about the product]

A person who is seriously concerned about emergency situations and who is wearing a MedicAlert bracelet is immediately identifiable to health workers who immediately know two things: a) that there is a potential issue to be considered and b) where to go for more information. This is a positive indicator.

With the My Health Record system, health workers need to go looking for evidence in the patient's My Health Record to identify if the patient is at risk. This can be time consuming and suffers from the problem that "Absence of evidence is not evidence of absence,"

A MedicAlert (or similar) solution provides immediate, positive evidence and delivers additional services other than access to raw data; relying on My Health Record is both time consuming and is unreliable.

![Australian Privacy Foundation logo]

3.8 Other Digital Health Initiatives.

In the review of the PCEHR in 2013, [8] use was made of a report from a presentation at a Healthcare Information Management Systems Society (HIMSS) conference in 2013 which quoted a Booz & Company National eHealth Benefits Model [10] to justify the move to opt-out. The HIMSS conference publication contained the following graphic (Figure 1), although the PCEHR review omitted the reference to the PCEHR:

Direct benefits from digitizing the healthcare sector can be measured – the challenge is realization

Australian Steady-State Annual Benefits by eHealth Application
(AU$ M, Year 2020, assumes full eHealth scope and international benchmark adoption rates)

Total = AU$7.6 billion

Potential benefits of PCEHR alone assuming adoption

Summary Care Record: $0.4
Decision Support: 0.5
Patient Self-Management: 0.9
EMR: 1.5
Quality and Performance Mgmt: 1.6
Medication Management: 2.7

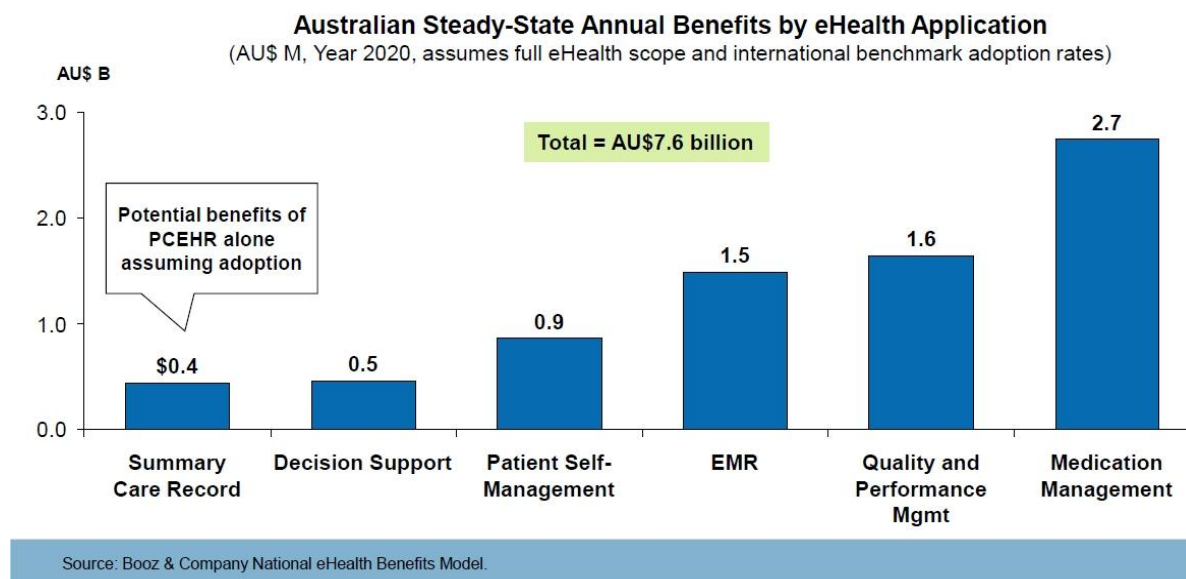Source: Booz & Company National eHealth Benefits Model.

Figure 1

The Summary Care Record was the least beneficial application identified by Booz and Company.

There is no evidence that ADHA is undertaking any of the other projects. Furthermore, the Booz & Company graphic implies that EMR (i.e. Electronic Medical Records, systems used at the point of care) could deliver nearly four times the benefit of a Summary Care Record.

The ADHA has never justified claims regarding how the My Health Record could contribute to any of these other initiatives. It is neither a necessary nor sufficient component for better health care in Australia.

Why the government should be pursuing an initiative that has the potential of realising only 5% of the claimed benefits of eHealth remains an unanswered question.

3.9 The Health Provider Perspective

Notwithstanding this lack of financial justification, there is a strong case that suggests the real aim of My Health Record is not better health care for patients, but a way of monitoring the decision making processes of health providers. In simple terms it is a way of matching existing MBS and PBS data with specific treatment and diagnostic decisions made by GPs and specialists. This theme is expanded in the article published by the Medical Journal of Australia Insight, "MyHR a path to nowhere". [11] (attached)

There is no clarity regarding how My Health Record will or could integrate into the wider set of Health IT systems that comprise the real, point-of-care data systems that support the delivery of health care. My Health Record just sits there on top of everything sucking in data, using up valuable patient consultation time, but delivering nothing, only empty promises.

GPs such as Dr Thinus make it clear that they are not impressed with the government's efforts to educate health providers and address their concerns "So Doctor, do you know what your duties and responsibilities are when using the My Health Record System?" [12]

Similarly, Dr Leon Piterman says "Trust is good for the body as well as the soul" [13]

3.10   Consent

The change to consent to register and acquire patent health data is a serious issue.

Moving to opt-out removes the need for explicit consent. This violates all the rules of good governance. This change has not been communicated to most Australians.

The consent issue is discussed by Dr Thinus in his blog: "Is Consent a moral dilemma or a mere medicolegal formality?" [14]

3.11   Trust and Privacy

Trust is critical to the delivery of health care. The relationship between patent and doctor relies totally on each trusting the other. Without that trust, patients may not fully share critical information with their doctor and if the doctor abuses that, trust the patient may cease to engage their services.

My Health Record intervenes in the relationship between patent and doctor. It requires health providers to share a patient's private and person health data with the government. The government treats itself as a special case, immune from the provisions of current and future legislation that prohibits data in My Health Record being shared with third parties not associated with the patient/doctor relationship without a court order. This means that the System Operator can legally access a patient's My Health Record without consent, without a court order, without being logged and without restriction. This is an unavoidable consequence of the System Owner's role in managing and maintaining the system.

The only safe and trustworthy way to avoid the possibility of this happening is for the government to be included as a third party, in which case the government should not run My Health Record.

This theme is expanded in the paper "Privacy, Trust and My Health Record", [15] (attached)

As Dr Leon Piterman says [13]

> "In Australia, it is common for patients to trust their own GP more than they trust the system. The ambivalent response to the government's attempt to enlist the nation into My Health Record is a reflection of this".

3.12   Prohibitions and Authorisations

The following is Section 71, from the current legislation. In essence it says that only data collected specifically for My Health Record is covered by the Prohibitions and Authorisations of the legislation. Most data in My Health Record is available in other systems therefore most of the data in the system is not subject to the Prohibitions and Authorisations

Division 3—Prohibitions and authorisations limited to My Health Record system

71 Prohibitions and authorisations limited to health information collected by using the My Health Record system

(1)   The prohibitions and authorisations under Divisions 1 and 2 in respect of the collection, use and disclosure of health information included in a healthcare recipient's My Health Record are limited to the collection, use or disclosure of health information obtained by using the My Health Record system.

