Submission to the

Community Affairs References Committee

Inquiry on

My Health Record

Ideas in Technology – Healthcare – Education
https://www.futurewise.org.au

Introduction

Thank you for the opportunity to make a submission to the Committee's inquiry on myHealthRecord system.

About Future Wise

This submission is authored by Future Wise. We are a group of Australian professionals of varied backgrounds who seek to promote ideas that improve the long-term direction of Australia, particularly in the areas of technology, health and education. More information about Future Wise is available on our website.[1]

The primary author of this submission is Dr Trent Yarwood, an infectious diseases physician in public and private practice. While informed by his clinical practice, the opinions in this submission represent those of Future Wise and should not be taken to represent the views of the Cairns and Hinterland Hospital and Health Service, Metro North Hospital and Health Service, Queensland Health or the Royal Australasian College of Physicians.

Dr Yarwood is happy to provide further clarification on any area of the submission, or to provide in-person evidence to the Committee hearing, if required.

We wish to thank Mr Justin Warren for his assistance in proofing this submission.

[1] https://futurewise.org.au/

Summary of Submission

Future Wise wishes to submit:

- Electronic Health tools have the potential to improve patient care, patient safety and medical communication and Future Wise supports a transition to eHealthcare
- The myHealthRecord system in its current form has some of these benefits of eHealth, however they are modest, in some cases overstated, and when taken together are insufficient to justify the significant risks associated with the system
- An opt-out model does not allow individuals the opportunity to weigh the risks and benefits of the system to their health and privacy. We believe that - like other medical interactions - that this should be done under a model of informed consent
- The myHealthRecord system was initially designed as an opt-in system, and this means the security considerations may not be suitable to be directly translated to an opt-out system
- Future Wise does not believe that the average level of knowledge of information security of medical practitioners is sufficient for the profession to be the gatekeepers of informed consent; an opt-out model exacerbates this risk by doctors potentially promoting the benefits of the system uncritically without due consideration of the risks
- The secondary use provisions (see also: the discussion paper from Department of Prime Minister and Cabinet, and Future Wise's response to it[2]) are inherently risky to privacy, and should be treated as human-subject research under the principles of the Declaration of Helsinki, and informed consent obtained
- The risks to patient privacy from improper access by authorised users far exceeds that of "hacking" by external agents
- "Anonymised" data from myHealthRecord should not be assumed to be non-privacy intrusive, due to the ability for this data to be linked with

[2] https://futurewise.org.au/files/20180731_FW_Data.pdf

other datasets, allowing potential re-identification, as occurred with the MBS/PBS datasets on data.gov.au

- Future Wise broadly supports the changes in the *My Health Record Amendment (Strengthening Privacy) Bill 2018*
- We believe that access to myHealthRecord data by designated agencies should still occur with the knowledge of the primary document authors, wherever possible
- The risks of a shared health record repository are sufficient that we believe that assumed consent (ie opt-out) is unsuitable for a program of this nature
- While individuals from disadvantaged or marginalised backgrounds potentially have the most to gain from a shared health record system, they are also less likely to engage with it and may therefore have a greater privacy risk than the general population
- Access to myHealthRecord data by insurance companies and other commercial entities must not occur
- The general privacy protections afforded to Australians should ideally be strengthened, to better underpin complex digital transformation projects such as this one
- There should be greater engagement with both the general public, but also with specialist digital rights organisations in the planning and roll-out of large digital projects such as this one.

Responses to Discussion Questions

a) the expected benefits of the my Health Record System

Future Wise is generally supportive of electronic health, and recognises the potential benefits of eHealth systems, including reduction in medication errors at the point of prescribing[3] and also during communication between hospital and primary care.[4]

Communication between general practice and hospital has frequently been described as a potential source of medical error[5] and a potential target for increase in usability of information.[6]

While electronic health tools may offer some solutions to these issues, it is not clear to what extent myHealthRecord (as it is currently designed) is suitable for these purposes. As it is an online summary of clinical documents, it does not improve communication unless clinicians take measures to upload up-to-date documents, and the receiving clinicians access and make use of them. The platform supports eReferrals,[7] however most referrals are currently performed with paper or by facsimile.[8] Until the platform is more mature and uptake of digital referral systems is better amongst healthcare workers, Future Wise believes the benefits in these areas are significantly overstated.

