



To: The Auditor General
Australian National Audit Office
19 National Circuit
Barton ACT 2600
Australia

From: Dr Bernard Robertson-Dunn
Board Member and Chair, Health Committee
Australian Privacy Foundation

19 February 2019

Subject: Performance audit of My Health Record

1 Introduction

The ANAO proposes to examine whether the:

1. Implementation of the My Health Record system promotes achievement of its purposes;
2. My Health Record system risks are appropriately assessed, managed and monitored; and
3. Monitoring and evaluation arrangements for the My Health Record system are effective.

This submission contains our analysis, observations and comments on the above scope.

We draw your attention to a request for a review submitted by Dr Bernard Robertson-Dunn to the ANAO in August 2017. This raised a number of issues regarding privacy, the way the Department of Health was representing My Health Record, an apparent lack of adherence to the proper processes as outlined in the Department of Finance's Gateway process, and the financial and clinical viability of the initiative. These issues are still unresolved and we believe are included in the ANAO's current examination. A copy is available here ¹.

Furthermore, we make reference to the Australian Privacy Foundation submission to the recent Senate inquiry and the verbal evidence provided at that inquiry. ^{2 3}

We also have a webpage that details the campaign we ran regarding My Health Record and which contains a significant number of links to media reports published during the opt-out period ⁴.

The author lives in Canberra and would be happy to attend your offices for a more detailed discussion of the issues surrounding the My Health initiative.

2 Our position

We have used the term "patient" to refer to the person registered for a My Health Record although the person may or may not be a patient in the strict sense of the word. In our opinion the more commonly used word "consumer" is not appropriate in the context of healthcare.

We have also used the term My Health Record to include its previous name the Personally Controlled eHealth Record. If the term PCEHR is included in a quote, it has not been changed.

Issue 1 Purpose

The original purpose of the My Health Record was to reduce the fragmentation of a patient's data across the healthcare system. As explained in more detail in Appendix A, it has not been implemented in such a way as to achieve this purpose.

In discussing the purpose and if the system achieves this purpose, it is important to understand a number of characteristics and features of the My Health Record and the principle document in My Health Record – the Shared Health Summary.

1. My Health Record is a secondary system, it requires time, effort and cost to manage. This is in addition to the that required by the patient's GP when using their primary clinical support systems;
2. A Shared Health Summary is manually prepared, managed and uploaded by the patient's nominated service provider (usually their GP). It involves more than a simple mouse click because the health service provider is required to ensure that it is consistent with the patient's condition and the existing contents of the patient's My Health Record. This is not a trivial task. The AMA guide to using the My Health Record system runs to 27 pages ⁵;
3. Access to the Shared Health Summary (or the Personal Health Summary or advance care planning information) cannot be controlled or limited by the patient ⁶ - in spite of the government's claim that the patient can control who sees their health data;
4. The Shared Health Summary contains very limited information. Potentially only data on allergies, immunizations, prescribed medicine and event summaries. Most of this can only come from the patient. This can be a problem, especially if they have ever changed GP - a problem that is not addressed by My Health Record;
5. Historical data such as test results and discharge summaries cannot be uploaded;
6. The needs of a patient with complex, chronic conditions would not be met with such minimal data;
7. Patients can chose to opt-out, control what is uploaded into the system or limit access to individual documents. This makes the data in the system unsuitable for clinical use. It also means the data in My Health Record is unsuitable for research purposes and
8. As explained below, most My Health Records have little or no current or relevant data. This makes it unsuitable for use in emergencies. It should also be noted that for emergency workers to access a patient's My Health Record, they need the surname, Medicare number and date of birth. It is unlikely that a patient who is taken into an Emergency Department unconscious would be able to provide such information.

A recently released research paper ⁷ that surveyed the opinions and experiences of Australian women regarding Digital Health included a section on My Health Record. The report concluded:

"Many participants demonstrated a lack of awareness of and interest in the Australian government's electronic patient record, My Health Record. Only one-third had signed up, suggesting that attempts by the government to publicise and promote the system have not been effective".

The My Health Record does not meet its intended or currently claimed purpose. My Health Record is not what the government claims it is and it is not what most people believe it is. It is not an online summary of all of a patient's health data, it is not a detailed patient health record, and it is not possible to hide all documents.

As has been identified and discussed elsewhere, ⁸ there are better, cheaper and less privacy invasive ways of achieving all the benefits that the government claims for My Health Record.