(2)   If health information included in a healthcare recipient's My Health Record can also be obtained by means other than by using the My Health Record system, such a prohibition or

authorisation does not apply to health information lawfully obtained by those other means, even if the health information was originally obtained by using the My Health Record system.

Information stored for more than one purpose

(3)   Without limiting the circumstances in which health information included in a healthcare recipient's My Health Record and obtained by a person is taken not to be obtained by using or gaining access to the My Health Record system, it is taken not to be so obtained if:

(a)   the health information is stored in a repository operated both for the purposes of the My Health Record system and other purposes; and

(b)   the person lawfully obtained the health information directly from the repository for those other purposes.

Note: For example, information that is included in a registered healthcare recipient's My Health Record may be stored in a repository operated by a State or Territory for purposes related to the My Health Record system and other purposes. When lawfully obtained directly from the repository for those other purposes, the prohibitions and authorisations in this Part will not apply.

Information originally obtained by means of My Health Record system

(4)   Without limiting the circumstances in which health information included in a healthcare recipient's My Health Record and obtained by a person is taken not to be obtained by using or gaining access to the My Health Record system, it is taken not to be so obtained if:

(a)   the health information was originally obtained by a participant in the My Health Record system by means of the My Health Record system in accordance with this Act; and

(b)   after the health information was so obtained, it was stored in such a way that it could be obtained other than by means of the My Health Record system; and

(c)   the person subsequently obtained the health information by those other means.

Note: For example, information that is included in a registered healthcare recipient's My Health Record may be downloaded into the clinical health records of a healthcare provider and later obtained from those records.

3.13   The Opt-Out Campaign

The opt-out campaign is fundamentally flawed for a number of reasons.

1. A number of necessary changes and preconditions were recommended before a move to opt-out was implemented. These were defined in the review of the PCEHR in 2013 [7] and the Minter Ellison Privacy Impact Assessment (PIA) [17]. These have not been implemented

    In the Minter Ellison PIA it specifically referenced the PCEHR review recommendation 13

    Transition to an 'opt-out' model for all Australians on their MyHR to be effective from a target date of 1st January 2015. This recommendation is subject to the completion of the minimum composite of records (recommendation 21) and the establishment of clear standards for compliance for clinical users via the Privacy and Security Committee.

    Recommendation 21 said:

    Implement a minimum composite of records to allow transition to an opt-out model by a target date of 1st January 2015 inline with recommendation 13. This will dramatically improve the value proposition for clinicians to regularly turn to the MyHR, which must initially include:
    • Demographics
    • Current Medications and Adverse Events

**Australian
Privacy
Foundation**

- *Discharge summaries*
- *Clinical Measurements*

Recommendation 21 has not been implemented. Of the current 6 million registrations for My Health Record, only 20% contain a Shared Health Summary. This means that at least 80% of current My Health Records do not include the above data.

2. It does not inform all Australians that they have a responsibility to consider opting out of being automatically registered for a summary health record, without their express consent.

3. The government's message is simplistic and confined to the claimed benefits of the system. It does not provide a comprehensive description of the system, including costs and risks, and the patient responsibilities that are being imposed upon patients to manage their own record. People should be provided with all this information in order that they can make an informed decision.

4. It does not explain why it may be a good idea for some communities to at least consider opting out.

5. It does not explain how those people who are on the wrong side of the Digital Divide (i.e. do not have access to, or are unable to, utilise modern technology) can participate in the system.

6. The lessons from the failed UK care.data initiative have not been learned. A major reason for the failure of care.data was given by Tim Kelsey, current CEO of the ADHA: "NHS England had not thoroughly explained the benefits of the potential database."

There could be two reasons for this, 1) a failure to communicate the message or 2) the message is invalid, i.e. to patients there are few if any "benefits of the potential database". (see the UK Experience, below)

3.14   Other voices

The APF is not the only voice to speak out about the many failings of My Health Record.

Just two include those of former Digital Transformation Office chief executive Paul Shetler and the former chief technology architect of the Health and Human Services Access Card, Marie Johnson

While we do not agree with Paul Shetler that My Health Record can be fixed, we do agree with his view that

> *"The first thing I would do is acknowledge there is a problem, and that they inherited a previous health record [the PCEHR, or personally controlled electronic health record], which nobody wanted.*

> *"But rather than trying to dragoon people into it using an opt-out – which is really the heaviest form of pressure – they should put an immediate pause on the project and acknowledge that they have heard what the public are saying." [18]*

Similarly, Marie Johnson said

> *"The politically designed or influenced model of a centralised database with widespread access at the edge is deeply flawed. This was the Access Card model and it's being done again with My Health Record.*

> *Everything else that flows from that defective model is problematic and unresolvable: legislation; operational performance; privacy; security; informed consumer choice; and highly contested value proposition.*

> *Politically driven or influenced design – in any domain - usually always ends in failure or compromised outcomes. Access Card was terminated on political grounds, notwithstanding*

**Australian
Privacy
Foundation**

alternative architecture models presented and some of which have now been implemented elsewhere." [19]

Dr Robertson-Dunn, the primary author of this document was also involved in the Human Access Card project, where he provided architecture assurance and advice to the Minister and Departmental Secretary. His conclusions exactly match those of Ms Johnson and, furthermore, was at the heart of his advice to NEHTA well before the system was implemented, in his response to the PCEHR Concept of Operation.

3.15   Alternative for health providers to access patient health data

The UK has a system called the Summary Care Record (SCR) [20]. It is an electronic record of important patient information, automatically created from GP medical records. It can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care.

It is a centralised database similar to My Health Record that, at a minimum, holds important information about a patient's;

- current medication
- allergies and details of any previous bad reactions to medicines
- the name, address, date of birth and NHS number

Those who participate can choose to also include additional information in the SCR, such as details of long-term conditions, significant medical history, or specific communications needs. To do this they must visit their GP. In the NHS a patient can only have one GP. Patients can opt-out if they wish.

However, the SCR differs from My Health Record in a number of significant ways:

- It can only be accessed by health and care staff. Although patients cannot access the system, patients can ask to view or add information to their SCR by visiting their GP practice
- Data is collected automatically from GPs systems with no involvement from the patient and minimal effect on the GP's workload.
- It is owned and run by the NHS not the government.
- The NHS (unlike the ADHA) has a demonstrated and justifiable reason for collecting detailed patient health data.

3.16   Alternatives for people/patients to access their health data

Most GP health records are already digitised. The issue is not how to digitise health data but how to provide digital access to this data for those who require it.

My Health Record makes the assumption that all Australians will benefit from having access to a summary of their medical data. This is false for two reasons. The first is the assumption that all Australians will be willing and able to participate in uploading data to their My Health Record.

The second is that all Australians will derive value from My Health Record. There is no evidence that either of these assumptions is valid.

My Health Record is unique, not because it is better but because it is not justifiable for governments to spend billions on a solution that delivers little benefit at high risk, especially when alternative solutions can be provided at zero cost to the government.

There are available in Australia and other countries, other solutions that facilitate patient access to personal health data, all of which are voluntary, better, cheaper and less privacy invasive. These are summarised below.