The medication summary view currently functions as a "laundry list" of dispensed PBS medications, which does not provide the same degree of clinical utility as a current medication list that has been curated by a clinical pharmacist or medical practitioner. In practice, the online lists may have a low signal-to-noise ratio, whereby multiple monthly dispensing of regular medications (or the dispensing of short course medications - for example vaccines or antimicrobials) may obscure useful information by the sheer volume of items in these sections of myHealthRecord.

---

[3] Australian Commission on Safety and Quality in Health Care. Electronic medication management systems: a guide to safe implementation. 3rd edition. Sydney: ACSQHC; 2017 available online: https://www.safetyandquality.gov.au/wp-content/uploads/2017/11/Electronic-Medication-Management-Systems-A-guide-to-safe-implementation-third-edition.pdf

[4] Tong EY et al. Reducing medication errors in hospital discharge summaries: a randomised controlled trial. Med J Aust 2017; 206 (1): 36-39 doi: 10.5694/mja16.00628

[5] Kripalani S, LeFevre F, Phillips CO, Williams MV, Sasavia P & Baker DW. JAMA. 2007; 297:831-41

[6] Belleli E, Naccarella L & Pirotta M. Communication at the interface between hospitals and primary care. Aust Fam Physic, 2013; 42(12):886-90

[7] https://www.myhealthrecord.gov.au/for-healthcare-professionals/ereferrals

[8] https://www.healthcareit.com.au/article/ubiquitous-fax-queensland%E2%80%99s-ipswich-hospital-directs-gps-use-antiquated-tech-all-urgent

Similarly, aggregated MBS data provides little benefit to an individual patient or clinician, although this information may at least have epidemiological value if the record holder has not opted out of secondary use.

Two other purported benefits of the myHealthRecord system as promoted by the Australian Digital Health Agency (ADHA) include[9] the ability of healthcare providers to access information in the event of an emergency; and reducing the need for patients to recall—and for doctors to re-take—patients' medical histories.

In a true medical emergency, healthcare staff will deliver care urgently, and are unlikely to have time to consult myHealthRecord prior to implementing life-saving care. Even if myHealthRecord is consulted, in the event of a critical illness, it is unlikely to significantly affect management decisions except in a few cases (for example, major drug allergies).

If a patient is found critically injured and unable to be identified, then there will be no way of accessing the appropriate myHealthRecord, so no information will be able to be obtained. Patients who self-present will, in many cases, be able to recount medical history themselves, or if a carer or relative is present, then it is unlikely that my Health Record will provide major additional benefits.

As discussed above, the benefits of (for example) a medication list may be obscured if the shared health summary has not been recently updated, or if the summary view is unable to be easily parsed to the list of medications being currently taken by the patient rather than a list of those recently dispensed by a pharmacy under the PBS (which may also exclude non-PBS prescriptions as well as the issues of short-course medication described above).

[9] https://www.myhealthrecord.gov.au/for-you-your-family/my-health-record-benefits

b) the decision to shift from opt-in to opt-out

Future Wise believes that an assumed-consent, opt-out model is wholly inappropriate for records relating to individuals' health information, as it does not give record holders the chance to consider the risks of a myHealthRecord in an informed way before one is created for them. Furthermore, we believe that default opt-in consent for secondary use is a violation of the principles of the Declaration of Helsinki[10] (the medical profession's ethical framework for human subject research) and as such is not only inappropriate, but unethical and should be immediately halted.