Issue 2 Risks

Privacy

The risks to the privacy of a patient are not matched by the benefits, which have never been properly enumerated by the government. Claims are made, but there is no evidence that a patient controlled summary health record can deliver those benefits.

In terms of privacy risk management, the My Health Record system has not been implemented as originally designed. The design called for identification of individual healthcare users of the system by means of two factor authentication. This was so that a patient could identify which individual had accessed their My Health Record. This functionality required implementation of the National Authentication System for Health (NASH) a component that was never implemented and there is no indication that it ever will be.

Downloads are not recorded and/or monitored such that a patient can see who and what has been downloaded. If a document is in error, no longer valid or necessary, it is virtually impossible for a patient to identify where that document has been downloaded to so that it can be corrected or deleted.

The legislation that enabled the government to change a fundamental design criterion of the system from opt-in to opt-out required a change to the National Health Act (1953) that permitted the Department of Health to store MBS and PBS data together in a single database. The Privacy Commissioner's rules that were part of the National Health Act (1953) and which had been published in 2008 prohibited storing MBS and PBS data in the same system.

The government claims to have strengthened the privacy legislation that covers My Health Record but has not informed the public that most of the data in My Health Record is not covered by this legislation. Section 71 of the My Health Record act specifically excludes data that is available in other systems – i.e. most of the content of a My Health Record.

Whatever legislative protection and restrictions the government may have put in place can be changed by another government in the future

My Health Record, a national health database, attached to the internet and a very large number of endpoints with approximately 900,000 authorised users, is an obvious hacker's honey-pot. In our opinion, the privacy risks are not worth the very limited benefits that will flow to most, if not all patients.

An area of risk is the use of health data in contexts other than patient healthcare. The government has expressed interest in linking health data with other data⁹; in releasing data for secondary use¹⁰; and in releasing health data sets as part of the proposed Consumer Data Right bill (section 1.47)¹¹. One of the major unknowns, yet to be fully explored, analysed and addressed is the issue of de-identifying and subsequently re-identifying health data^{12 13}

Systemic Risks

There would appear to be a major risk associated with the way that the ADHA has managed (or failed to managed) system problems.

According to media reports^{14 15}:

a technical problem with the My Health Record system had hampered attempts by some doctors to upload clinical information about their patients to the system.

According to a leaked briefing, some doctors in clinics using older IT systems were left oblivious to the problem, leading them to believe patient information had been properly updated when it hadn't. The briefing warned it created risks of "missing clinical information in

a consumer's My Health Record" and "amendments not uploading resulting in out-of-date or incorrect information".

There was discussion on Dr David More's Australian Health Information Technology blog for Wednesday, January 30, 2019 ¹⁶ on this issue. The comments are informative. Most are anonymous because they are from people who are in a potentially vulnerable, but knowledgeable position.

There was a follow-up blog post after the second Guardian article ¹⁷ which made reference to a comment ¹⁸ posted a few days earlier:

The ADHA spokesperson is fraudulent in the facts, or ADHA clearly has no record. The Microsoft Security Patch was released several months prior to ADHA official commencement. NEHTA tried to address the issue and it was NEHTA not ADHA that released the updated guidance.

This issue was carried over to ADHA with then then acting CEO of NEHTA. The issue was presented to the then interim CEO of ADHA. The current CEO, COO and The head of Core Services and System Operations. This issue has been carried with ADHA is has been well known from Directors to General Managers to Executives. The response to this has not been to work to ensure it is resolved but rather to leave a trail of "hush" sackings.

What we are witnessing is panic and ass covering. Internally the witch hunts have begun, but not towards The CEO, COO, Board or Executives for their neglect but simply because cruelty towards staff and the public are at the core of their DNA.

Whatever the true situation regarding the problem and its resolution (or not), there was a risk; there may still be a risk. The way the ADHA has handled the issue does not engender trust in the system or ADHA's ability to manage technical risk.

The above problem clearly illustrates that the biggest risk to patients is the existence of My Health Record.

My Health Record is not a separate, stand alone system. It is part of a much larger, interconnected system of systems. There are hospital systems, medical centre systems, GP systems, smartphone apps etc etc.

My Health Record links all these systems in a variety of ways. By doing so it introduces a huge number of weaknesses and potential problems, all outside the control of ADHA. Data comes from systems outside My Health Record and goes to other systems, also outside My Health Record.