3.16.1 Australia

MedicAlert

(See section on Emergency Use, above)

The government has a range of solutions that have been available for a number of years, but is somewhat reticent to talk about these in the same context as My Health Record. These include:

Medicare Express Plus from the Department of Human Services.

The website for this app tells us that you can "Access your Medicare information and complete a range of services using your mobile device."

These include:

> *"Medicare*
>
>> *View your Medicare card details and current card members.*
>>
>> *Update contact details.*
>>
>> *Update bank account details.*
>>
>> *Order a replacement or duplicate Medicare card.*
>
> *Medicare benefits*
>
>> *Submit claims for most services.*
>>
>> *View, download, print or email your Medicare Claims History statements for the last 3 years.*
>
> *Medicare Safety Net*
>
>> *View your Medicare Safety Net balance.*
>
> *Australian Immunisation Register*
>
>> *View, download, print or email Immunisation History Statements for:*
>>
>>> *yourself*
>>>
>>> *your child under the age of 14*
>
> *Australian Organ Donor Register*
>
>> *Register your organ donation decision.*
>>
>> *Change your organ donation decision.*
>>
>> *Request a new Australian Organ Donor Register card.*
>>
>> *View a digital copy of your Australian Organ Donor Register card.*
>
> *Office Locator*
>
>> *Locate a service centre."*

https://www.humanservices.gov.au/individuals/services/medicare/express-plus-medicare-mobile-app

The Head to Health Initiatives from the Department of Health, which ironically has this statement:

> *"Australia has great mental health services and resources, but it can be tough finding the ones that suit you best. We've made your search easier by hand-picking resources from publicly funded providers."*

https://headtohealth.gov.au/

The Medicine Wise app of the National Prescribing Service.

The National Prescribing Service (which is funded by the government) website tells us that its mission is:

> *"Making Australia more medicinewise, through digital health and data insights, health professional education and reliable health information for consumers."*

The Medicine Wise app does far more than just list your medicines; which is all My Health Record does. It will:

> *"remind you how and when to take your medicines so you can get the most out of them*
>
> *help everyone involved in your health care to know which medicines you use so medicines mistakes are prevented*
>
> *help your doctor and pharmacist to check and review your medicines so they can make the right decisions about your health*
>
> *provide vital information about your medicines in an emergency, helping to ensure your safety."*

https://www.nps.org.au/medical-info/consumer-info/keeping-a-medicines-list?c=medicinewise-smartphone-app-f58d5ec1

3.16.2   UK

GP online services

> *These are designed to support GP practices to offer and promote online services to patients. These services include:*
>
> *booking and cancelling of appointments*
>
> *ordering of repeat prescriptions*
>
> *viewing of their GP record (which includes coded information about allergies, immunisations, diagnoses, medication and test results).*

https://www.england.nhs.uk/patient-online/

Co-ordinate My Care

> *This is a London specific system which works to empower patients to have choices about the care they receive and to make those choices known to those who care for them. They look to continually link up the organisations and individuals that provide care for a patient, such as doctors, nurses, social care providers and emergency services including the London Ambulance Service, NHS 111 and the out of hours GP service.*
>
> *GPs work together with their patients to create a personalised urgent care plan that is prepared and recorded on CMC to ensure all care providers can access this information all day, every day.*
>
> *They are developing partnerships across all of the NHS and the private sectors.*

http://coordinatemycare.co.uk/

Area of coverage

http://coordinatemycare.co.uk/cmc/wp-content/uploads/2014/06/map_london_boroughs_feb17.pdf

Patient Knows Best (patient portals in use in Wales, Surrey and Sussex)

Wales

https://www.digitalhealth.net/2018/08/welsh-patients-know-best-after-being-given-access-to-their-records/

> *Certain patients in Wales have been given access to their own health records, allowing them to collaborate more closely with clinicians on care needs.*

> *Abertawe Bro Morgannwg University Health Board is the first board in Wales to offer access to the Patients Know Best (PKB) portal, which gives patients instant access to their medical records.*

> *It also gives them the ability to choose with whom they want to share their medical information, and to create a digital care plan.*

> *As well has being shared with doctors, this care plan can also be seen by relatives and carers.*

Surrey and Sussex

> *Surrey and Sussex Healthcare NHS Trust is to offer patient-controlled electronic records to more than 3,200 people with inflammatory bowel disease.*

> *The solution is integrated with the hospital's Cerner Millennium electronic patient record, allowing the patient record to augment the hospital record.*

https://www.digitalhealth.net/2016/03/surrey-and-sussex-trust-to-use-pkb-with-3200-ibd-patients/

3.16.3 NZ

Online health portals prove popular in New Zealand

> *"Nearly a quarter of a million New Zealanders are now using a patient portal to access their health information, the Government has revealed.*

> *Patient portals enable patients to manage aspects of their own healthcare such as booking appointments, requesting repeat prescriptions and messaging clinical staff directly"*

https://netguide.co.nz/story/online-health-portals-prove-popular-new-zealand/

3.16.4 USA – client portals

Individuals' use of online medical records is on the rise

> *"It's taken years, but healthcare consumers are now becoming comfortable with the notion of accessing their medical records online. In fact, the use of portals and other mechanisms to access medical records is rising, according to the Office of the National Coordinator for Health Information Technology."*

https://www.healthdatamanagement.com/list/individuals-use-of-online-medical-records-is-on-the-rise

3.16.5 Sweden

> *National e-health services in Sweden provide citizens with health information, contact details of providers, and interactive services where they can ask questions anonymously that are answered by healthcare professionals within seven days. The national portal My Healthcare Contacts lets citizens request, cancel, or reschedule healthcare appointments, renew prescriptions, and request contact with a specific clinician or hospital. Each healthcare centre or other local provider decides which e-services people can use to interact with them. People log in to the portal using either an electronic ID or their Swedish personal identity number. Recent figures show that over 2 million people have set up accounts in My Healthcare Contacts (about a fifth of the Swedish population). During*

November 2014 over 135 000 contacts with healthcare were made through the portal nationally.

Sweden is currently planning to make full electronic medical records available to all citizens who want them. A pilot study in Uppsala County in 2002 ran into legal problems as citizens in Sweden did not have the right to have direct online access to their medical record.2 However, ensuing discussions resulted in the introduction of the Patient Data Act in 2008, which solved this problem. Through the Sustains project (www.sustainsproject.eu/), all citizens in Uppsala were given access to their records through the secure My Healthcare Contacts platform in 2012.2

Other national e-health initiatives under way include the My Care Pathways project. This will allow patients to follow, own, and manage their care processes online. Three groups of patients with specific conditions were involved in the initial design of the service. The project also aims to adapt and further develop the Swedish National e-service and provide a platform for developing new e-services (http://healthinnovationplatform.se/en/), such as allowing patients to track the status of referrals and other planned interactions with healthcare services.

https://www.bmj.com/content/350/bmj.h359

https://www.futurehealthindex.com/2017/10/30/access-electronic-health-records/

3.17   The Legislation To "Strengthen" Privacy

There are several issues we have with the legislation

- The claim that there is no additional cost. This is only true if the real problem of deleting inactive records is not properly addressed. (see the attached article The My Health Record Delete Problem for a more comprehensive treatment of the issue)
- The presumption that people will not want to delete individual documents from the health record
- The reality that the government can change the legislation at any time in the future.
- The reality that My Health Data will flow into other systems that have nothing like the safeguards built into My Health Records and where the prohibitions and authorisations of do not apply, as per Section 71 of the legislation. (See above "Prohibitions and Authorisations")
- The government treats itself as a special case, for which they have provided no justification. The government needs to treat itself as a third party in the patient/health provider relationship.

