Submission to the Senate Community Affairs References Committee's Inquiry into My Health Record System 2018

About the Health Workers Union-Victoria

The Health Workers Union has a proud history since its inception in 1911 of fighting for workers' rights and better work conditions in Victoria's hospitals and other healthcare facilities. We are a strong and growing union that aims to use its combined power to improve working conditions and to maintain reasonable wages and benefits for our members. The Health Workers Union (HWU) of Victoria represents a broad spectrum of workers employed in hospitals, pathology, dental, aboriginal, disability and aged care services.

For further information please contact:

Kamal Bekhazi
Senior Research & Project Officer

Health Workers Union
Level 5/222 Kings Way
South Melbourne 3205
Telephone: 03 93413300
Email: Kamal.Bekhazi@hwu.org.au

Contents

Preamble..3

Introduction..4

The HWU Response to the Inquiry Terms of Reference

Terms of reference A: The expected benefits of the My Health Record system..5

Terms of Reference B: The decision to shift from opt-in to opt-out........................8

Terms of reference C: Privacy and security, including concerns regarding........10

i. the vulnerability of the system to unauthorised access........................10
ii. the arrangements for third party access by law enforcement, government agencies, researchers and commercial interests........................11
iii. arrangements to exclude third party access arrangements to include any other party, including health or life insurers........................14

Terms of Reference D: The Government's administration of the My Health Record system roll-out, including:

i. the public information campaign..17

Terms of Reference E: Measures that are necessary to address community privacy concerns in the My Health Record system..18

Terms of Reference F: How My Health Record compares to alternative systems of digitising health records internationally..19

References:..22

Preamble:

The Health Workers Union (HWU) welcomes the opportunity to contribute to this inquiry by providing feedback to the Senate Community Affairs Legislation references committee inquiry into My Health Record system 2018. We are disappointed that the Coalition government has not consulted widely with the community and other stakeholders during the long and expensive process that has produced what the government refers to as My Health Record system. We urge the senate to reject the Bill in its current form!

Our submission has been informed by a review and examination of the My Health Record system. We examined alternative existing medical records data system across the world, especially in OECD and European countries. We also sought feedback via substantial consultations with HWU employees and members.

In order to ensure that this submission represented the diversity of the HWU membership, workers' from a broad range of occupational backgrounds that work within metropolitan, rural and remote areas of Victoria's health system were invited to provide verbal or written feedback to the HWU. We have included their feedback in our submission. These individuals are representative of tens of thousands of other health workers statewide and we thank them for taking the time to share their stories.

Introduction:

Australia needs a better healthcare record system for better managing and keeping track of each individual's health data. The HWU acknowledges the government's attempt to improve the current health records system. We have come a long way from the previous paper trail, hand written file notes, photocopying and facsimiles. Our current medical records system has been replaced by digital files that are able to be quickly and easily accessed by medical professionals.

In many instances these changes have resulted in better health outcomes for patients and a more efficient and productive health system. This is evidenced by enhanced management of chronic conditions and diseases, timely and more accurate communication with patients and between medical professionals.

However, the current My Health Record system 2018 that the government has recently introduced to the public is inadequate and fraught with problems and risks!

The HWU Response to the Inquiry Terms of Reference

a. the expected benefits of the My Health Record system

My Health Record has the potential to improve health outcomes for most people. In particular, minority groups that have found it difficult to engage with health services and navigate their way through our fragmented and complicated health system would benefit the most.

For example, the following groups would benefit the most from the introduction of the My Health Record System:

- **Aboriginal and Torres Strait Islander people according to leading health practitioners who work with Indigenous communities**

Over 75 per cent of Indigenous Australians reside in urban and regional locations (Australian Bureau of Statistics, 2015a, 2015b). The Australian Institute of Health and Welfare (2013) reported that Australia's Indigenous community do not fully utilise existing primary healthcare services, including aged care services Australian Bureau of Statistics (2013).

Many are forced to travel long distances to receive health care. Moreover, many ATSI health service providers report that they find it difficult to keep track of their client's medical conditions because a significant proportion of their patients live a transient life.

For example, if a patient that has travelled from their home in Southern Western Australia to Northern Western Australia to visit family attends a medical center, the treating doctor finds it difficult to not access their medical records or their previous medical practitioner. My Health Record would allow the doctor to access the patients' health information important quickly.

- **People in rural and regional Australia**

Over the last decade or so it has become increasingly obvious that rural and remote Australia's cultural complexity and dispersed settlement pattern requires a dedicated policy and service delivery response (National Commission of Audit, 2014a,b; National Strategic Framework for Rural and Remote Health, 2012).