In particular, the Declaration states:

> 9. It is the duty of physicians who are involved in medical research to protect the life, health, dignity, integrity, *right to self-determination, privacy, and confidentiality of personal information* of research subjects. The responsibility for the protection of research subjects must always rest with the physician or other health care professionals and never with the research subjects, even though they have given consent.
>
> 32. For medical research using *identifiable human material or data*, such as research on material or data contained in biobanks or similar repositories, *physicians must seek informed consent for its collection*, storage and/or reuse. There may be exceptional situations where consent would be impossible or impracticable to obtain for such research. In such situations the research may be done only after consideration and approval of a research ethics committee.
>
> [emphasis ours]

[10] https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

Future Wise has believes the current myHealthRecord system is incompatible with these principles for the following reasons:

Consent Processes

The media has reported multiple instances of individuals who have discovered they had myHealthRecords created for them that they did not request,[11] violating the right to self-determination and informed consent as outlined above.

Doctors' groups have expressed concerns about their roles in obtaining informed consent from patients for the creation of records,[12] raising questions about how effective their role in this process will be.

An important principle of informed consent as it is used by medical professionals is that the staff member obtaining informed consent should have familiarity with the procedure being consented for.[13]

Given that the healthcare sector is renowned for lack of technical knowledge[14] and is the most commonly reported source of notifiable data breaches[15], it is unlikely that most doctors will have a sufficient understanding of the cybersecurity implications of myHealthRecord to be able to provide a true assessment of the risks to privacy of the system. Medical attitudes to confidentiality are grounded in the mentality of paper charts in locked filing cabinets, and have not adjusted well to the random-access capability of digital health records.

Ethical issues relating to "de-identified" data

Secondary use of myHealthRecord data has the potential for significant benefits to the health system - through better understanding of disease epidemiology, health service planning and the potential for new discoveries through data linkage analysis.

[11] https://amp.slate.com/technology/2018/08/how-australias-my-health-record-program-became-opt-out-violating-citizens-privacy.html
[12] https://www.healthcareit.com.au/article/racgp-claims-gaining-patient-consent-my-health-record-uploads-not-job-doctors-and-calls
[13] https://www.bma.org.uk/advice/employment/ethics/consent/seeking-consent
[14] https://blog.malwarebytes.com/101/2018/02/physician-protect-thyself-healthcare-cybersecurity-circling-the-drain/
[15] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/quarterly-statistics-report-january-2018-march-2018

Although it is impossible to predict the potential benefits, advances in machine learning technology mean that it is likely there will be future benefits to health.

This lack of concrete benefits is therefore more difficult to balance against the risks in order to provide a process of truly informed consent.

Advocates for secondary use of myHealthRecord data claim that secondary use of this data can be done "without risk to privacy".[16] However, it is widely agreed by information security professionals that data breaches require a "when, not if" risk analysis.[17,18] The computer security research group from the University of Melbourne who were responsible for re-identifying the MBS/PBS dataset released to data.gov.au note in their paper[19]

> "A significant proportion of the [Privacy Preserving Record Linkage] literature has been published outside of Computer Science and Information Security venues, with a particular prevalence for publication within the medical domain. This has resulted in proposals not being subjected to the normal level of rigour and analysis associated with information security".

This research group demonstrated that through the combination of publicly available data (for example social media posts, stories in the mainstream media) with a linked data set, that re-identification of individual records was not only possible, but trivial. It is important to emphasise that this is not abstract computer security research - indeed it is the very foundational principle of data linkage - that combining different datasets leads to new insights.

In contrast to the positions of some of the other digital and privacy rights organisations, Future Wise is not opposed to the use of linked data research for public health. However, we very strongly believe that the risks should not be downplayed. Linked data should be considered potentially re-identifiable, which very firmly places secondary use research under the remit of the Declaration of Helsinki, and therefore a similar comprehensive process of seeking informed consent is required.

[16] https://www.crikey.com.au/2016/08/08/comments-census-data/
[17] https://www.housingwire.com/articles/43427-cybersecurity-experts-data-breaches-are-a-matter-of-when-not-if
[18] https://www.baesystems.com/en/cybersecurity/cyber-security-breaches-its-not-if-but-when
[19] Culnane C, Rubinstein BIP & Teague V. arXiv cs.CR, https://arxiv.org/abs/1802.07975

How this is achieved in practice is a challenge that needs to be addressed - as discussed previously, general practitioners are neither willing[12] nor capable of obtaining meaningful informed consent from research participants.