Australian
Privacy
Foundation

4 The UK Experience

care.data

The UK National Health Service attempted to introduce a health data acquisition scheme that automatically collected patient data and stored it in a centralised government database. This was known as care.data. Media reports said:

> *"The care.data programme was first approved in 2012 as an ambitious project to expand the Hospital Episode Statistics and to link them to other data sets, starting with GP data, and to make this available to researchers and others.*
>
> *It quickly came under heavy criticism for confusion over what the data would be used for and how patients could opt out, including suggestions that the psuedonymised data could be sold to insurers and marketing companies.*
>
> *These concerns were further exacerbated when NHS England attempted to run a public information campaign in January 2014. The campaign was criticised by clinicians for sending out a 'junk mail' leaflet that failed to mention the project by name, or include an opt-out form."*

https://www.digitalhealth.net/2016/07/care-data-dumped-after-caldicott-review/

The initiative was halted and Dame Fiona Caldicott conducted a review which published a report: "Information: To share or not to share? The Information Governance Review"

Following the review, the care.data initiative was abandoned.

In the UK government's response it published what it called "The Revised Caldicott Principles"

1. Justify the purpose(s)

   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

   Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

   Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Australian
Privacy
Foundation**

6. Comply with the law

> *Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.*

7. The duty to share information can be as important as the duty to protect patient confidentiality

> *Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.*

NHS Digital Systems and Services

In the UK, the NHS delivers a wide range of digital systems and services to support health care.

Their website says:

> *"We deliver systems and services to the NHS and the wider health and social care sector which help providers deliver better care. Our information, data, and IT systems help health professionals, commissioners, analysts and managers give the best outcomes for patients."*

Their website lists well over 100 systems and services (including the Summary Care Record [20]) and covers a variety of applications and outcomes.

Contrast the NHS with the Australian Digital Health Authority which is fixated on My Health Record. Digital Health is more than document management of historical data.

References:

The Information Governance Review (Caldicott Report)
https://www.gov.uk/government/publications/the-information-governance-review

UK government's response to the Caldicott Report)
https://www.gov.uk/government/publications/caldicott-information-governance-review-department-of-health-response

Thanks to Care.data, your secrets are no longer safe with your GP
https://www.wired.co.uk/article/care-data-nhs-healthcare

A simple guide to Care.data
https://www.wired.co.uk/article/a-simple-guide-to-care-data

care.data:-a-media.disaster
https://web.archive.org/web/20140315001251/http://www.ehi.co.uk/insight/analysis/1253/care.data:-a-media.disaster

Care.data campaign leaflet slammed
http://ehi.co.uk:80/news/ehi/9131/care.data-campaign-leaflet-slammed

Cameron adviser leaves controversial NHS data scheme for private sector
https://www.theguardian.com/society/2015/sep/17/cameron-adviser-leaves-controversial-nhs-data-scheme-private-sector

NHS Digital Systems and Services
https://digital.nhs.uk/services

**Australian
Privacy
Foundation**

References

[#1] Health Care Homes
http://www.health.gov.au/internet/main/publishing.nsf/Content/health-care-homes

[#2] The Federal Government's Health Care Homes is forcing patients to have a My Health Record
https://www.healthcareit.com.au/article/chronic-care-patients-forced-have-my-health-records-access-governments-health-care-homes

[#3] The Heroism of Incremental Care, Atul Gawande, New Yorker, January 23, 2017
http://www.newyorker.com/magazine/2017/01/23/the-heroism-of-incremental-care

[#4] For-You and Your Family. What's in My Health Record?
https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record

[#5] For-You and Your Family, How Tos, FAQs
https://www.myhealthrecord.gov.au/for-you-your-family/howtos/frequently-asked-questions

[#6] My Health Record Statistics
https://www.myhealthrecord.gov.au/about/my-health-record-statistics

[#7] Benefits of My Health Record for healthcare professionals
https://www.myhealthrecord.gov.au/for-healthcare-professionals/what-is-my-health-record/benefits-my-health-record-for-healthcare

 [#8] PCEHR Review 2013
http://content.webarchive.nla.gov.au/gov/wayback/20150322014955/http://www.doctorconnect.gov.au/internet/main/publishing.nsf/Content/46FEA5D1ED0660F2CA257CE40017FF7B/$File/FINAL-Review-of-PCEHR-December-2013.pdf

[#9] MedicAlert
https://www.medicalert.org.au/

[#10] Using 21st Century Tools to overcome the 'fear of frying' and build success. Presentation by Professor Mukesh Haikerwal (World Medical Association and NEHTA) and Chris Bartlett (Booz & Company) at Healthcare Information Management Systems Society conference, 2013
https://vdocuments.mx/healthcare/overcoming-fear-of-health-technology-programs.html

[#11] MyHR a Path to Nowhere, Dr Bernard Robertson-Dunn, MJAInsight
https://www.doctorportal.com.au/mjainsight/2018/25/my-health-record-on-a-path-to-nowhere/

[#12] So Doctor, do you know what your duties and responsibilities are when using the My Health Record System? Dr Thinus' musings

Australian
Privacy
Foundation

https://tvren.wordpress.com/2018/08/31/so-doctor-do-you-know-what-your-duties-and-responsibilities-are-when-using-the-my-health-record-system/

[#13] Trust is good for the body as well as the soul, Dr Leon Piterman, The Medical Republic
http://medicalrepublic.com.au/trust-good-body-well-soul/16625]

[#14] Is Consent a moral dilemma or a mere medicolegal formality? Dr Thinus' musings
https://tvren.wordpress.com/2018/08/20/is-consent-a-moral-dilemma-or-a-mere-medicolegal-formality/

[#15] Privacy, Trust and My Health Record, Journal of the International Association of Privacy Professionals ANZ (iappANZ) Edition no. 85, August 2018
Available here:
https://privacy.org.au/privacy-trust-and-my-health-record/

[#16] The biggest privacy risks to your My Health Record – the Government
https://privacy.org.au/2018/07/24/media-release-the-biggest-privacy-risks-to-your-my-health-record-the-government/

[#17] Minter Ellison PIA
https://www.myhealthrecord.gov.au/sites/g/files/net4206/f/pcehr_opt_out_pia_-_2015.pdf?v=1520887003

[#18] How to fix the MHR, Paul Shetler, InnovationAus
https://www.innovationaus.com/2018/07/Shetler-How-to-fix-the-MHR

[#19] Why My Health Record is flawed, Marie Johnson, CIO
https://www.cio.com.au/article/645498/why-my-health-record-flawed/

[#20] UK Summary Care Record
https://digital.nhs.uk/services/summary-care-records-scr

Australian Privacy Foundation

Australian Privacy Foundation
https://privacy.org.au/

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 and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

**Australian
Privacy
Foundation**

5 Attachments

Reference [9]

My Health Record: on a path to nowhere?