Moreover people living in rural and remote regions of Australians have higher exposure to health risks and injury, experience higher levels of disease and have less access to and use of health services compared to people in metropolitan areas.

Issues such as redressing the geographic inequitable distribution of healthcare professionals, poor workforce retention and service coordination, increased health risks to injury, higher levels of chronic illness can be addressed in part by the My Health Record system.

- **People from Culturally and Linguistic Diverse Backgrounds**

Australia's most recent Census in 2016 (Australian Bureau of Statistics, 2018) revealed that Victoria is the most Culturally and Linguistically Diverse (CALD) state in Australia, comprising of people that have immigrated from over 200 countries and that speak more than 400 languages and follow more than 120 religions. Although Victoria's culturally rich background is an asset to the state, it also presents many challenges, especially in regard to the provision of health services.

For many people from culturally and linguistically diverse backgrounds, accessing health care can be problematic (Henderson & Kendall, 2011). The average Australian can struggle to navigate the health system and to access relevant information about health services. This can be especially true for frail elderly people from non-English speaking backgrounds as well as socially

isolated people. To further complicate matters, very few bi-lingual health workers exist and many health workers struggle with cross cultural issues and the delivery of culturally sensitive services (Henderson & Kendall, 2011).

My Health Record would allow doctors to overcome the language barrier, providing them with the patients' health information quickly. Moreover, My Health Record in combination with existing digital health technology that facilitates access to interpreters can improve the health outcomes for people from CALD backgrounds. In particular, medical mishaps that can occur due to communication breakdowns can be significantly reduced.

The Chairperson of the Federation of Ethnic Communities' Councils of Australia (FECCA) agrees with the above assessment and supports the implementation of My Health Record. She added that My Health Record has the potential to reduce hospital admissions and duplication of tests, improved coordinated care, and better informed treatment decisions.

Other benefits associated with My Health Record 2018

- My Health Record has the potential to reduce medication related errors that result in the hospitalisation of more than 230,000 people each year.

For example, My Health Record can reduce serious illness attributed to the following factors:

1. unknown allergies,
2. drug interactions,
3. confusion associated with the various brands of a particular medication.

- Continuity of care,
- Prompt access in emergency situations,
- Government administered,

- Contribute to improved policy development,
- Capacity to be improved as digital health technology evolves,
- Enhanced patient access to their medical records,
- Better informed and more involved patients,
- improved service planning,
- research potential.

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

The decision to shift from opt-in to opt-out disempowers the citizen. That is, the individual has not been consulted and asked to make an informed decision about how they would like their health record to be administered. The government is sending the wrong message to the person and their responsibility for their own health related decision.

The decision also reeks of political manoeuvring. The government is cognisant of the fact that a federal election is looming and appears to have made this decision to increase the likelihood of the scheme to succeed by increasing the number of people registered on the system. If people were given the opportunity to choose to opt-in, it is highly likely that the majority would not have done so.

The government obviously assumed that when faced with change, most people tend to prefer to stick with the current system. If this had occurred and the roll out of My Health Record failed, the opposition would use the failure to campaign against the government and the billions of dollars that it wasted on a failed quest to improve our health system.

The decision to shift from opt-in to opt-out increases the likelihood that people who have been involuntarily registered on to My Health Record lack sufficient knowledge about the many aspects of the system. For example, the person may not be aware of the range of health workers that have access to their personal

health information. The fact that an individual can be registered on to MHR without their consent raises significant privacy and ethical issues.

More specifically, one of the main features of MHR allows an individual to personalise access of specific documents. That is, they can set up the system to prevent certain healthcare professionals or organisations from accessing their personal records. Another feature of MHR allows a person to request an SMS alerts when a healthcare organisation accesses their record for the first time. These features are rendered redundant if the person has no knowledge of their existence.

The decision to shift from opt-in to opt-out appears to be based on the flawed assumption that an individual has sufficient knowledge of the MHR system privacy controls and multiple other complicated functions. Moreover, the reality of the MHR system requires the user to have significant computer and knowledge. Notwithstanding, in order for the MHR system to be used as envisaged, the user is assumed to have a strong grasp of and familiarity with digital technology.

Unfortunately, the reality is that a large number of people do not possess the required computer and digital literacy skills! This is particularly concerning given that six million Australian's are already registered on to MHR. The government has not consulted widely, or invested in training people in the use of the system.

