



Whose Health Record is it anyway?

Australian Council of Trade Unions submission to the Senate
Standing Committee on Community Affairs Inquiry into the My
Health Record system.

ACTU Submission, 14 September 2018
ACTU D. No 183/2018

Contents

| | |
|---|---|
| Introduction | 1 |
| Background on MHR..... | 1 |
| Benefits of the MHR system..... | 1 |
| Unions concerns about MHR impacts on workers..... | 2 |
| Case Study 1 – Pre-Employment | 3 |
| Case Study 2 – Employment | 3 |
| Case Study 3 – Workers Compensation..... | 3 |
| Specific concerns about MHR policy and legislation..... | 4 |
| Inadequacies of the Healthcare Identifiers Act 2010 (Cth) protections | 4 |
| Access and disclosure | 5 |
| Lack of effective control of information upload | 6 |
| Data longevity and genomic data | 6 |
| Opt-out and default settings..... | 7 |
| Solutions..... | 7 |

Introduction

The Australian Council of Trade Unions (ACTU) welcomes the opportunity to make a submission to this inquiry. The ACTU is the peak body for Australian unions and represents 1.6 million union members Australia wide. As the voice of workers, the ACTU believes that this inquiry and the scrutiny of the My Health Record (MHR) system it represents are crucial.

Australian unions have deep and abiding concerns about the current MHR legislation and the impact it will have on the rights of workers to keep their medical information private. While we acknowledge the potential clinical merits of a centralised health records system, we believe that the current formulation of the MHR system leaves open unacceptable privacy gaps. This submission will outline a number of privacy, access and legislative concerns that the ACTU believes must be addressed. It will also outline our proposals to address these issues while attempting to maintain the potential clinical benefits that centralised health data can have for patients and clinicians.

Background on MHR

The concept of an E-Health Record (EHR), then known as the Personally Controlled Electronic Health Record (PCEHR), was originally introduced in Australia 2012 on an opt-in basis with the name changing to 'My Health Record' in 2015.

My Health Record is an online summary of an individual's key health information and is managed by the Australian Digital Health Agency (ADHA). Initial uptake on PCEHR and MHR was slow. The legislation was amended in 2015 through Schedule 1 of the *Health Legislation Amendment (eHealth) Bill 2015*. This allowed the Minister to make rules by legislative instrument, including rules to change from an opt-in to an opt-out scheme. After an initial trial involving a million accounts, by 2018 only 5 million Australians had opted to create a My Health Record. In May 2018, the ADHA announced it would create a My Health Record for every Australian who had not opted out of the system, giving the public only between 16 July and 15 October 2018 to opt out.¹ The Health Minister later extended the opt-out period to 15 November 2018. After this time, MHRs will be accessible to the individual patient and every medical practitioner that the individual attends. Patients retain some control over what data others can access, but in some circumstances, the information can be disclosed without the patient's consent. This announcement received a mixed response, with privacy advocates expressing deep concerns about both the MHR systems privacy settings and the decision by the government to reverse an opt-in system to an opt-out system. Some Clinicians, academics and health workers however emphasised the utility and importance of such systems, urging the public to remain in the system.²

Benefits of the MHR system

Prior to entering into a discussion of the concerns that the ACTU has with the current MHR model, it is important to acknowledge the real clinical and workplace benefits that such a system could deliver. Genuine clinical and workplace benefits could be realised in areas such as:

¹ <https://www.myhealthrecord.gov.au/news-and-media/media-releases/my-health-record-opt-out-date-announced>

² <https://theconversation.com/my-health-record-the-case-for-opting-in-99850>

- Reductions in the rate of medication errors;
- Reduced and more efficient pathology ordering due to increased availability of previous ordering information and test results;
- Increases in system efficiency reducing administrative demands on healthcare staff;
- Significant benefits to medical research through greater access to de-identified population-level data.
- Greater access to medical information during emergencies; and
- Reductions in doctor-shopping, over-prescription and greater detection, and hopefully treatment, of addictions causing these behaviours.

These benefits are real and it is no exaggeration to say that they may mean the difference between life and death for some number of patients each year and that they will make a real positive impact on the work done by the thousands of healthcare professionals in Australia. It is surely for these reasons that the MHR has the support of both the AMA and a RACGP, whilst acknowledging that there are, at the very least, 'ambiguity' around access and privacy issues.³ Australian unions recognise these benefits, and this is why we support, in principle, the concept of E-health records. It must be acknowledged however that any such system, no matter how it is constituted, represents some compromise position in striking the right balance between clinicians' needs for comprehensive medical information and patients' needs to restrict and control their medical information, along with privacy and security concerns.

The implementation of the current MHR system and legislation appears to have made a number of choices about this balance that the ACTU believes to be concerning and which should be remedied prior to the system 'opting in' millions of Australians – potentially without their knowledge.