Medical Journal of Australia: Insight. July 2018

My Health Record is on a path to nowhere, writes Bernard Robertson-Dunn …

The impending move to opt out of the My Health Record will potentially have a very significant impact on GPs and their work practices. It is suggested that GPs need to make informed decisions regarding their use of the system and the advice they give to patients.

The following is a summary of the My Health Record, its context within the government's broader agenda for acquisition of health and other datasets as well as the way the government is attempting to persuade GPs to participate in its use.

What is My Health Record?

According to the government's website myhealthrecord.gov.au, "My Health Record is a secure online summary of your health information".

This gives the impression that when a patient signs up for a My Health Record, or is registered for one under the opt-out scheme, they will get a summary of their health information. They won't.

The opt-out scheme will only register a patient for a My Health Record. If a patient wants their My Health Record to contain a Shared Health Summary (SHS), they must appoint a nominated service representative (often their GP) and work with them to populate, manage and regularly update the information. It won't happen automatically, and it isn't just a simple matter of clicking on a button and uploading data. This is what the government's website says:

> "The first time you log into your My Health Record there may be little or no information in it. Information will be added after visiting a healthcare provider such as a GP, pharmacist or hospital. You can begin to add your personal health information and notes straight away."

Most of the data in My Health Record are not health information; they are data relating to a patient's medical treatment. The system is not designed to store health data such as weight, height, blood type, alcohol use, smoking and exercise patterns.

My Health Record is a simple document database. It is based primarily on pdf files, which are simply aggregated without being integrated or managed from a clinical perspective. It is owned and controlled by the federal government and attached to clinical, hospital, pharmacy, imaging and pathology systems, which can upload medical data to it and download medical data from it.

Ironically, for a supposedly personal health record, a patient cannot print a copy of their health information.

My Health Record is an additional record system, on top of, and in addition to, GPs' existing systems. It requires extra effort to manage, yet it offers no benefit to the GP because most if not all the data

are already in the GP's existing clinical system. The pdf format of the data files makes it difficult and time consuming to access, and the lack of context makes their use in research or analytics problematic.

Uploading an SHS is not simply a matter of clicking a button. The patient's GP takes on an unknown responsibility and/or liability, in the sense that this has not yet been defined in legislation or tested in court. The AMA's "Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System" makes it clear that uploading a SHS is not trivial exercise.

My Health Record may also include discharge summaries. A recent *MJA InSight* article was critical in its analysis of these. Under the title of "GPs want clinical handovers, not discharge summaries" the authors said:

> "In the real world, GPs are grappling with being thrown links to hospital electronic records through systems such as 'The Viewer'. Investigations are likely to be uploaded (after a delay) to My Health Record. These are raw data, unfiltered and disorganised, and more of a throw than a handover. Being thrown raw data and being expected to catch them in this way is akin to a hospital doctor being given the login to the GP clinic's patient management system and being expected to extrapolate a referral."

This probably applies equally to all the summary documents: the SHS, discharge summaries and event summaries.

> The issue of raw data in My Health Record applies also to test results, which, without context, are useless at best and dangerous at worst.

> "Among patients with low health literacy and numerical skills, confusion about the meaning of results is common. Many tests are reported in the same form that the doctor sees them, which even savvy patients may find 'literally meaningless' ... In some situations we run the risk of patients misinterpreting that there is no problem when there is one, or assuming there's a problem when there isn't."

In addition to summary documents and test results, there are data that are derived from government systems.

My Health Record is not designed to replace existing clinical systems. This is appropriate because the federal government is not directly involved in, or responsible for, the delivery of health care services. My Health Record is an additional source of summary health care data, where the data are derived from existing health care systems. In other words, most, if not all, the data in a patient's My Health Record are already in their GP's clinical system.

By far the largest number of documents come from the Medicare system, comprising only billing data, with minimal clinical information, and Pharmaceutical Benefits Scheme prescription data (677 177 059 combined) compared with clinical documents (5 477 845), as reported on 29 April 2018.

**Australian
Privacy
Foundation**

My Health Record in context

Announcements from the Australian Digital Health Agency website seem to suggest that the government will be extending My Health Record in order to relate the Medicare Benefits Schedule and Pharmaceutical Benefits Scheme data to health care activities. Without the detailed data held in GP and hospital systems, it is difficult to see how this could be useful to either clinicians or medical researchers.

It might help GPs to know that My Health Record is not the only initiative that the government is pursuing with regard to health data and what the government is, or could be, using these data for. These include:

- An Australian Bureau of Statistics project, the Multi Agency Data Integration Project (MADIP) which is designed to link data from the Department of Social Services, the Department of Health, the Department of Human Services, the Australian Taxation Office and the Australian Bureau of Statistics. The purpose of the MADIP is to "create an enduring, linked, publicly accessible research dataset, which is on hand to help government agencies and researchers respond to nationally important policy and service delivery questions".

- The Practice Incentives Program – "activities include continual improvements, quality care, enhanced capacity, and improved access and health outcomes for patients".

- A new division of the Department of Health, Provider Benefits Integrity Division, that "is responsible for identifying, investigating and treating incorrect claiming, inappropriate practices and fraud. The Department is consulting stakeholders with the intention of changing a number of acts. The proposed changes would amend the *Health Insurance Act 1973*, the *Health Insurance Act 1973*, and the *Dental Benefits Act 2008* to allow the Department to directly collect information from employing organisations, corporations and hospital authorities such as practice records".

Persuasion

The government is planning to actively promote the use of My Health Record among GPs through a variety of techniques and technologies. Some information about its intention is available through a Request for Expression of Interest (REI) for what the government calls "test beds".

The repeated objective of the test beds project is to identify benefits of My Health Record. Not costs, not risks, not to evaluate My Health Record, just to identify benefits.

As it says on slide 16 (at 21 minutes 30 seconds) of a presentation available on YouTube:

> "*Their purpose is to promote innovation to address Australia's highest priority health challenges, generating evidence of how the new approaches* improve health outcomes."

The tender documentation says:

> "*This REI process is intended to enable the Agency to establish test bed projects that will produce evidence of the positive impact of new digitally enabled services and models of care, and demonstrate that they are sustainable and scalable.*"

and:

> "*The first tranche of test beds should include use of the My Health Record system and how it can be utilised to create new, digitally enabled services and models of care, particularly where these can be rapidly implemented or are already underway.*"

In an addendum to the Test Bed REI, the Australian Digital Health Agency provided some information about its activities. These are the six evaluation projects mentioned in the YouTube presentation:

- evaluating how GPs in primary care use My Health Record to improve their patients' health through improved medicines management, sharing information, and reducing unnecessary duplication of diagnostic services, with the National Prescribing Service (NPS) MedicineWise and the University of Melbourne;

- evaluating how GPs and hospitals use My Health Record to improve their patients' health through improved medicines management, reducing unnecessary duplication of diagnostic services, and reducing hospital admissions and length of stay. This is with PenCS, Western Sydney Primary Health Network, the University of Western Sydney, and NSW Health;

- educating GPs about how to use My Health Record to improve their management of patients' medicines (specifically deprescribing inappropriate medicines) and reduce unnecessary duplication of diagnostic services. This project is a specific multifaceted education intervention with MedCast and the University of Wollongong;

- quarterly tracking of health care providers to investigate awareness, readiness, attitudes, and experience regarding the My Health Record system through to early 2019. This is with McNair YellowSquares and Rodika Research Services;

- changing clinical behaviour in primary care using My Health Record to improve uploading and viewing of documents, sharing of useful and accurate information, and informed clinical decision making. This project involves the discipline of behavioural economics and is with the Behavioural Insights Team Australia; and

- evaluating the performance of the My Health Record system by conducting data analytics on de-identified, administrative, non-clinical My Health Record data to investigate the impact on medicine management, ordering diagnostic services, adherence to evidence-based care, patterns of health care use, and associated costs.