For example, the MHR system has a default setting that gives health professionals and organisations access to certain information about the patient. If an individual wants change the default settings do that a podiatrist cannot access their mental health records, they must log in to and personalise their privacy and security settings.

A significant majority of the Health Workers Union members reported that they had little or no knowledge of the abovementioned default settings, privacy codes, and other aspects of the MHR system. Moreover, members reported that they

"had no idea how they would log on to MHR and make any changes". They also expressed concern about the fact that the government planned to implement the MHR system in August of 2018 without providing people with sufficient knowledge and training about how a user can manage their MHR account.

c. Privacy and Security, including concerns regarding:

i. the vulnerability of the system to unauthorised access

The Australian Privacy Foundation, the Australian Medical Association, the Royal Australian College of GPs, other and other consumer peak organisations recognises that electronic records systems can assist clinicians and improve the quality of health care for individuals and support the MHR system. However, all of these organisations have expressed concern about potential for privacy and security breaches.

Cyber security experts and privacy advocates have raised concerns about the security of information, particularly for those with conditions that might result in discrimination, such as mental health problems or sexually transmitted infections.

There is also a big chance that a person's medical record may contain info about their significant others. Meaning that a carers confidential information can be accessed via their loved ones electronic medical records. Moreover example, mental health clinicians often include their client's carer's predicament and ongoing stress related to the person that they care for.

For example, the Carer Crisis Fund (CCF) requires the clinician to complete a form stating what problems (stress, financial, accommodation, mental health) the carer is experiencing in order to justify assistance from the CCF.

In relation to security safeguards, the Australian Digital Health agency (ADHA) has stated that My Health Record has multiple safeguards in place to protect an

individuals' information including encryption, firewalls and secure login. This information was sourced from the MHR website and does not provide information on the type of system that is being used to protect the MHR system from hacking.

Despite reassurances from the ADHA and the Federal Health Minister who stated that the MHR system was protected by 'military-grade' security, on August the 2nd 2018, the Australian Digital Health Agency has admitted that the My Health Record system has been hacked on numerous occasions, at least nine times (Nova100, 2018). These revelations raises serious concerns about the system's so called security safeguards and demonstrates that personal data being stored on MHR can be compromised.

In reference to the Honourable Health Minister's comments about the My Health Record system having military grade security, it is common knowledge that Australia's Signals Intelligence Agency security was breached by a hacker between July and November 2016. During that period, a hacker downloaded 30 gigabytes of restricted information on the F-35 Joint Strike Fighter, the P-8 submarine hunters and Australian naval vessels (The Australian, 2017).

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

Section 70 of the My Health Record 2018 legislation allows government agencies access to a person's confidential health records. Centrelink, the Australian Taxation Office and other agencies can access any persons MHR file. These and other government agencies seem to have unrestricted access. That is, they can access information about a particular person's current medication regime. This type of access increases the number of people (non-healthcare related) able to access confidential medical information and the likelihood of personal information falling into the hands of third parties.

Some people may say that it is OK for the above government agencies to access an individual's MHR because the workers are government employees and already have access to other information about Australian citizens. Privacy advocates have significant concerns about the number of people that can access private information on the MHR system.

A very important fact that remains unclear based on the current information that the government has made public is does a patient own the data about them in the My Health Record system 2018? According to the MHR government website, the government makes the following statements:

- you cannot delete your record,
- you can only deactivate it,
- the contents of documents in your record are owned by and can only be changed by the author,
- the government has multiple legal reasons to access and use data in your health record without consulting or informing you,
- your GP can upload a shared health summary without your permission or discussing with you the contents.

Therefore, based on the above information, it is unlikely that a patient owns their data. This raises questions about privacy of information and the Health Workers Union urges the Senate to investigate this matter in detail before passing the legislation.

Can a My Health Record user restrict access to their information?

The HWU has added the above subheading to this document due to the lack of clarity about the capacity of a MHR user to limit access to their health information. The My Health Record Website (2018), Set Privacy and Security Controls page states "It's an individual's choice who sees their My Health Record, what's in it and who it is shared with".

However, after reading more about the ability of an individual to restrict access, it appears that the restriction controls only apply to organisations. Meaning that individual health providers are exempt to the 'restrict access' settings.

Furthermore, it appears that the MHR website uses carefully chosen words or semantics that confuse the average patient. The choice of words MHR website uses make a significant difference in relation to access to patient information. And in many cases a legal expert is required to interpret what the actual statements carried over from clauses used in the MHR 2018 system legislation.