Unions concerns about MHR impacts on workers

Union concerns about the MHR can be broadly divided into two categories: Impact on workers and privacy concerns. Australian union's concerns about MHR's impact on workers are predominantly related to employer and insurer access to the MHR data as part of pre-employment checks, worker's compensation processes and as part of regular employment-related health checks. The ACTU is concerned that it appears the default settings may allow:

- Employer-nominated doctors – and by extension employers - to have access to job seekers' medical history during pre-employment medical assessments or regular employer sponsored medical examinations/assessments;
- Employer/insurance company-nominated doctors to have access to injured workers' unrelated medical history, such as during independent medical examinations required under workers compensation laws; and

³ <https://www.theguardian.com/australia-news/2018/jul/25/my-health-record-ama-says-it-will-do-whatever-it-takes-to-ensure-privacy>

- Health information recorded in the My Health Record to be disclosed for ‘secondary use purposes’ under control of a Governance Board which has not yet been established.

We are concerned that, with these settings, employers and insurers would be able to gain access to workers’ detailed medical records – allowing discrimination on the basis of medical history. This would represent an unacceptable invasion of privacy for workers and would place ever more power in the hands of employers.

Below are three case studies which illustrate hypothetical scenarios under the present default settings about which we are deeply concerned.

Case Study 1 – Pre-Employment

Manisha is an office worker who in an old job needed to take 6 weeks off for stress that was approved by her private doctor, who also prescribed some medication that is commonly associated with mild depression. Manisha returned to work 18 months ago and has worked successfully ever since.

Manisha is looking to progress her career and is applying for a new job and the company she is seeking work with has a medical doctor in house or available to them for advice. Manisha has a great resume and impressed in the interviews and the company is on the verge of hiring her.

The company performs a My Health Record check on Manisha as part of their standard pre-employment checks before hiring new staff. The company doctor sees that Manisha took stress leave and depression medication as part of her digital My Health Record and reports it to the company who then decide not to hire Manisha.

Case Study 2 – Employment

5 years ago Shinji went through a period of using illicit drugs on the weekends. There was no impact on his workplace performance. He eventually decided to stop using and sought help from a doctor who prescribed medication as part of a rehabilitation program which Shinji successfully completed and has been ‘clean’ ever since. Shinji attends an annual free medical provided by his employer. It is understood that any information relevant to Shinji’s employment arising from the consultation will be passed on to Shinji’s employer. Shinji’s medical history as part of his My Health Record includes medication related to his recovery treatment and is made known to the employer. They have flagged Shinji for increased drug tests at work as a result and will keep a close eye on his performance and behaviour.

Case Study 3 – Workers Compensation

Hamid injured his right arm at work and is entitled to workers’ compensation entitlements, both lump sum and payments to cover ongoing medical treatment.

The insurance company doctor accesses Hamid’s My Health Record and discovers that Hamid injured his right arm 8 years ago playing footy on the weekend but was left with no real residual deficit. The insurance company then uses the information accessed via My Health Record as the basis for claiming a reduction to Hamid’s payout and ongoing assistance because they argue Hamid already has a pre-existing medical condition with his right arm.

We believe that many workers would, if they were aware these scenarios were possible, strongly object to their employer potentially gaining access to their detailed health records. While the

government has attempted to deny that such access is possible⁴, citing the *Healthcare Identifiers Act 2010* (Cth) (HI Act), the ACTU has received legal advice that such assertions are optimistic at best due to issues with both the HI Act and the MHR system design. These specific issues, and others, are explored in the next section of this submission.

Specific concerns about MHR policy and legislation

Inadequacies of the Healthcare Identifiers Act 2010 (Cth) protections

As referenced above, the government's response to Australian unions' concerns about employer and insurer access to the MHR system has been to point to the safeguards integrated into the HI Act. The Government's argument has been that s 14(2) of the HI Act prohibits healthcare providers from collecting, using or disclosing a healthcare identifier number to access a person's My Health Record for employment and insurance purposes. Section 14(2) of the HI Act makes it illegal to use the Healthcare Identifier of a patient to access health information for the purpose of communicating or disclosing health information for purpose of:

- underwriting a contract of insurance that covers the healthcare recipient;
- determining whether to enter into a contract of insurance that covers the healthcare recipient (whether alone or as a member of a class);
- determining whether a contract of insurance covers the healthcare recipient in relation to a particular event; or
- employing the healthcare recipient.