The flows of data outside My Health Record are not under the control of My Health Record or even visible to it. The interfaces into My Health Record are also largely outside the control of ADHA.

All the clinical data in My Health Record has come from other systems. The idea that someone can permanently delete a My Health Record is just plain silly. The data in a deleted My Health Record almost certainly still exists in the ecosystem and if required it can probably be reconstructed, along with much more data.

The reality of My Health Record is that it does not address the problem of data fragmentation across the healthcare industry (which was its original purpose), it does not deliver interoperability, all it does is punch security, privacy and patient safety holes in the healthcare data ecosystem.

Appendix B provides further information on the risks to the privacy of patients.

Issue 3 Monitoring and Evaluation of the System

The ADHA on its website and in its board papers concentrates exclusively on the delivery and monitoring of its supposed benefits. There is little or no information on costs or risks.

My Health Record has never been properly evaluated. As we asserted in the audit request in 2017, we do not believe the My Health Record project was sufficiently well analysed and the potential benefits and expected costs properly identified and/or justified. It is highly unlikely that a full business case for the My Health Record was ever prepared. This is based in part upon the total lack of justification ever provided for the claimed benefits and there being no evidence that the full costs of the system have been estimated.

Financial Costs and benefits

The government has indicated that the cost of developing, implementing and supporting the My Health Record system is approximately \$2billion.

One of the major costs not mentioned by the government is that incurred by healthcare professional using the system. To the best of our knowledge, this has never been estimated. These are substantial and an order of magnitude can easily be estimated.

Our submission to the Senate inquiry ³ included the following (section 3.5)

The review of the PCEHR in 2013 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 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.

The government currently pays an incentive to GPs to upload patient documents to the My Health Record system ¹⁹. It is unclear how much these have been in total or how long such an incentive will last. As a minimum such expenditure should be included in any cost estimates.

To the best of our knowledge, there has been no realistic analysis of the financial benefits of My Health Record. For example, since July 2012, how many times has a My Health Record been accessed in the delivery of healthcare and provided critical information? What are the scenarios where My Health Record could potentially save time and money in the delivery of healthcare? How many times does each scenario occur per year? What is the required accuracy and completeness of the data for these benefits to be delivered? Does My Health Record data meet these requirements?

Other Costs

In addition to financial costs, there is increasing evidence that the use of electronic health record systems is resulting in physician burnout^{20 21 22 23 24 25 26}. This is from using their primary systems. The implementation and use of My Health Record will further exacerbate this well known problem.

We have seen no evidence that any analysis has been undertaken regarding the potential impact My Health Record may have on harm. It might be that My Health Record reduces or increases harm, depending on the situation and the state of the data in a patient's My Health Record.

There has been no indication that any of the above issues have ever been addressed or considered by the government. Without such analysis both prior to the initiative being approved and after it was implemented, the justification for My Health Record is based on wishful thinking.

Published Statistics

The only public evaluation of My Health Record are usage statistics published by the government on registrations and documents uploaded. The government claims this as usage, but they obviously aren't. Meaningful, healthcare usage means downloading data and using it in the delivery of healthcare.

The following table is based upon published government statistics (originals available on request).

	8-Jan-17	2-Jul-17	14-Jan-18	1-Jul-18	13-Jan-19
# days		175	196	168	196
Total Registrations	4,473,322	4,970,687	5,457,903	5,905,604	6,450,277
Increase		497,365	487,216	447,701	544,673
Daily Rate of Registration		2,842	2,486	2,665	2,779
Total Shared Health Summaries uploaded	512,749	910,840	1,380,911	1,871,039	2,350,961
Increase		398,091	470,071	490,128	479,922
Daily Rate of Shared Health Summary uploads		2,275	2,398	2,917	2,449

The key information is the daily rate of uploads of Shared Health Summaries which show the total number ever uploaded since July 2012. Shared Health Summaries are not edited, they are replaced.

Since July 2012 2,350,961 Shared Health Summaries have been uploaded.

This means that the maximum number of My Health Records that contain a Shared Health Summary cannot be greater than 36%

In the calendar year 2018 the number of Shared Health Summaries uploaded represents a maximum of 15% of registrations. This means that at least 85% of people registered for a My Health Records have either an empty Shared Health Summary or one that is over 12 months old.

The daily rate of Shared Health Summary uploads in the six months of the opt-out period was less than that in the previous six months. The publicity surrounding My Health Records did not result in more people arranging with their GP to either upload a Shared Health Summary for the first time or to update one if they already had one.