This does not mean that secondary use research should be scrapped; but equally the very real privacy risks must not be swept under the carpet in the interests of big data evangelism.

c) the privacy and security, including concerns regarding:

i) the vulnerability of the system to unauthorised access

It is important to remember that the primary stated benefit of myHealthRecord is of increasing ease of access to summary patient information. It therefore follows that the risk of inappropriate access is also increased as a necessary consequence of ease of proper access; no security system is 100% reliable.

Future Wise has advocated strongly in its media work on myHealthRecord to try to correct misinformation about the risks of unauthorised access to myHealthRecord. Meaningless security marketing terms such as "bank-grade" security and "never been hacked" serve only to divert attention from the far greater risk to privacy, which is of improper access to records by authorised users.

The false dichotomy between "hacking" and "unauthorised access" was also evident during the 2017 availability of patient's Medicare numbers on the internet.[20] The security issues were reported as "traditional criminal activity" as opposed to the system being "hacked", to create false reassurance as to the security of the system. The distinction is meaningless to those whose personal data was compromised.

In 2018 there has been well-publicised disciplinary action against healthcare workers in South Australia[21] and Western Australia for inappropriately accessing individual records to which they had no clinical need to access, highlighting the importance of

[20] https://www.theguardian.com/australia-news/2017/jul/04/federal-police-asked-to-investigate-darkweb-sale-of-medicare-data
[21] https://www.adelaidenow.com.au/news/south-australia/more-sa-health-staff-sacked-and-disciplined-for-spying-on-patient-records/news-story/e20475ef3b7a9451252e140f78310049

the "insider threat" to privacy..[22] Outside of the health sector, similar authorised-but-improper access of police databases has been widely reported.[23]

Privacy of medical confidentiality is a one-way door; penalties and sanctions may serve as deterrents, or as compensation for the loss of privacy, but neither give individuals their privacy back if it is breached. It is particularly true in this area - as in much of medicine - that prevention is better than cure. Medical information is of commercial interest to insurance and pharmacetical companies, as well as its potential use in identity theft.

Regardless of the sort of improper use, Australians are concerned about the privacy of their confidential health information, and more robust systems to protect it are needed.

Risk to privacy from "Hacking"

There are a number of different risks to the security of myHealthRecord data; these can be summarised as:

- extenal, unauthorised access - typically framed in the media as "hacking"
- internal, unauthorised access - the use of valid credentials to view records to which access ought not be allowed; eg: other staff in the practice accessing records via a logged in computer, or healthcare worker reviewing the data of an individual who is not their patient
- misuse of authorised access - for example a healthcare worker access the record of someone who is their patient, but for improper reasons (eg: stalking)

While highlighting the far greater risk of insider threat, Future Wise does not wish to minimise the risk of external, unauthorised access - what has been framed in the media as "hacking". The widespread impact in the healthcare sector of the WannaCry ransomware[24] highlights the risk to healthcare IT systems. Given that doctors' computers will be a primary portal of entry to myHealthRecord, and lack of clarity

[22] https://www.perthnow.com.au/news/public-health/snooping-perth-hospital-staff-caught-in-40-patient-privacy-breaches-ng-b88945573z
[23] https://www.theguardian.com/australia-news/2018/aug/02/queensland-police-computer-hacking-no-action-taken-in-nearly-90-of-cases
[24] https://www.healthcareit.com.au/opinion/one-year-wannacry-and-healthcare-organisations-are-prime-targets-cyber-attackers

about whether practice management software will keep local copies of myHR data, the importance of an industry-wide focus on digital security cannot be underestimated. This is particularly critical given the exclusions in s71 of the *My Health Records Act*, which state that if the data are collected for another purpose (ie: for the formation of the primary medical record), then the safeguards and penalties associated with the myHealthRecord act may not apply.

ii) the arrangements for third party access by law enforcement, government agencies, researchers and commercial interests, and

The arrangements proposed under s70 of the my Health Record Act allowing warrantless access to myHR data for administrative or investigative purposes is inimical to the ethical obligation of doctor-patient confidentiality.