The ACTU is of the view that that this protection, is not adequate in relation to MHRs. The exclusions under the HI Act could only apply in cases in which a patient's individual Healthcare Identifier (IHI) is used to access their MHR. This might be sufficient if the IHI is the only method of accessing a patient's MHR, but it appears from the government's own explanation of the MHR provider portal that this is not the case. The portal guide makes clear that MHRs can be accessed using either the IHI, a Medicare number or a Department of Veteran's Affairs number.⁵ If this is the case and if it is also the case that the HI Act protection only applies when the IHI specifically is used, then the protections under that act are radically insufficient to protect worker's privacy – particularly if those wishing to gain access to MHR records are aware of this loophole. Anecdotal advice, in line with common sense, suggests that a Medicare number is used to access the portal in the vast majority of cases.

The exclusion in s14(2) of the HI Act does not in any event protect disclosures to employers arising from health checks during employment because the relevant exclusion only applies to health information disclosed for the purpose of 'employing the healthcare recipient', that is, during recruitment, rather than where the recipient is already employed.

⁴<https://www.smh.com.au/business/workplace/unions-urge-members-to-opt-out-of-myhealth-record-20180806-p4zvr6.html>

⁵ <https://www.digitalhealth.gov.au/files/assets/cup-articulate/using-the-provider-portal/providerPortal/index.html>

Access and disclosure

Under s61 of the *My Health Records Act 2012 (Cth)* (MHR Act), a participant in the MHR system is authorised to collect, use and disclose a healthcare recipient's health information in their MHR for the purpose of providing healthcare (in accordance with the recipient's MHR privacy settings). 'Healthcare' means a 'health service' as defined by s6FB of the *Privacy Act 1988 (Cth)*, which is defined very broadly. A 'health service' includes, amongst other things, any activity intended or claimed to assess, maintain or improve an individual's health. This means a broad range of persons – medical, allied health and other practitioners, including dentists, podiatrists, occupational therapists, music therapists, social workers and so on, may be able to access a patient's full medical history on the patient's MHR, and even where the medical information is unrelated to the issue at hand, unless the patient imposes security restrictions. While this is not necessarily an undesirable outcome, members of the public should be made aware of the full range of persons who might access their MHR and the extent of access under the default settings.

A further concern is that s70(1) of the MHR Act authorises the System Operator to disclose health information within an MHR if it reasonably believes it is necessary for certain purposes of an enforcement body, including preventing/investigating/remedying, crime, breaches of a laws imposing a penalty, and/or the protection of public revenue. Disclosure can be to an entity other than an enforcement agency for these purposes.

It is conceivable in the wake of the 'Robo debt' scandal that this Government could use this legislation to enable Centrelink to access the population's MHR records for the purpose of trying to claw back disability and other welfare payments. In the case of 'Robo debt' this was done by using software to analyse Centrelink and ATO records and then issuing debt notices on the basis of any superficial anomaly and putting the onus on the payment recipients to disprove their 'debt'. A high proportion of these 'debts' were later found to be unfounded. One can imagine s70(1) of the MHR Act being used to match health records against Centrelink data in a similar way for the putative purposes of protecting public revenue.

We are further concerned that the definition of 'enforcement body' refers to that in s6(1) the *Privacy Act 1988 (Cth)*, which primarily includes various crime enforcement agencies such as state and Federal Police and public prosecutors. However, it also includes the Immigration Department and any other "...agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law".⁶ This would appear to include industry-specific licensing bodies such as nursing, medical and other AHPRA registered professions, law societies, plumbing, and electrical trade license issuing/monitoring authorities.

While we understand the government is pursuing an amendment to the MHR Act to prevent enforcement bodies accessing records without a court order, all access to MHRs under s70(1) should be subject to court order and should be limited to crime enforcement agencies for the purposes of investigating crime.

⁶ *Privacy Act 1988 (Cth)* s6(1)f.

There are other aspects of the legislation that leave the class of persons and entities that can access personal health information in MHRs too open-ended. The ADHA's 'My Health Record: Frequently asked questions' website appears to be inaccurate.⁷ The website states that:

"Only registered healthcare providers involved in your care and who are registered with the My Health Record System Operator are allowed by law to access to My Health Records."

However, participants in the My Health Record system able to access health information on MHRs also include contracted service providers providing services to registered healthcare providers.⁸ Further, under s98 of the MHR Act, the System Operator can delegate one or more of its functions to various listed persons and, with the consent of the Minister, to any other person whatsoever.

The ADHA states that:

*"This delegation is used for administrative and procedural matters - for example, to enable the Department of Health to provide education on the My Health Record system. This does not and cannot provide access to individuals' personal records or any other health information in My Health Record."*⁹

Whilst the legislation places restrictions on the purpose for which health information can be accessed, the legislation clearly states that the system operator's powers include the power to 'collect, use and disclose health information about a healthcare recipient' for certain purposes (see s58) and those powers can be delegated under s98.

The legislation ought to be amended to remove the System Operator's capacity to delegate access to individuals' personal health information other than to those entities already prescribed in s98. Further, contractors providing services to registered healthcare providers should not gain access without a patient's explicit consent.