For example, the MHR website states that the user has the "choice who sees their My Health Record what's in it and who it is shared with". However, "choice who sees their My Health Record" is not equivalent to "choice who sees the data in My Health Record" (My Health Record Website, 2018).

Therefore, patient data contained within a patients My Health Record is basically a blueprint copy of data that has emanated from or has been transferred to other systems. The MHR system 2018 legislation stipulates that the "prohibitions and authorisations do not apply to this data" (My Health Record Website Legislation and Governance page, 2018). Meaning that the "prohibitions and authorisations" only apply to data collected specifically for My Health Record.

Moreover, the MHR legislation reads as follows "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" (My Health Records Act 2012).

For example, if a patients Doctor downloads a record of a consultation or an Area Mental Health Discharge Summary from My Health Record into their own database, the "prohibitions and authorisations" of the My Health Record are not

applicable in this instance. Basically, once data has been accessed from any given patients My Health Record electronic files, only restrictions that apply to normal health data are valid.

In a nutshell, once data has been accessed and left the My Health Record system 2018, all trace of it vanishes. Furthermore, the legislation is absent of any clauses that stipulate the need for an audit trail of patient data that has left the MHR system.

The Health Workers Union urges the Senate to explore this aspect of the MHR system 2018 legislation. We recommend that the Senate alter the MHR legislation 2018 so that patient data cannot just vanish into thin air after it has been accessed. An audit trail is required to prevent third party for profit organisations obtaining patient data.

Existing clauses within the MHR legislation are a slippery slope that can lead to a broad spectrum of organisations and individuals gaining access to an individual's private and confidential medical records. In fact, this point is connected to the next section of the submission, or the next terms of reference of the senate inquiry. In particular, third party access to health insurance agencies and employers.

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

The governance relating to third party access to My Health Record accounts has been a source of major discussion. Multiple organisations and private citizens have raised concerns about the wealth of data that will be generated by MHR and the potential for third party users to gain access to it and as a result increase the potential for privacy breaches.

The Australian Digital Health Agency (ADHA), which is responsible for the implementation of MHR and multiple government spokespersons have stated that the My Health Record system will allow patients to elect to opt-out from having their personal information used for secondary use purposes. Apparently all they have to do is to select the 'withdraw participation' option, wherever that may be located.

Moreover, third party access for the purpose of 'purely commercial' purposes, private health insurers, and others are apparently forbidden from accessing confidential patient information. The Australian Institute of Health and Welfare (AIHW) has been assigned the task of managing secondary uses. The AIHW has stated that they will be seeking consultation (the coming months and years) with relevant stakeholders to assist in policy development in this important area.

Australia's My Health Record system's privacy structure is indistinguishable from the botched MHR system that the English government implemented several years ago. The United Kingdom government realised that the digital medical records system they adopted lacked the necessary privacy safeguards after discovering that the system was selling patient data to drug and insurance companies.

The English version of MHR gathered patient information from GP, hospital and other health professionals and established a database. MHR administrators then proceeded to sell, for a profit, confidential patient information to drug and insurance companies. The dataset included sensitive information about patient's mental health and chronic disease conditions, smoking, drinking behaviour, as well as other demographic information.

Australian private health insurance companies have already expressed their desire to access patients MHR information and stated that they expect that they will be able to gain access to a person's health records in the near future.

Employer groups have gone on record that they should be able to access the private medical records or their employees and appeared to be confident that they would be granted access in the not too distant future. Obviously their industry representatives have been lobbying government and may have received positive feedback from various government advisors and ministers.

The Health Workers Union and its members are concerned about employers, insurance companies and others gaining access to confidential patient medical records. We unequivocally believe that granting such organisations access to patient's medical records would be a breach of privacy laws. We oppose the prospect of patient's confidential records being shared with insurers, employers and others.

Moreover, under the current MHR system healthcare providers are able to initiate uploading of two years of MBS and PBS data of users, once they activate their record. This is concerning because involuntary registered MHR patients and patients with little to no computer and digital health capabilities are not in a positon to deny access to organisations logging on and accessing their data if they do not access their record first and decide to change the default data access parameters.

For example, organisations would be able to access a client's prescription information and use it to determine their diagnoses. Due to greed and the fact that medical records are highly sought after by various companies, it is most likely that the MHR third party access arrangements will lead to privacy breaches.