Australian Privacy Foundation

Conclusion

The Australian Digital Health Agency (the operators and custodians of My Health Record) and the government have failed to understand that health care professionals need better access to current, accurate, well formatted and managed high quality patient data. Only a few patients want access to their medical data. This could be achieved at minimal to zero cost to government through improved interoperability and patient portal access to GP systems – as is available in Sweden. GPs could benefit from tools that assist them to understand the data and to make better decisions.

Current, accurate point of care data are much more important than historical data. The current focus on health and medical records is in danger of turning GPs into data entry clerks and can lead to burnout. An ineffective, pseudo health summary record system doesn't meet the needs of health professionals or of patients. All it does is increase costs, reduce medical effectiveness, and put patient privacy at risk.

Better sharing of patient data among health professionals has significant potential medical benefits. Giving them to the government doesn't, especially if the intent is to monitor and question the activities and decisions of health professionals. An unintended consequence could be that health professionals are further distracted from health care by having to justify their activities and decisions.

Quo vadis My Health Record?

My Health Record replaces nothing; it does nothing for GPs apart from increasing their workload; it does nothing for a patient that a GP can't do at minimal cost as and when required; it is on a path to nowhere; it is a major privacy risk and will potentially lead to further bureaucratic inefficiencies.

It may also provide insights into GP work practices and clinical methodologies.

The government has made plans to persuade GPs to participate in My Health Record using a variety of mechanisms, mostly so far unannounced. It would be wise for GPs to be fully aware of the nature of My Health Record, the full range of uses the government could make of data in the system over and above any benefits that might accrue to patients, and the techniques the government is contemplating bringing to bear on GPs and potentially other health providers.

The future of My Health Record is in the hands of GPs.

**Australian
Privacy
Foundation**

Reference [13]

Privacy, Trust and My Health Record.

First published in Privacy Unbound, the Journal of the International Association of Privacy Professionals ANZ (iappANZ) Edition no. 85, August 2018

https://gallery.mailchimp.com/3e9414f2c1f6070d011172186/files/e2da0c5e-36f4-437e-aa64-1cc055ab6b95/iappANZ_Privacy_Unbound_Edition_85.02.pdf

1   Introduction

Dr Bernard Robertson-Dunn is an electronic and automation engineer, has a PhD in modelling the electrical activity in the human small intestine and has had over forty years modelling, architecting and designing large scale information systems, mostly in government environments.

These include the Departments of Health, Finance, Immigration, Defence Bernard has been following the progress of, and has contributed to, the debate on the My Health Record for over ten years. He has no association or affiliation with any vendor or government organisation. Bernard is chair of the Health Committee of the Australian Privacy Foundation.

The views in this article are his considered opinion and are provided to Privacy Unbound to provide a broad contextual analysis of the issue surrounding health records and My Health Record in particular.

2   A Medical Record primer

Back in the day, when General Practitioners wrote on paper with black ink about the consultation they had just had with their patient, there was an implied joint contract and mutual trust. The doctor wanted to remember what their patient's symptoms were, what he (they were nearly always he in those days) had prescribed and his musings and guesses as to what you were suffering from. You didn't have to know or remember what you were suffering from. You both had in interest in the existence of the record. It was written by and for the doctor, you never saw it and it was called a medical record.

There was a reasonable balance between two parties with different but compatible and complementary objectives. You trusted your GP to keep your data confidential and do their best to make and keep you well; the GP wanted to stay in business and he valued his reputation.

3   Automation

Then along came computers. Initially all they did was store the same information in the same manner as did the paper records. There was the odd downside; computers are more expensive than pen and paper; GPs had to learn how to use a keyboard and how to operate a computer. The relationship between patient and GP didn't change much. The GP probably spent more time looking at a computer screen than they did when they used pen and paper, but that was seen as a small price to pay for improved record keeping.

It was a similar situation in those hospitals that implemented electronic health records, although there are some horrendous tales of failed IT projects, but that's not particularly uncommon in such complex environments.

With early computerisation, the situation regarding privacy, confidentiality and trust between patient and health care provider was largely unchanged. The IT systems were more prone to single points of failure, to ransom-ware and to data breaches but they were issues that could be solved with proper management and attention to technology.

There were, and still are, some major problems with the access to, and management of, health care information. Much data is transferred via fax, only a small amount of information is interchanged,

**Australian
Privacy
Foundation**

sometimes data exists but this is unknown to health providers who could benefit from having it available.

However, the old medical record systems did have one advantage. Only those involved in a particular aspect of a patient's care had access to a patient's data about that care. Poor sharing of data was a two edged sword. It was privacy enhancing but there were clinical downsides.

When it comes to addressing some of the problems facing data management in the health care system – better access to health information dispersed throughout a large, multifaceted industry - there are two potential approaches. These can be summarised as decentralised or centralised.

4   Distributed Health Eco-systems

A decentralised, or distributed system would create a mechanism for identifying the location of a patient's health data and allowing a health provider to access that data. There would need to be a mechanism for implementing a need to know principle – i.e. a health provider could only see that data they needed to in order to treat or advise their patient. The holder of that information would be responsible for granting access to the data.

All data could remain where is was; thus not complicating data consistency, which would occur if data were copied from one system to another. However, there may be a good argument that there should be a single source of truth, which would logically be the patient's primary health provider – their GP.

A distributed system has the added advantage or being far more resilient and thus reliable than a centralised one which is at risk of being overloaded in times of high usage e.g. in an epidemic or bio-hazard situation, or prone to failure dues to power or communication loss. It is far less risky to have clinical systems located as close as practical to the point of care.

A distributed system has the characteristics of a virtual health ecosystem, rather than a health record. Additional capabilities at the health provider level can include such integrated functions as appointments, repeat prescription requests and a patient portal access to relevant information. Such systems are being implemented overseas.

The result would be an eco system of health information in which a virtual medical record existed. This record, although distributed, could be made available to systems that could undertake complex analysis and predictive functions that would assist health providers in their diagnosis and treatment of the patients. The major characteristics would be flexibility, coexistence of a variety of capabilities and a platform for small scale innovation that would scale or find a niche if useful or atrophy if not.

The privacy, trust and confidentiality issues would not be unduly challenged; the symmetry of need between patient and health provider would be retained. The health provider would be responsible for maintaining patient privacy and the patient would only need to trust a single party.

5   Centralised Health Records

The alternative is a centralised system such as My Health Record. This requires a database at the hub and a system which acquires and stores data. If it only passed on the data and did not retain it, it would functionally be the same as a distributed system.