Furthermore, the daily rate of registrations in 2018 was 2,726 and that for Shared Health Summaries was 2,665. In other words, more people registered for My Health Records than uploaded a Shared Health Summary.

One would expect that people who opted in to the system in 2018 would create their first Shared Health Summary and that a significant number of existing records would be updated. This cannot be happening.

This means the trend for My Health Records is that the data in it is gradually becoming older and over time the proportion of records with data less than a year old will decline.

It is reasonable to conclude that Australian patients who already have registered for a My Health Records under the opt-in arrangements are not eager to make use of the system.

The above data all refer to registrations and uploads of Shared Health Summaries. The government has never released any similar statistics regarding download rates or meaningful use of the data in My Health Records.

It should also be noted that as soon as the opt-out initiative is completed, the proportion of registrations that will have a Shared Health Summaries less than a year old will fall to approximately 5%.

After six years of use and at least \$2billion expenditure, fewer than about 6% of registrations will have a Shared Health Summary less than one year old.

Of the total population of Australia this figure will be less than 4%

It is difficult to see how this number can increase substantially. With the system as opt-in, one would assume that these people wanted a My Health Records. When it is changed to opt-out, a large number of people will not know they have one and will not be inclined to upload data into it.

In response to a written question in Senate estimates on 24/10/2018, the government recently released data on the number of My Health Record registrations that have been cancelled ²⁷.

The Department of Health's answer states "The total number of My Health Record registrations that had been cancelled as of 11 November 2018 is 287,995". This number raises questions about the statistics released by the ADHA. For example, as of 13 January 2019 (the latest available data) 6,450,277 consumers were registered. Does this number include those registrations that have been cancelled?

An indication of the answer could be inferred from the statistics the ADHA provides about healthcare provider organisations registered. The ADHA data shows that the total is 15,315. However looking at the detailed figures, this total includes "Organisations with a cancelled registration". This strongly suggests that the ADHA statistics are lifetime totals (i.e. the number since July 2012), not current totals.

If this is true then the statistics released by the ADHA are meaningless when it comes to assessing the true state of the data in My Health Record. It means that the analysis of data in the table above becomes questionable – those questions include:

What does the "Total Registrations" number actually represent? Does the figure for "Shared Health Summaries" uploaded include those that were uploaded to records that have subsequently been cancelled? It could be argued that the ADHA seems to be keen to exaggerate the number of registrations, institutions and documents associated with the My Health Record rather than identifying healthcare outcomes. Why this is so is an interesting question, one that we are unable to answer, but would be interested in learning the answer if it is true.

Conclusions

The value to patients and healthcare professionals of the My Health Record system as claimed by the government is based upon guesswork and has never been substantiated. The benefits are



usually predicated on the invalid assumptions that it is a complete medical record of a patient that is accurate and kept up to date, and that most Australian's will have one.

The full costs have never been identified and published. A simple estimate of the usage of the system and the (unjustified) value of the system would indicate that it makes no economic sense whatsoever.

The government claims that Australia leads the world in having a patient controlled health record²⁸. They are undoubtedly correct. However the reason why Australia is unique is because nobody else considers that such a system has a significant, if any value. Even full national health record systems such as those that have been tried in the UK, France and Germany have not been embraced by the medical professions or their patients. The most frequent reason cited is that additional, administrative tasks such a record keeping cost far more in time and effort than they deliver in clinical benefits.

The Australian healthcare industry has not accepted the system as being useful. Most Australians are either unaware of the system, or are not convinced of its benefits.

There is no clinical benefit from the government running a national database of mostly useless health data, however there is a significant risk to patient privacy both from the system itself and its secondary use. Unless the government can present a good argument that the benefits outweigh the costs and risks, we recommend that the system be discontinued.

Appendix A Purpose

In the PCEHR Concept of Operations²⁹ that was circulated for discussion prior to the release of the My Health Record in July 2012 it included:

Section 1.1

The need for a PCEHR System

The implementation and adoption of a national PCEHR System addresses a current challenge faced by the Australian health system - the fragmentation of information spread across a vast number of different locations and systems. In many healthcare situations, quick access to key health information about an individual is not always possible.

and

The purpose of the PCEHR System is to address information fragmentation by allowing a Patient to more easily access their own health information and make their health information securely accessible to different healthcare providers involved in their care.