And even though the MHR system allows a MHR user to advise their healthcare provider(s) not to upload individual items to their My Health Record, the system does not allow a user to prevent past MBS and PBS data from being accessed. The HWU believes that this is a significant flaw in the system and must urgently be rectified! That is, the default setting must not others to access patients MHR

unless they change their setting and personalise them.

The Office of the Australian Information Commissioner (OAIC) recently released its second report on the Notifiable Data Breaches (NDB) scheme. The report revealed that a significant number of breaches reported to the privacy watchdog were related to malicious or criminal attack (Office of the Australian Information Commissioner, 2018).

The majority of breaches were related to cyber hacking. Other breached involved data or paperwork theft or loss (mental health clinician forgetting client file on a Tram) employee sabotage and the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes (Office of the Australian Information Commissioner, 2018).

Consistent with the first NDB scheme report, the largest number of breaches occurred within the health sector. Forty nine of the breaches were reported by health service providers (Office of the Australian Information Commissioner, 2018a, 2018b).

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

i. the public information campaign

The Australia government has been working hard to convince its citizens that the My Health Record system is the only option available for better managing the health care information of Australians. We have witnessed an orchestrated campaign involving media advertising, frequent political commentating, the use of general practitioner clinics, pharmacies and other means to win the publics support for the electronic My Health Records system 2018.

The Health Workers Union is concerned about the amount of money being spent to sell the My Health Record system to the public. The government has reportedly allocated $55 million for the education, training and support of healthcare providers for the Opt-Out phase of the campaign! The government has spent more than $100 million just on the Opt-out Phase of their campaign!

Of greater concern to the HWU is that the government has spent over $2 billion dollars on the My Health Record system (Minion, 2018). The government initially commenced the digital health record project in 2012 under a different title, namely, Personally Controlled Electronic Health Record. Current estimates put the number of people signed up for My Health Record at 6 million (Minion, 2018).

The Health Workers Union is disappointed that the government has not adequately consulted the community and relevant organization's and stakeholders. Much of the information disseminated about the MHT system has been recent.

e. measures that are necessary to address community privacy concerns in the My Health Record system

Due to the privacy breaches reported by the Office of the Australian Information Commissioner (2018 and other data breaches being reported in the media (email accounts, bank accounts, identity theft and so on) Australians demand world class privacy and security protections. If the My Health Record System 2018 cannot deliver such assurance then its release must be delayed until such a time that it can.

The federal health minister recently announced changes to the MHR system that will allow the deletion of records and restrict government agencies' access to patient data. These steps go some way towards reassuring patients abut are not enough.

Despite the government's claims, the HWU does not believe that privacy issues not been fully addressed. The MHR system allows confidential data to easily be taken out of the system. The system has been designed so that data can readily be transferred in and out of it. However, this function threatens patient privacy and must be altered by the government or the Senate so that data is more secure and tracked when it is taken out of the system.

The number of organisation's and health care professionals that have access to the MHR system must be limited. Privacy protections must be put in place that prevents unauthorized persons or organsiation's from accessing patient information.

The Australian Digital Health Agency (ADHA), which is responsible for the implementation of MHR, has recently stated that a range of safeguards existed to stop patient data being given to companies. Based on these comments and other assurances, is it clear that the ADHA has not learnt from the English experience with an equivalent MHR system.

We urge the ADHA and the senate to study what occurred in the UK when they attempting to roll out their digital health record system. We also urge the government to implement additional features and safeguards to prevent the same thing happening in Australia.

f. how My Health Record compares to alternative systems of digitising health records internationally

Before we compare My Health Record to international systems of digitising health records, we will introduce a number of local alternatives. The federal government has been exploring a range of other systems for a number of years. However, the government has not mentioned these comparative systems that it could use as alternatives to MHR. The alternative digital health record systems include the following:

- Department of Human Services- Medicare Express Plus,
- The Medicine Wise app of the National Prescribing Service.

It is important to compare My Health Record to alternative international systems. Such comparisons allow us to gauge how Australia is progressing. However, comparing Australia's progress to other countries in regard to the implementation and adoption of digital health is fraught with difficulties. That is, other countries have different healthcare systems and different models of digital health.

The Australia government appears to have decided that a government-owned consolidated database containing copies of summary and some test data is the best way forward. Very few countries have adopted this approach. Countries like the United Kingdom, Sweden and New Zealand have moved towards providing access to patient data that is held local at medical center's or general practitioner offices (Bernd, 2018; New Zealand Ministry of Health, 2016).

