

Submission to the Finance and Public Administration
Reference Committee



Inquiry on the circumstances in which Australians'
personal information has been compromised

Introduction

Thank you for the invitation to make a submission to the inquiry on the circumstances in which Australian's personal information has been compromised and made available for sale illegally on the 'dark web'. Dr Trent Yarwood received the invitation via email on 21st August 2017, and has contributed to this joint submission.

We note the short time frame available for submissions and trust that submissions received will be given due consideration, given the importance of protection of health information.

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 which improve the long-term direction of Australia, particularly in the areas of technology and health. More information about Future Wise is available on our [website](https://futurewise.org.au/).¹ We are happy to provide further clarification of any of the points in the submission, or for one of the authors to attend the hearing in person if required.

Dr Yarwood is currently contracted as a medical advisor to the Australian Commission on Safety and Quality in Healthcare's AURA surveillance system. He does not work with the Commission's e-Health team. His contribution to this submission is in his personal capacity as a member of Future Wise and as an independent medical specialist, and should not be considered to reflect the position of the Commission or the Commonwealth Public Service.

Summary of Submission

Future Wise notes the high importance Australians place on the privacy of their healthcare data. While this data breach posed little risk of sensitive health information being available, it still posed a significant risk to patient privacy. The greatest part of this risk comes from the possibility of linking the Medicare number to other information. As the Medicare number / card is considered a

¹ <https://futurewise.org.au/>

secondary form of identification in Australia, the availability of these numbers increases the risk of identity fraud.

The secondary risk comes from the potential for publicly available Medicare numbers to be linked to other publicly available datasets. While this would also facilitate identity fraud, there is a separate and additive risk to individuals' privacy. In general, the Australian public has little awareness of the risks of "big data linkage" and its use in building comprehensive identity profiles of individuals. These linked datasets - currently most commonly used for marketing - are themselves a high value target for cyber crime, but also for misuse by corporate entities.

The Australian Government does not have a good record in terms of IT project management, and there have been a large number of data breaches over the past 18 months. The government's response to these breaches has been piecemeal, and does not demonstrate a good understanding of principles of data protection.

Future Wise calls on the Government to adopt a "privacy first" policy on data management, whereby the minimum necessary data are collected; where data security is given priority and to a more needs based access control system, rather than solely relying on the deterrent effect of penalties for inappropriate data access.

This Medicare number breach highlights many issues which privacy advocates have expressed concern about in discussing the implementation of the myHealthRecord.

Future Wise supports electronic health, but believes that myHealthRecord should not be made opt-out until many of the issues highlighted in this submission are addressed.

Terms of Reference

Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web', including:

- a. any failures in security and data protection which allowed this breach to occur;
- b. any systemic security concerns with the Department of Human Services' (DHS) Health Professional Online Services (HPOS) system;
- c. the implications of this breach for the roll out of the opt-out My Health Record system;
- d. Australian government data protection practices as compared to international best practice;
- e. the response to this incident from government – both ministerial and departmental;
- f. the practices, procedures, and systems involved in collection, use, disclosure, storage, destruction, and de-identification of personal Medicare information;
- g. the practices, procedures, and systems used for protecting personal Medicare information from misuse, interference, and loss from unauthorised access, modification, or disclosure; and
- h. any related matters.

Response to discussion points

a. any failures in security and data protection which allowed this breach to occur;

"Australians are more conscious of personal data issues than ever before", [noted](#)² Australia's Privacy Commissioner during Privacy Awareness Week in May. The theme for this year's Privacy Awareness Week was "trust and transparency" which speaks to the importance of organisations handling personal information with care.

The government was not transparent about the failures which allowed this breach to occur. Information surrounding the details of this data breach have not been made available to the public. [Statements](#)³ made to the media by the Human Services Minister, The Hon Alan Tudge MP suggest that the breach occurred by a user with access to the Medicare records data, who accessed the information inappropriately.

This sort of "insider threat" breach is very difficult to prevent, given that legitimate users of the system require access in order to be able to use it for its intended purpose. Increasing the level of security on access to this data will make legitimate access for the bulk of HPOS / PRODA users more difficult and potentially result in inefficiencies in healthcare delivery.

Future Wise highlights that a sanctions-based penalty for inappropriate access to the personal information of Australian citizens works as a deterrent only and does not increase security *per se*. This means that a privacy breach has already occurred, and the affected individuals are not able to "regain" their privacy (for example by obtaining a new Medicare number as would be done with a credit card, for example).