A centralised system results in the database becoming the defining feature of the health information ecosystem. Innovation is stifled because compatibility with the database is essential. In a distributed system, local innovation is possible and preferable – it can be tested and assessed locally. Change in a centralised system is totally dependent on the hub and would need to happen globally.

The primary issue of a centralised system is "who owns the database in the hub?" Ownership bestows significant privileges; the owner runs the system and any access rules do not apply to the owner.

Australian Privacy Foundation

This single characteristic completely changes the dynamics of the health data environment.

Now there are three parties –the patient, the health provider and the system owner. In the case of My Health Record, this is the Australian Digital Health Agency, an Australian government entity that both reports to, and is funded by, the Federal Minister for Health.

What was a symmetry of needs between the patient and their health provider is fundamentally altered. Not just changed but distorted.

If the health provider is a GP, then a number of changes are introduced into the interaction between the GP and their patient. My Health Record is an additional, summary system over and above the GP's clinical support system. Uploading data into My Health Record is not a simple matter of a few clicks. The AMA has produced a set of guidelines [1] that GPs are supposed to follow. It is a 27 page document and following it takes time out of a consultation to manage a patient's My Health Record.

In addition, and this is a significant issue, the government, through a variety of mechanisms, pays the GP to provide the patient's data. It could be argued that this is "selling" patient data to the government. This may or may not be a valid description, but it does introduce a real or perceived conflict of interest. The patient suffers from less attention; the GPs is paid for something that does not involve treating the patient. The patient may not be happy with the financial arrangement and may perceive a conflict of interest. This issue has the potential to have a negative impact on the trust between the patient and their GP.

The relationship between the GP and the government is primarily financial. The GP gains little or no benefit, they already have the data. The GP still gets data from other providers via the traditional mechanisms - fax, or emails. Data that is not provided to GPs may or may not be uploaded to My Health Record. Patients have the option of requesting that pathology labs or specialists do not upload data. There is no guarantee that data that a new GP or an A&E department would like to see is in My Health Record. In short, it is unreliable. There are also reports that data is sometimes incorrect or uploaded to the wrong patient resulting in either compromised treatment or the need for a patient to spend significant time and effort correcting the error, if they discover it.

The relationship between the patient and the Federal government, a funding agent, is totally un-necessary for the delivery of health care. However, it represents a real and potential problem for the patient. Why does the Federal Government want such detailed health data? This is a question that has never been answered satisfactorily. There is an argument that the government needs aggregated data in order to develop policy, but there is no rationale for more detailed data. Furthermore, there is a suggestion that it could match detailed health data to its existing payment data looking for patterns of health care decisions by health providers; but this is only supposition. However, this uncertainty does nothing to engender trust.

The existence of a centralised database means that data from different providers will be stored in a single location; data which is available to anyone authorised to see the record. The inherent privacy advantages of a distributed system, where only the originating health provider has access, are nullified. In order to retain the trust levels inherent in a distributed system there needs to be an access control mechanism that, at a minimum, mimics that of the old system. My Health Record does not provide this. My Health Record has a complicated, poorly implemented set of access controls that require the patient to take responsibility for monitoring and managing access controls. In a similar way that automation has failed to help GPs manage input and usage of data in their clinical system, My Health Record has introduced extra responsibilities into the management of a patient's health data. This is a responsibility that most patients are unaware of, and are potentially unable to take on. If they don't, their privacy is at risk from third parties.

**Australian
Privacy
Foundation**

6 Privacy and My Health Record

The symmetry of the original relationship between patient and GP has now been destroyed. To some, there is now the feeling that there is a spy in the consulting room – the government. In addition, the effort required by the patient to manage their own data has been increased. Hardly an improvement.

The government introduced legislation in 2016 that set the scene to make the system opt-out. Australians now have a three month window in which to tell the government they do not want to be automatically registered for a My Health Record.

In order to enable an opt-out approach the government has had to remove the need to obtain explicit consent to register people and to acquire and disseminate their health data.

Because of the change to My Health Record from opt-in to opt-out, the legislation, especially that in Section 70 has recently become a major issue.

Section 70 includes a wide range of circumstances where it can release or make available My Health Record data. These include providing data to courts, tribunals, coroners and to other government agencies "in the protection of the public revenue". This last item has never been defined by the government but appears to be related to investigation of fraud and applies to any government, state or federal, that is able to impose fines.

The courts have long been able to subpoena health data from a health provider but, according to a report from the Parliamentary Library [2], the ease with which documents can now be obtained has been significantly increased. This report contradicts the Health Minister's claims that a warrant is necessary to obtain information under Section 70. The library also makes the observation that the legislation is a major weakening of existing protections around health records. The Minister has also been contradicted by the Queensland Police union [3]. That the Minister for Health, himself a lawyer is seen to be (allegedly) misrepresenting the legal standing of My Health Record is not adding to the trust Australians might have had in the system.

The minister did not add to a feeling of trust or enhance his credibility when the Parliamentary Library withdrew the original document and replaced it with another, revised version.

Even the Human Rights Commissioner has concerns about confidence in the privacy and security of the system and wants the government to improve privacy protections. "I think we can do better. We definitely are saying that there are problems with My Health Record." He told the ABC [4]

7 Conclusions

Unfortunately, there are significant consequences from having the government both own the system and set the laws and regulations that govern it. The big problem is that a government in the future could change the rules that permit easier access to My Health Record data.[5] What these are is a matter of guesswork and supposition, but is likely to be unsettling to a population that has already rejected several Identity Card/Number initiatives.

Privacy seems to matter to many Australians and they are not routinely likely to trust government initiatives, especially after problems with the recent census and the so called Robodebt debacle the result of the ATO and Centrelink sharing and linking data, something the government has expressed a desire to do with data from other agencies, including Health, more often. We do not know if that will include My Health Record data, but it could, in the future.

How the My Health Record initiative will all turn out is a matter of conjecture. What is certain is that My Health Record, if widely adopted by patients and health providers will have major consequences for the dynamics of health care system in Australia. Patients will need to become more involved in the management of their own summary health data; GPs will need to spend more time managing health record systems – their own and the governments; and the government will need to continue funding, maintaining and operating the system as well as protecting the data for

**Australian
Privacy
Foundation**

the foreseeable future. The cost of this system is currently over $AUD2billion; what the return on this investment will be is not yet known.

Even if the issue of government ownership is resolved, there are other characteristics of a centralised system that make its use and effectiveness problematic and questionable. In summary these include:

- The security of a system that is attached to the internet;
- The system is designed to promote data being downloaded to other systems with fewer controls and less visibility;
- The responsibility for accuracy, currency and completeness lies with the patient;
- The significant cost and effort required by patients and GPs to maintain the system.

These are significant obstacles to making any centralised system acceptable for clinical use.

From a privacy and trust perspective, the distributed approach has much to recommend it. The simple yet important relationship between a GP and their patient is a significant driver in the maintenance of a high degree of privacy. Both have a lot to lose. The introduction of a third party, the federal government, apart from distorting the privacy trust relationship is also an asymmetry of power. Taking on the government is no trivial task and only one has a lot to lose.

My Health Record, even after six years operation is still very much a work in progress. The government is currently going through a market testing process that is looking at completely revamping system. This is an implicit acknowledgement that the system as it exists is not fit for purpose.