The above approaches have the benefit that other capabilities such as appointments, prescriptions, patient results and so on can be accessed through the same access method. The above mentioned approach is patient centered and is in stark contrast to the My Health Record system.

For example, Australia's federal health system faces different challenges in making major nation-wide policy changes compared to countries such as New Zealand and Singapore who have unitary political systems (Bernd, 2018). Nonetheless, attempts to implement digital health records across the world have run into multiple problems and that it takes decades for a country to set up a workable and secure system.

Australia's focus on building the foundations for a national system which delivers interoperability across states and healthcare organisations places us in good stead for the following phases of the role our of MHR.

One indicator of a successfully implemented digital health record system can be seen in the country's ability to address interoperability (Bernd, 2018). For example, the United States has invested significant funding on incentive payments for health care providers that ca demonstrate significant and successful use of Electronic Health Records (Bernd, 2018).

Although the above mentioned incentive program has improved the use of electronic health records by healthcare providers, the United States continues to face major barriers when it comes to sharing electronic health data across organisations.

Compared to other countries implementation of electronic health records, Australia's MHR system is still in the roll out phase. In contrast, Singapore and Denmark commenced rolling out their E-Health records system in the 1990's. This has resulted in their electronic health records system to be improved and in an advanced stage compared to Australia's and many other countries (Bernd, 2018).

References

Australian Bureau of Statistics (2018). Victorian Census 2016. Viewed on 2/08/2018, at:http://www.censusdata.abs.gov.au/census/services/getproduct/census.

Australian Bureau of Statistics (2013). Australian Aboriginal and Torres Strait Islander health survey: First results, Australia, 2012-13. Canberra.

Australian Bureau of Statistics (2015). Labour Force Survey, Australia Unemployment by Region, October, Cat. No. 6202.0 Canberra.

Australian Bureau of Statistics (2015b). Labour Force, Australia, Oct. Latest ISSUE Released at 11:30 AM (CANBERRA TIME) 12/11/2015

Australian Institute of Health and Welfare (2013). Aboriginal and Torres Strait Islander Health Performance Framework 2012: Detailed analyses. Cat. No. IHW 94. Canberra: AIHW.

Bernd, B (2018).Interoperable EHR Systems – Challenges, Standards and Solutions. EJBI – Volume 14 (2018), Issue 2.

Henderson, S & Kendall, E (2011). Culturally and linguistically diverse peoples' knowledge of accessibility and utilisation of health services: exploring the need for improvement in health service delivery. *Australian Journal of Primary Health* 17(2) 195-201.

My Health Record Website (2018). Set Privacy and Security Controls page, Viewed on 29 August 2018 at: https://www.myhealthrecord.gov.au/for-you-your-family/howtos/set-privacy-and-security-controls.

My Health Record Website (2018). Viewed on 29 August 2018, at: https://www.myhealthrecord.gov.au/.

My Health Record Website (2018). Legislation and Governance page. Viewed on 13/9/2018, at https://www.myhealthrecord.gov.au/about/legislation-and-governance.

My Health Records Act (2012). Federal Register of Legislation, Viewed on 26th August 2018, at: https://www.legislation.gov.au/Details/C2017C00313

Minion, L (2018). Exclusive: Leaked ADHA document shows the agency grappling with My Health Record concerns. Healthcare IT News. Viewed on 29 August 2018 at https://www.healthcareit.com.au/article/exclusive-leaked-adha-document-shows-agency-grappling-my-health-record-concerns

National Commission of Audit (2014a). Volume 1, section 9.9 Aged care, Commonwealth of Australia.

National Commission of Audit (2014b). The Report of the National Commission of Audit, Phase one: Towards Responsible Government, Commonwealth of Australia.

National Strategic Framework for Rural and Remote Health (2012). Commonwealth of Australia standing council on health Department of Health and Ageing, GPO Box 9848, Canberra ACT.

New Zealand Ministry of Health (2016). Establishing the Electronic Health Record. Strategic Assessment. Prepared by: Craig Reid, Ministry of Health & Graeme Osborne.

Office of the Australian Information Commissioner (2018a). Notifiable Data Breaches Quarterly Statistics Report: 1 April – 30 June 2018.

Office of the Australian Information Commissioner (2018b). Notifiable Data Breaches first Quarterly Statistics Report: January 2018 – March 2018

The Australian (2017). Primrose Riordan. Accessed on 13/9/2018 at, https://www.theaustralian.com.au/national-affairs/defence/top-secret-australian-defence-data-hacked/news-story/2e014ae4a379ba2ba95fd72c1733e1fc