² <https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-awareness-week-launched-for-2017>

³ <http://www.abc.net.au/news/2017-07-04/tudge-calls-for-afp-to-investigate-medicare-card-numbers-dark-w/8676678>

"Privacy first" system design would create a system whereby the minimum necessary set of data was collected, stored in a secure way for the minimum possible time, with access granted to only those with a legitimate need to access it. Healthcare is an increasingly complex system, and works more and more using a multidisciplinary team model. This complexity means that there may well need to be some compromised made in order for the data to have utility to healthcare workers. At present, Future Wise believes that the balance is too far in the direction of ease of use. It is, however more likely that data security was not considered in as much depth as it needed to be at the time of designing the system, rather than a conscious choice of utility over security.

The Department is required under the privacy act to take "reasonable steps" to keep personal information secure, including from unauthorised access or use, and Future Wise believes that this bar has not yet been reached.

b. any systemic security concerns with the Department of Human Services' (DHS) Health Professional Online Services (HPOS) system;

The HPOS system has, until recently, been primarily been protected by a public-key infrastructure (PKI)-based system. This system involved providers having a certificate, which was stored on a removable memory stick, and needed to be plugged into the computer on which HPOS was being accessed (aka a "dongle"). Although this fulfils the criteria for 2-factor authentication (2FA), in practice it does not represent robust security.

Many healthcare providers leave the dongle plugged into an admin computer (on which the bulk of Medicare work is done). If the dongle is never removed from the computer, then it would be possible for an unauthorised user to gain access to the HPOS system using this computer. In essence, the benefits of 2FA is neutralised by being left in-situ at all times. If the computer in question was to have saved passwords (or a sticky note with passwords written down), then the system would be immediately vulnerable to unauthorised access.

As mentioned in the response to the previous point, these security measures only restrict unauthorised access to the HPOS. Improper use by users who do have a valid reason for accessing the system is not prevented. Future Wise notes that, at present, HPOS has a mandatory check-box whereby users affirm they are accessing the data only for billing purposes, but how this is verified or audited is not known.

The new system for authorising access to HPOS is the Provider Digital Access (PRODA) system. Problems identified with PRODA by Future Wise include:

- 1) Registration is via three forms of identification, verified online. There is no protection against identity theft; the combination of a compromised email address and a stolen wallet, combined with publicly accessible information from the web would be sufficient to register for an account with identity verification. Status as a healthcare worker is verified by comparing the biographic details entered with the provider's registration number with the Australian Health Professionals Regulation Authority registration number. This number is available to public search via APHRA's website, and requires only the name and professional stream of a healthcare worker to find.
- 2) The site uses 2-Factor authentication. The 2nd factor can be delivered by a specific PRODA mobile phone app, available for iPhone and Android. When Dr Yarwood tested this in August 2017, the Android version of the app was not able to be used to link to his account due to poor design of the App. Of the twelve reviews on the [Android App store](https://play.google.com/store/apps/details?id=au.gov.humanservices.authenticator.release#details-reviews),⁴ 7 are 1- or 2-star, and there is only a single positive comment. There is no option for delivery of the second-factor by OTP/TOTP or any other widely accepted internet standard for 2FA. In addition to being a widely accepted and trusted standard, this would remove the need for a custom app to be

⁴ <https://play.google.com/store/apps/details?id=au.gov.humanservices.authenticator.release#details-reviews>

developed and maintained by the Department so that users can log on. The other options currently available for delivering the second factor are either by email or SMS, neither of which are secure methods of delivery.

c. the implications of this breach for the roll out of the opt-out My Health Record system;

This breach of Medicare data highlights the ease with which personally sensitive data can be accessed. Given that Australians place a high value on the privacy and security of their [healthcare information](#),⁵ this should raise major concerns. Significant work will need to be done by the Digital Health Agency to restore necessary trust in the system. Australians will avoid dealing with organisations due to privacy concerns, as [shown](#)⁶ in the OAIC's recent survey on Australian Community Attitudes to Privacy. The number of people that have opted out from the trial of myHealthRecord has not been publicised, but a number of privacy groups have been running campaigns encouraging Australians to opt-out.

The 2015 [Privacy Assessment](#)⁷ on myHealthRecord (then known as the personally-controlled electronic health record - PCEHR) recommended that multiple pieces of personal information be required to access the myHealthRecord - full name, date of birth, gender and Medicare Number. The addition of the Medicare Number to the more traditional demographic details was intended to reduce the ability of healthcare workers to access the records not relevant to their work.

Much like the leaving of the dongle in the PC, having an easy method for bypassing a security measure means that it is not a "reasonable step" in the circumstances to protect the sensitive information. Having Medicare numbers

⁵ <https://www.digitalhealth.gov.au/australias-national-digital-health-strategy>

⁶ <https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017>

⁷

<https://web.archive.org/web/20160302060248/https://myhealthrecord.gov.au/internet/ehealth/publishing.nsf/Content/ehealth-program-info-privacy>

made publicly available therefore removes this additional barrier to access to patient records.