This appears to be a widely-held misconception among doctors and also the public that the access principles for myHealthRecord are similar to the existing principles for traditional medical records. This is not the case. Medical records are the property of the healthcare worker who prepares them (or the hospital or other healthcare facility in which they work), and the record owner is involved if there is a request for access.

Given the model of myHealthRecord as a shared summary, the point of contact for release of information becomes the system operator: ADHA. This means that record creators are cut "out of the loop" on access requests to patient data.

In addition, the clauses relating to access to myHealthRecord are unreasonably broad, allowing access for "law enforcement purposes" rather than for the investigation of serious crimes. Future Wise believed this threshold was too low, and actively campaigned for the provisions of section 70 to be amended. We were particularly concerned at the possibility that information could be released as was done with the Centrelink information of blogger Andi Fox for the purpose of "correcting the public record" by the Social Services Minister.[25]

The *My Health Records Amendment (Strengthening Privacy) Bill 2018*[26] goes some way to correcting these issues - inserting the requirement for a warrant to be obtained. However, the included list of "designated entities" who can apply for a

[25] http://www.abc.net.au/news/2017-02-27/dhs-warns-to-disclose-centrelink-recipients-history/8307958
[26] http://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6169_first-reps/toc_pdf/18173b01.pdf;fileType=application%2Fpdf

warrant remains very broad, and Future Wise would favour further restriction of this access.

In addition, there is no requirement that the primary record creator (doctors or other healthcare workers) be notified when this administrative access has occurred, removing the protections provided to patient confidentiality by their healthcare workers having an active role in the disclosure of confidential information when required by law. Future Wise believes that the amendment bill should also include provisions whereby the creator of the myHealthRecord entry is notified prior to the release of information.

The potential privacy implications of data in myHR which is considered to be "less privacy intrusive" must also be considered. For example, PBS dispensing data not only sometimes allows the identification of a specific medical condition in a person's medical history, it may also provide privacy-intrusive data in aggregate. For example, most PBS medicines in Australia are dispensed a month at a time. It is therefore possible to use dispensing information to determine a person's likely location as within a given radius of a particular pharmacy. Regulations regarding the minimum distance between pharmacies helps with making quite accurate estimates for an individual's likely location at a given time.

iii) arrangements to exclude third party access arrangements to include any other party, including health or life insurers;

Future Wise supports the exclusion of access to myHR data by health and life insurers, and believes this should not only be maintained, but broadened to include pharmaceutical companies and other commercial entities. The combination of myHR secondary use data with other publicly available data may allow insurance companies to build rich profiles on their customers, further putting their privacy at risk.

d) the government's administration of the My Health Record system roll-out, including:

i) the public information campaign

The public information relating to myHealthRecord has been particularly one-sided, with active dismissal of the risks raised by privacy advocates and doctors. In addition,

the Digital Health Agency has responded poorly to public concerns; the @AUDigitalHealth twitter account during the first week of the opt-out campaign continued to broadcast boilerplate replies to anybody expressing concerns about the program.

While Future Wise welcomes the introduction of the *My Health Records Amendment (Strengthening Privacy) Bill* 2018,[26] we note that up until the day before the privacy amendments were announced, both the Agency and the Minister continued to insist in the media that the concerns of privacy advocates were invalid. Future Wise also reiterates our concerns about the technical knowledge of medical practitioners, and encourages the Government and ADHA to engage with privacy and technology advocates and not just the medical profession in this area.

Additionally, Future Wise has lodged a Freedom of Information request to assess the veracity of the claims about the Agencies internal policy; as of the time of preparing this submission, there has been no response to the request.[27]

We further note the significant concerns of the technology community regarding exactly how difficult the deletion of records from complex databases may actually be.[28]

ii) the prevalence of "informed consent" amongst users;

Future Wise is aware of reports[29] in the media about users attempting to opt-out of mHR, only to discover they already have one.[30] In many cases, these records will presumably have been created during the opt-in period, but without appropriate informed consent. As highlighted above, we believe that the potential privacy risks associated with myHR justify a comprehensive informed consent process, and given the move to opt-out, this now seems even less likely to occur than before.