Lack of effective control of information upload

While the current settings for the MHR system appear to allow users with a significant amount of control over how and when information is accessed from their MHR, this is not evidently the case in terms of information being uploaded. The ACTU understands that under the current policy settings, a patient may object to information being uploaded, but that this objection must be made explicitly. Without such an objection, all medical information will be automatically uploaded to a patient's MHR. This system relies too greatly on patients being aware of their rights and having the expertise to understand what information is being uploaded to their MHR and what inferences may be drawn from it. We believe that users must have the same quantum of easy control over what information is uploaded to their MHR as they will have about who has access to that information.

Data longevity and genomic data

A concern that arises from the digital nature of the MHR, combined with the lack of control over information upload, is the likely outcome that the MHR will become a repository of vastly more

⁷ See <<https://www.myhealthrecord.gov.au/for-you-your-family/howtos/frequently-asked-questions>>, accessed 11 September 2018.

⁸ See s5 of the *My Health Records Act 2012* (Cth).

⁹ *Ibid.*

medical information than any paper record – both in terms of the quantity of information included but also in the type of information included.

As our understanding of human genetics improves and with advances in gene therapy for some conditions, it is not impossible to imagine a near future in which a patient's entire genetic code may be uploaded to their MHR. This may be problematic for a number of reasons. This information may be able to be used in future to predict future health outcomes, the likelihood of particular conditions appearing and other such predictive information. If proper safeguards are not put in place around the use of MHR data, genomic data could become a significant source of interest to health insurers seeking to deny claims or to increase costs based on genetic information. This is particularly concerning if we consider that MHR data may outlive the patient and indeed, through family linkage, affect the health records of future generations.

MHR must not result in a future in which someone is unable to work as a pilot due to their parent's alcoholism, for example, or in which people are expected to pay more for insurance due to the minutiae of their genetics.

Opt-out and default settings

As outlined in an earlier section of this submission, the government's decision to alter the MHR system from opt-in to opt-out appears to have been driven by insufficient take-up rates in the first five years of the system and the probable benefits of the system. While the ACTU has no in-principle objection to an opt-out methodology, we do believe that when such a system is used for a program with consequences as significant as the MHR system, greater consideration must be applied and proper and comprehensive protections embedded and guaranteed by law.

The current program settings have created a situation where many Australians, potentially without their knowledge, will be not only forced onto the MHR system, but will have MHRs created with the lowest possible privacy settings by default. It is our belief that when it is possible for someone to be unaware that a repository of their health records is being created, that repository should be protected by more than the user's security settings and certainly more than the current level of default security. Any such system, as acknowledged above, must strike a balance between access and privacy but any outcome where an Australian's health data might be shared without their knowledge must be considered to be unacceptable.

Solutions

As mentioned at the beginning of this submission, Australian unions believe that the MHR system can bring real benefits to Australians both as patients and workers in the health system. The issues we have outlined above are not intended as arguments against why such a system should be implemented, but as a list of issues to address. To this end, our proposed solutions to some of these issues can be found below:

- Directly including a clause similar to s14(2) *Healthcare Identifiers Act 2010's* (Cth) into the MHR Act that excludes access for the purposes described in that clause. The exclusion should clearly apply irrespective of how the MHR is accessed (i.e. using a IHI or Medicare number, etc) and also cover access during employment and not just recruitment. Some allowance has to be made for the sharing of information based on consent from the patient, but consent needs to be clearly delineated in the legislation and needs to rely on clear, informed consent of what the patient is agreeing to. Consent also needs to be purpose-based and be considered to expire when the purpose does;

- ‘enforcement bodies’ should include only crime enforcement agencies seeking access for the purpose of investigating crime and authorisation should require a court order;
- Non-compliance with MHR requirements around privacy must include significant penalties for both organisations and individuals;
- Legislative obligations around data security, privacy, probity etc must also apply to the holder of the database, not just those accessing it;
- Legislative safeguards against privatisation or commercialisation of the database;
- Clearer and easier to use controls over data upload;
- Taking measures aimed at increasing the default privacy settings for those automatically opted-in;
- Consideration should be given to the longevity of MHR data and the impacts that new data types being included in MHRs may have;
- The legislation ought to be amended to remove the System Operator’s capacity to delegate access to individuals’ personal health information other than to those entities already prescribed in s98. Further, contractors providing services to registered healthcare providers should not gain access without a patient’s explicit consent; and
- In light of the above, the opt-out date should be extended to allow these issues to be addressed.

address

ACTU
Level 4 / 365 Queen Street
Melbourne VIC 3000

phone

1300 486 466

web

actu.org.au
australianunions.org.au

ACTU D No.

183/2018