Future Wise is supportive of the concept of electronic health. Unfortunately, the current form of myHealthRecord is not particularly clinically useful to healthcare workers, and does not meaningfully address the concerns of privacy advocates. It is truly a compromise which pleases none of the stakeholders.

This recent data breach is an example of what is unequivocally the greatest risk to the privacy of myHealthRecord holders - which is not "hackers" or "cybercriminals" but improper access by authorised users - and does little to ease the concerns of privacy advocates. HPOS has similar access controls and logging to the myHealthRecord system, and this did not prevent a user from retrieving and selling Medicare numbers on the Web on demand.

The following is a quote from the myHealthRecord website's [privacy and security section](#)⁸

The My Health Record system has bank-strength security features. These include strong encryption, firewalls, secure login/authentication mechanisms and audit logging. To date, there have been no identified instances of malicious attacks.

This is obfuscatory language at best and misleading at worst. At the time it was reported in 2015, the largest ever reported data breach involved [bank data](#),⁹ so bank-strength security is not proof against data breaches. Encryption of data protects against external access, but not internal access, and is susceptible to social engineering attacks. It is worth noting that the Federal Government also believes that encryption should not necessarily have priority over national security

8

<https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/privacy?OpenDocument&cat=Privacy%20and%20Security>

⁹ <http://mashable.com/2015/11/10/bank-data-breach-100-million/#bcEDwJYJIEqY>

concerns. Secure login, authentication and audit logging exist, but did not prevent this current data breach, and “closing the hole” after a large-scale data breach occurs is not a solution for privacy.

d. Australian government data protection practices as compared to international best practice;

The Australian Government’s data protection practices cannot in any reasonable sense be considered best practice.

Major Australian Government IT projects have been beset with technical and planning failures and subject to widespread criticism in the mainstream media, in technical circles and by the general public. In the last 18 months, in addition to this breach, there has been the [reidentification](#)¹⁰ of provider numbers from the Data.gov.au Medicare dataset; the [leaking](#)¹¹ of parliamentarians’ phone numbers, the [deliberate](#) release¹² of personal information of blogger Andie Fox in response to her articles about the Centrelink automated debt recovery, and the public service census [data breach](#)¹³ potentially leaking the personal details of 96,000 public servants.

These examples are specifically related to data protection, and have occurred at the same time as a large number of non-security-related IT issues - the [electronic census](#)¹⁴ website outage now popularly known as “#Censusfail” and [multiple outages](#)¹⁵ of the Australian Tax Office’s website.

¹⁰ <https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy>

¹¹ <http://www.abc.net.au/news/2017-03-20/phone-numbers-of-federal-mps-former-prime-ministers-published/8370418>

¹² <http://www.canberratimes.com.au/comment/time-for-the-truth-behind-centrelink-controversy-and-andie-fox-20170303-gupt6o.html>

¹³ <http://www.canberratimes.com.au/national/public-service/96000-public-servants-in-new-data-breach-20161004-grul2p.html>

¹⁴ <https://www.cnet.com/au/news/macgibbon-report-senate-2016-census-fail-fallout-privacy-security/>

¹⁵ <http://www.news.com.au/national/australian-tax-office-website-suffers-another-outage-after-string-of-crashes-in-last-six-months/news-story/14a3db04a04d0dea2eafc7e66d4404d8>

In light of the government's commitment to "[digital transformation](#)"¹⁶ and the significant [expenditure](#)¹⁷ on Federal Government IT services, such a laundry list of issues in little over a year represents something very far from international best practice.

Future Wise notes that the Digital Health Strategy includes the creation of a specific Digital Health Cyber Security Centre. This is in addition to the [Australian Cyber Security Centre](#)¹⁸ and the [Joint Cyber Security Centre](#)¹⁹ program. While we absolutely support the importance of security of digital health (and cybersecurity generally), it would seem very likely that a specific digital health cyber security centre will introduce significant duplication and overlap of functions, which could most likely be dealt with by a team or unit within the ACSC or one of the JCSCs.

e. the response to this incident from government – both ministerial and departmental;

Understandably, the Minister for Human Services sought to reassure the public about the risks associated with this data breach. However, as discussed above, the differentiation between "cybercriminals" and "traditional criminal activity" does not have any practical meaning other than diverting attention away from a straw-bogey-man which the government itself has created through relentless focus on cybercrime. The Minister particularly downplayed the privacy risks to individuals, focusing the fact that myHealthRecord data could not be accessed with a medicare number alone.

As discussed above, the Medicare number was supposed to be an additional point of identification to prevent the unauthorised access by registered healthcare workers, so while technically correct that the medicare number of itself does not allow access to myHR, it forms a part of the puzzle.