Of particular concern to Future Wise is the socioeconomic inequity factors associated with access to digital health. Individuals from disadvantaged, or from non-English-speaking backgrounds, are less likely to access digital health tools[31] and less likely to

[27] https://www.righttoknow.org.au/request/procedure_for_release_of_myhealt#comment-2190
[28] https://theconversation.com/my-health-record-deleting-personal-information-from-databases-is-harder-than-it-sounds-100962
[29] https://slate.com/technology/2018/08/how-australias-my-health-record-program-became-opt-out-violating-citizens-privacy.html
[30] http://www.abc.net.au/news/science/2018-07-18/my-health-record-opt-out-confusion/10000008
[31] https://eprints.utas.edu.au/22551/1/whole-Showell-thesis-2014.pdf

have the privacy awareness or digital literacy to be able to opt out. ICombined with one-sided evangelism from ADHA, and endorsement by their doctor (who may not fully understand the risks), then these individuals are much less likely to opt-out.

This presents a "double threat" to these patients, who are more likely to have greater levels of health needs, combined with poorer access to healthcare. In their PhD thesis, Dr Showell notes that while ADHA consulted extensively with medical and technical stakeholders, there was a distinct lack of engagement with patients or the community.[31]

e) measures that are necessary to address community privacy concerns in the my Health Record system;

Future Wise believes that the opt-out model of myHealthRecord is deeply flawed for the reasons we have outlined above and that it should be ceased, pending a review of the program and measures put in place to address concerns with the system.

A comprehensive education campaign targeting healthcare professionals on digital security and the risks of myHealthRecord should be a high priority, to improve the skills of healthcare providers in seeking informed consent to enrol patients in both the myHealthRecord system generally and in the secondary use components specifically. Improving general community education on digital literacy would also be of benefit not only relating to myHealthRecord, but also to modern life more broadly.

Engagement with digital civil society organisations— have been actively campaigning on myHealthRecord—is essential, rather than only with medical bodies and patient organisations.

f) how my Health Record compares to alternative systems of digitising health records internationally

Future Wise does not have experience with digital record systems in other countries. However, we note again the important difference that myHealthRecord is a shared document store, rather than a truly universally-accessible health record, as it is commonly perceived to be.

We further note the parallels with the UK's care.data[32] program, which seems particularly relevant as the head of ADHA was heavily involved with this program in the UK. The care.data program was ceased following the UK Caldicott Review.[33]

g) any other matters

Even prior to the introduction of the European *General Data Protection Regulation* (GDPR), the UK had significantly greater protections on the privacy of health data than apply in Australia, even under the *Privacy Act*.

Future Wise believes that a similar data-protection regime would benefit Australians, and that a tort of privacy or a Bill of Rights would serve to further protect the privacy of Australian citizens.

Conclusions

The move to digital health is inevitable. However, a poorly implemented program which results in a major data breach of citizens' confidential medical information will do irreparable damage to trust in the Government's ability to manage digital projects - which is already at low ebb in light of issues with the 2016 online census and automated Centrelink debt recovery. The Senate is well aware of these issues, having already conducted an inquiry into the digital delivery of Government services.[34]

Although the myHR program to date has been a large expense, the program should be reviewed; many of the putative benefits to patients of myHR could be resolved with other elements of the Digital Health strategy - for example secure online medical communication systems. Pursuing the program out of a sunk-cost fallacy or desire to save face poses what we believe to be an unacceptable risk to patient privacy for relatively few benefits, which cannot be said to outweigh the very substantial risks.

Engagement with the community, and with digital civil society is essential to ensure not only that the benefits outweigh the risks, but that this can be communicated in an effective way to the public.

[32] https://en.wikipedia.org/wiki/Care.data
[33] https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs
[34] https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/digitaldelivery/Report