In the explanatory memorandum accompanying the original My Health Record legislation published in 2011 it stated that:

The PCEHR system

As part of the 2010-11 Budget the Australian Government announced funding of \$467 million over two years to build the key national components of the national PCEHR system. The PCEHR system is the next step in using e-health to enhance the healthcare system. It enables the secure sharing of health information between a consumer's healthcare providers, while enabling the consumer to control who can access their PCEHR.

The PCEHR system builds on the foundation laid by the introduction of national healthcare identifiers for consumers, healthcare providers and healthcare provider organisations, as well as the National Authentication Service for Health, clinical terminologies and methods for communicating health information between healthcare providers such as discharge summaries and electronic referrals.

The PCEHR system places the individual at the centre of their own healthcare by enabling access to important health information when and where it is needed, by consumers and their healthcare providers. A PCEHR will be assembled from distributed participating repositories which will hold summarised clinical information. These repositories will be operated by a mix of private and public sector organisations and will need to conform to strict specifications.

The development and operation of the PCEHR system will provide a range of benefits to healthcare consumers, providers and service organisations, and to the Australian economy more broadly. The benefits arise directly from providing consumers and healthcare providers with better access to health information, and indirectly by enabling reform of the way healthcare is delivered.

It is clear that the intention was to make it easier for health professionals and patients to more easily access a patient's health data that is spread around multiple existing systems (repositories).



It is also useful to examine what the government currently claims is the purpose of My Health Record.

From the government website ³⁰

What is My Health Record?

My Health Record is an online summary of your key health information.

When you have a My Health Record, your health information can be viewed securely online, from anywhere, at any time – even if you move or travel interstate.

This gives the impression that when a patient is registered for a My Health record they will get a summary of their “key health information” and that “your health information can be viewed securely online”.

The reality is that this is simply not true.

The government’s website ³¹ also says

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 Patiental health information and notes straight away.

Uploading old tests and scans

Your medical history, such as older tests and scan reports, will not be automatically uploaded to your My Health Record. Only new reports can be uploaded by participating pathology labs or diagnostic imaging providers.

Talk to your doctor about uploading a shared health summary to your My Health Record. This summary can capture important past health information such as results from previous tests or scans, which can be shared with your other treating healthcare providers.

The original intent of the My Health Record was that data would be “assembled from distributed participating repositories” It is obvious from the government’s website and the operation of the system that data is uploaded to a central database, rather than the data remaining in repositories controlled and managed by health professionals. In other words, the My Health Record does not meet its intended purpose.

Appendix B Risks

Weakening of the privacy protections of MBS/PBS data in the National Health Act (1953)

In March 2008 the Privacy Commissioner issued Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs under section 135AA of the National Health Act 1953 (Cth) ³²

One of the guidelines, 7.2, applies to the Department of Health and says:

The Secretary of the Department, or delegate, must not permit the establishment of a system which stores claims information from both the Medicare Benefits Program and Pharmaceutical Benefits Program in a combined form.

Without consultation or public announcements, the Department of Health inserted an exception to the National Health (1953) Act ³³ which weakened the privacy protections that applied to MBS/PBS data. This legislation, that also enabled changing the system to opt-out, was passed in 2015.

The exception was required because the Department wanted to extract data from DHS' MBS and PBS systems and store them in a Departmental system (My Health Record)

This is the exception:

(5AA) Nothing in this section, or in the rules issued by the Information Commissioner, prevents the My Health Record System Operator including information to which this section applies in the My Health Record of a healthcare recipient.

Failure to implement the National Authentication System for Health (NASH)

NASH was never implemented ³⁴, as intended in the PCEHR Concept of Operations ²⁹ or in the NASH Concept of Operations ³⁵.

It was intended to uniquely identify individual healthcare users of the My Health Record by means of a token system (e.g. smartcard). The government's website now makes it clear that only the healthcare institution accessing a patient's record are identified and logged. Considering that a large group of hospitals (e.g. all of South Australia's public hospital system) is a single institution, this level of granularity is of little use to a patient interested in who has access their health record.

The following is from the NASH concept of operations.

1.2 System overview

The NASH is a system that provides authentication credentials for healthcare provider organisations, healthcare provider individuals and other healthcare delivery organisations that may be issued with a Healthcare Identifier.