¹⁶ <https://www.dta.gov.au/>

¹⁷ [http://www.abc.net.au/news/2017-08-28/federal-governments-\\$10bn-bill-rivals-newstart-cost/8849562](http://www.abc.net.au/news/2017-08-28/federal-governments-$10bn-bill-rivals-newstart-cost/8849562)

¹⁸ <https://www.acsc.gov.au/>

¹⁹ <https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx>

Following on from this, given the Medicare number is an accepted secondary identity document, access to an individual's Medicare number may facilitate the acquisition of a false identity. This poses a much greater risk to the privacy of individuals than access to their myHealthRecord (which statistically, is most likely devoid of any information at all given the very low rate of uptake by the public).

f. the practices, procedures, and systems involved in collection, use, disclosure, storage, destruction, and de-identification of personal Medicare information;

The potential for misuse of medical data is significant, and under-recognised. For example, a list of healthcare providers who have seen an individual could be combined with freely available information on the internet to piece together parts of a patient's medical history. For example, if a person has on record a consultation with a doctor who works in a sexual health clinic, or drug dependency clinic, or practices as a psychiatrist, then it is not only the content of the consultation that is sensitive, but the fact that the consultation has occurred at all.

The framework for dealing with Medicare information does not deal well with these issues, and instead maintains an attitude that it is the "content, not the metadata" which is the privacy sensitive part of the information. Future Wise rejects this assertion utterly, and refers you to our [submission²⁰](#) on the *Telecommunications (Interception and Access) Amendment Bill (Data Retention) 2014* for a more complete discussion of why metadata is highly privacy intrusive.

Future Wise believes that all Medicare information should be considered sensitive personal information under the *Privacy Act*, and that requirements be put in place for it to be stored securely and securely deleted when no longer required.

²⁰ <http://www.aph.gov.au/DocumentStore.ashx?id=74c65dcc-63b7-4a32-a977-249e503f8e2b&subId=302783>

There are definitely benefits to the use of appropriately deidentified Medicare data - in health service planning, and well as in as-yet unrealised benefits from the application of Big Data to the dataset. However, the reidentification of provider numbers from the MBS/PBS strongly highlight the need for this to be done in a way that does not allow reidentification. The introduction of laws criminalising the reidentification of a deidentified dataset again do not *protect* privacy, but only sanction persons who breach it. Future Wise believes that a privacy first approach which takes greater steps to reduce the risk of these breaches occurring is much preferred to increasing penalties for non-compliance.

Greater transparency in the ways in which the data are collected, handled and used would give much greater confidence to Australians that the government is taking appropriate steps in safely handling their sensitive health information.

g. the practices, procedures, and systems used for protecting personal Medicare information from misuse, interference, and loss from unauthorised access, modification, or disclosure; and

As mentioned above, Future Wise believes that increased transparency in these data handling procedures are required. Australia's open data repositories (for example data.gov.au) are an excellent resource, but clear statements and publicly accessible policies and procedures on data management, which have truly been written with best practice data management techniques are required.

Future Wise does not believe that patient controlled access restrictions to electronic health data are practical or feasible; modern healthcare is multidisciplinary and team-based, and requiring patients to grant access to individual healthcare workers would reduce utility and safety of the health record and place a much greater onus of data management on to the individual who controls the record.

A “hub and spoke” model of permissions could be feasible, whereby a primary healthcare worker (identified by AHPRA registration etc) is then given the ability to grant secondary access to a number of staff (for example, clinic administration staff). This access is recorded as belonging to the delegated staff member, but access is linked back to the primary healthcare worker. Responsibility for inappropriate access could then be channelled through the primary healthcare provider. Future Wise believes, however, that there would need to be a major education initiative to users of HPOS so that they understand the privacy implications and would be aware of the risks to patient privacy and confidentiality posed by granting secondary access to their staff.

h. any related matters.

The Australian Government should clarify its position on encryption, reaffirming that robust encryption is a key component of digital commerce, digital health and modern society, and that the privacy and security of patients’ health data must take priority over all other considerations, including those of national security.

Conclusion

Future Wise thanks the committee for promptly calling this inquiry, into what was unequivocally a serious breach of confidentiality. We call upon the Government to consider not only the implications of this breach, but the potential for this information to be combined with other personal or health information which is either already available on the Internet, or has been made available as part of another data breach; or which one day in the future may be made available.

The power of data is in its aggregation. Each individual point of data must therefore be protected to the highest level of security possible, to ensure it does not become the “final piece in the puzzle” and allow more serious breaches of confidentiality, or other more serious crimes.

Future Wise believes that a more privacy-centred approach to data management is urgently needed by the Government.

Thank you for the opportunity to make this submission. Please contact info@futurewise.org.au if you require additional supporting information, or would like one of our members to attend an in-person hearing to discuss our submission further.