It is possible, even likely, that over the opt-out period public reaction will result in the government changing its mind regarding such things as the legislation that protects the privacy of My Health Record users. Unfortunately there are two characteristics that cannot be changed.

1. My Health Record means the government acquires and keeps highly personal health data. It can also potentially track the behaviour and performance of health providers.

2. The government has already changed the legislation from opt-in and a need to get a patient's consent to opt-out and no need to get consent. At the end of the second week of the opt-out period, the government has been forced by statements made by the AMA and the Queensland Police to change the legislation to "remove ambiguity" and improve the protection of Australian's privacy.

What has the potential to totally destroy any trust people may have in the government is the reality that in our political system there is nothing is to stop this or future governments from further changing the privacy protection.

Not only is My Health Record a work in progress, so is the government's attempt to persuade Australians to adopt this scheme. Unfortunately for the government the twin problems of a lack of a guarantee regarding future governments and the reality that there is a better, cheaper, more flexible system with inherently better privacy protection means they have a difficult job ahead.

References

[1] AMA Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System
https://ama.com.au/sites/default/files/documents/AMA_Guide_to_using_the_PCEHR_Final_June_2012_Formatted_300812.pdf

[2] Law enforcement access to My Health Record data
Both the original and revised versions and a comparison are available through this site:
https://privacy.org.au/campaigns/myhr/

[3] My Health Record: Greg Hunt's warrant claims contradicted by police union
https://www.theguardian.com/australia-news/2018/jul/26/my-health-record-greg-hunts-warrant-claims-contradicted-by-police-union

[4] My Health Record needs privacy improvements to restore public confidence: Human Rights Commissioner
http://www.abc.net.au/news/2018-07-24/my-health-record-human-rights-commissioner-wants-changes/10028618

[5] My Health Record: it's worse than you think
https://libertyworks.org.au/my-health-record-its-worse-than-you-think/

The My Health Record Delete Problem, or
How to cripple a large scale Government Information System with one simple decision.

Simple solutions to complex problems always create further problems. My Health Record is an example of this phenomenon. Digital Health is far more than simply automating old manual processes that document medical treatment prescribed by doctors.

The Health Minister's decision to completely delete a person's cancelled record is a simplistic solution to what seems to be a simple problem. What the Health Minister does not understand are the complex consequences of his decision to overturn one of the most fundamental requirements in the initial design stage of My Health Record. These early decisions are the most important in the design cycle and the hardest to modify once development and implementation proceed. An analogy is the position of a building on a block of land. It is much easier to move a building 10 cm before any construction has commenced than after it has been built and occupied.

Background

First some background on deleting data from a system as technically complex as My Health Record.

Most systems have functions to create, read, update and delete data, or CRUD. In the case of My Health Record it was decided early on that no data would ever be deleted. This decision was documented in the Concept of Operations, a document that the ADHA no longer makes available, but which is still obtainable from here [1]. It is worth noting that it has never been updated, although it does say "The Concept of Operations will be periodically updated as the development of the PCEHR System progresses".

The Concept of Operations specified that:

> *"The PCEHR System will always ensure that individuals and healthcare providers are presented with the most recent version of a clinical document. If a prior version is available, individuals and healthcare providers will be given the option to access prior versions of clinical documents if they require."*

There is no evidence that this function has been implemented, there is no indication in the My Health Record itself of this capability and this function is not referred to in any of the material on the government's website.

The decision not to delete any data has an enormous significance on the subsequent design and implementation of the system. It removes the need to develop approximately half of the normal functionality. There is no need to update the data; old documents can be replaced by new documents and the old ones kept, but hidden from normal viewers. Likewise, there is no need to delete data, just flag it as hidden.

Even if a document has been uploaded to a patent's MyHR in error, it cannot be deleted, it is "effectively removed" as the Concept of Operations quaintly describes it.

Back-up and Restore

Apart from simplifying the functionality of the system, the no delete decision also makes back-up and restore much easier.

There are two types of back-up and restore.

The first is to protect against catastrophic failure of the system. This is a Disaster Recovery function and involves taking a regular snapshot of the whole system along with partial back-ups in-between major backups. This is so that, in the event of a failure of the system for whatever reason, the system could be re-built either in the same premises or in alternative premises and the system restored to its state before the event.

**Australian
Privacy
Foundation**

The second is to allow deleted information to be recovered after the deletion. In Microsoft Windows this is like using the Recycle bin. If you don't want to keep a deleted copy, you can delete the document immediately.

New Problems

By making the decision to delete records of people who wish to cancel their registration, the Minister has created multiple problems.

To immediately delete a complete record from an operational system is actually very unsafe. If the System Operator accidentally deletes a record (for whatever reason) then they can't get it back. If they do a recycle bin delete, they are not complying with the legislation. The normal process is to flag the record as deleted and/or keep a log of the deleted data, once again not complying with the legislation.

It is very unusual for a Disaster Recovery backup to be modified. Its value lies in the integrity of its data. In a system as complex as My Health Record, an individual's health record will be spread out over multiple database tables, so it is not just a case of deleting a line in a file or a row in a spreadsheet.

Deleting data safely from a Disaster Recovery backup would probably require downloading the back-up to another version of the operational system, restoring the data, and deleting the data using system functionality that ensures the data retains its integrity. Apart from the fact that currently there is no system delete functionality, interfering with the Disaster Recovery back-up is highly risky. However, the Minister has promised that a health record would not be retained by the government. What the Minister has announced will happen; it will be costly and cumbersome – if done properly.

It should be noted that the proposed legislation only applies to complete records. What about the potential need to delete documents in a current record? The big problem here is that the people have not been asked if they want it or not.

They have not been asked if they are happy to have old documents available for the System Operator to see (nobody else can see them, or maybe they can, we don't really know) or if they want old documents deleted by request.

This means that the Minster has created a big problem for ADHA with his changed requirements and created the possibility that he has created an even bigger, but uncertain problem regarding old documents.

The functionality required to delete individual documents could probably quite reasonably be incorporated as is commonly implemented - flag the document as deleted and then purge it after a given time. When creating a Disaster Recovery back-up do not include deleted documents.

These are just suggestions; it needs a complete requirements analysis and identification of the most efficient strategy - the sort of thing that should always precede any design and implementation activities.

One of the issues is making sure the requirements are complete. For instance, what are the requirements regarding records that have already been de-activated? Should they be deleted from the operational system? From old Disaster Recovery back-ups?

If old documents are to be deleted from current records how would that work?

What are the requirements for documents and/or records that have been downloaded to other systems connected to My Health Record but which people might want to have deleted?

Doing such things after six years of operations is challenging at best.

One approach is to completely redesign the system, something that ADHA seems to be considering as part of its re-platforming initiative.

Australian Privacy Foundation

One hopes that someone in government asks the question: What is the return on the $2b that has been expended on My Health Record that indicates that another $1-2b can be justified?

The statistic that ADHA has provided that only about 20% of the 5.9 million registrations have a Shared Health Summary, along with the unexpected negative reaction in many quarters to the opt-out initiative should give pause for thought. One can but hope.

Reference

[1] Concept of Operations
http://content.webarchive.nla.gov.au/gov/wayback/20140801043103/http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/CA2578620005CE1DCA2578F800194110/$File/PCEHR-Concept-of-Operations-1-0-5.pdf