The NASH:

- *Enables healthcare providers to assert their Healthcare Identifier (HI) based identity accurately, securely and consistently within a healthcare delivery context. This includes use within electronic communications such as the Personally Controlled Electronic Health Record (PCEHR), Referrals, Diagnostic Services, Discharge Summaries, Medications Management and other clinical packages.*
- *Provides a framework in which credentials for other Healthcare authentication purposes may be implemented in a consistent way which enables those credentials to be interoperable with NASH credentials.*

and

1.2.2 General nature of system

The NASH is more than just business services and technology. It combines technology under enabling legislation, policy and operational services that work together to facilitate consistent use of authentication for healthcare providers with healthcare delivery.

NASH will provide a strong authentication service for the Australian healthcare sector and contribute to providing a capability that "...ensures that transactions are private, traceable and only conducted by known identities..."

The NASH framework will provide:

- *An overarching set of authentication policies and procedures to define and endorse the issue and management of trusted digital credentials to all participants in the healthcare sector, enabling the traceability of eHealth transactions with trusted identities whilst respecting appropriate privacy and confidentiality*
- *A centralised source of authentication Credentials for healthcare providers, based on the use of Public Key Infrastructure (PKI) and Tokens (such as Smartcards)*
- *A PKI hierarchy dedicated to eHealth in which healthcare communities are able to issue and manage authentication credentials locally, supported by national infrastructure*
- *A governance approach for the NASH PKI*
- *Authentication Credentials that are based on well-established standards that are supported by existing systems and applications. This will mean that the NASH credentials will be usable with little or no extra coding required by implementers.*

Currently there is no national capability within the Australian healthcare delivery sector that provides standardised trusted digital credentials for the purposes of reliably identifying and authenticating any eligible party across the entire sector. Without the accurate identification and authentication of healthcare provider individuals and organisations, eHealth systems are only able to operate across limited communities within the overall sector.

The failure to implement NASH means that the last paragraph, above, details the current situation.

Section 71 of My Health Record Legislation

Section 71 of the My Health Record Act ³⁶ limits legislative protection to data collected explicitly and solely for My Health Record. Most data in My Health Record either comes from or has been transferred to other systems, sometimes via My Health Record, other times directly. This means that the My Health Record legislation does not apply to those data.

For reference, this is Section 71 in full

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.

Section 71 restricts the legislative protection of a patient's privacy to only a very small amount of data in My Health Record – primarily, the contents of a Personal Health Summary, and an Advanced Care Directive. All other medical data is unprotected by the My Health Record legislation.

References

- 1 Request for a review by ANAO of the Department of Health's My Health Record initiative
http://www.drbrd.com/docs/myhr/ANAO_MyHR_Audit_request.pdf
- 2 Australian Privacy Foundation's evidence to Community Affairs References Committee
11/09/2018
My Health Record system
<https://www.aph.gov.au/DocumentStore.ashx?id=277cb8da-def9-4c39-8c31-95b8cae7f5e6&subId=659502>
- 3 Australian Privacy Foundation's evidence to Community Affairs References Committee
11/09/2018
My Health Record system
<https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees/commse n/0b1b0fd0-9f50-442e-ac5d-0401c291161c/0003;query=Id:%22committees/commsen/0b1b0fd0-9f50-442e-ac5d-0401c291161c/0000%22>
- 4 Australian Privacy Foundation campaign page
<https://privacy.org.au/campaigns/myhr/>
- 5 AMA Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System
<https://ama.com.au/system/tdf/documents/AMA%20Guide%20to%20using%20the%20PCEHR%20Final%20June%202012%20Formatted%20300812.pdf?file=1&type=node&id=36028>
- 6 My Health Record website, privacy policy, under Access Controls
<https://www.myhealthrecord.gov.au/about/privacy-policy>
- 7 "The Australian Women & Digital Health Project: Comprehensive Report Of Findings
<https://apo.org.au/sites/default/files/resource-files/2019/01/apo-nid220326-1332626.pdf>
- 8 The truth about My Health Record
Under: Are There Alternatives?
<http://medicalrepublic.com.au/truth-health-record/15335>
- 9 Multi-Agency Data Integration Project (MADIP)
<http://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP>
- 10 Implementing the Framework to guide the secondary use of My Health Record system data
<http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth-framework>
- 11 Treasury Laws Amendment (Consumer Data Right) Bill 2019
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6281
- 12 Health Data Governance: Re-identification of health records
<https://www.pwc.com.au/legal/assets/legaltalk/data-governance-11may17.pdf>

13 Health record details exposed as 'de-identification' of data fails
<https://www.smh.com.au/technology/australians-health-records-unwittingly-exposed-20171218-p4yxt2.html>

14 My Health Record: government warned of 'significant' patient data glitch
<https://www.theguardian.com/australia-news/2019/jan/25/my-health-record-government-warned-of-significant-patient-data-glitch>

15 My Health Record 'minor glitch' still generating thousands of pages of internal files
<https://www.theguardian.com/australia-news/2019/feb/15/my-health-record-minor-glitch-still-generating-thousands-of-pages-of-internal-files>

16 This Is What Is Actually Called Deliberate Deception Of The Public. It Is Appalling, Dishonest and Heads Should Roll If True
<https://aushealthit.blogspot.com/2019/01/this-is-what-is-actually-called.html>

17 Blog Readers Provide Additional Information Regarding A Very Worrying Article Around The ADHA And Its Attitude To Honesty And Transparency
<https://aushealthit.blogspot.com/2019/02/blog-readers-provide-additional.html>

18 Comment on Guardian Article
<https://aushealthit.blogspot.com/2019/02/the-college-of-gps-racgp-takes-look-at.html?showComment=1550359199992#c9033243460558718560>

19 DHS eHealth Incentive
<https://www.humanservices.gov.au/organisations/health-professionals/enablers/ehealth-incentive/47761>

20 EHR Technology a Key Contributor to Physician Burnout
<https://ehrintelligence.com/news/ehr-technology-a-key-contributor-to-physician-burnout>

21 EHR Use, Administrative Burden Accelerating Physician Burnout
<https://ehrintelligence.com/news/ehr-use-administrative-burden-accelerating-physician-burnout>

22 Work–Life Balance, Burnout, and the Electronic Health Record
[https://www.amjmed.com/article/S0002-9343\(18\)30286-9/fulltext](https://www.amjmed.com/article/S0002-9343(18)30286-9/fulltext)

23 Doctors say electronic health records up burnout risk
<https://www.futurity.org/doctors-electronic-health-records-burnout-1925112/>

24 Stress from using electronic health records is linked to physician burnout
<https://news.brown.edu/articles/2018/12/burnout>

25 Physician stress and burnout: the impact of health information technology
<https://academic.oup.com/jamia/advance-article-abstract/doi/10.1093/jamia/ocy145/5230918?redirectedFrom=fulltext>

26 EHR Alarm Fatigue May Lead Physicians to Quit Their Jobs
<https://ehrintelligence.com/news/ehr-alarm-fatigue-may-lead-physicians-quit-jobs>



27 How many people have cancelled an existing MHR to date? Please provide by a breakdown by state/territory.

<https://www.aph.gov.au/api/qon/downloadattachment?attachmentId=b7528c9e-7ec4-4351-8e97-5ba6479477f5>

28 Media release - International review puts Australia ahead in personal control of electronic health records

<https://www.digitalhealth.gov.au/news-and-events/news/media-release-international-review-puts-australia-ahead-in-personal-control-of-electronic-health-records>

29 PCEHR Concept of Operations

This document is no longer publicly available from the ADHA website.

The following is a link to a copy. It was referred to in ADHA's submission to the Senate inquiry, so it is assumed to be a valid copy.

https://www.privacy.org.au/Campaigns/MyHR/docs/PCEHR_110912_Concept_of_Operations.pdf

30 Federal Government My Health Record website

<https://www.myhealthrecord.gov.au/for-you-your-family>

31 Federal Government My Health Record website

What's in My Health Record

<https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record>

32 Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs

Issued by the Privacy Commissioner under section 135AA of the National Health Act 1953 (Cth)

Date of Issue: 6 March 2008

Date of Effect: 1 July 2008

<https://www.legislation.gov.au/Details/F2008L00706/>

33 National Health Act (1953)

<https://www.legislation.gov.au/Details/C2018C00410>

34 Media Report on the failure of the NASH project

IBM's NASH deal gets terminated

<https://delimiter.com.au/2012/10/23/ibms-nash-deal-gets-terminated/>

35 NASH Concept of Operations

<https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-1011-2012/nehta-1014-2012>

Login required, a version is available here

http://www.drbrd.com/docs/myhr/NEHTA_1014_2012_NASH_ConceptOfOperations_v1.0.pdf

36 Current My Health Record Legislation,

<https://www.legislation.gov.au/Details/C2018C00509>