Australian Nursing And Midwifery Federation

SUBMISSION TO THE SENATE INQUIRIES INTO THE:

- My HEALTH RECORD SYSTEM
- My HEALTH RECORDS AMENDMENT (STRENGTHENING PRIVACY) BILL 2018

Australian Nursing & Midwifery Federation

Annie Butler
Federal Secretary

Lori-anne Sharp
Assistant Federal Secretary

Australian Nursing and Midwifery Federation
Level 1, 365 Queen Street, Melbourne VIC 3000
T: 03 9602 8500
F: 03 9602 8567
E: anmffederal@anmf.org.au
W: www.anmf.org.au

Introduction

The Australian Nursing and Midwifery Federation (ANMF) is Australia's largest national union and professional nursing and midwifery organisation. In collaboration with the ANMF's eight state and territory branches, we represent the professional, industrial and political interests of more than 275,000 nurses, midwives and carers across the country.

Our members work in the public and private health, aged care and disability sectors across a wide variety of urban, rural and remote locations. We work with them to improve their ability to deliver safe and best practice care in each and every one of these settings, fulfil their professional goals and achieve a healthy work/life balance.

Our strong and growing membership and integrated role as both a trade union and professional organisation provide us with a complete understanding of all aspects of the nursing and midwifery professions and see us uniquely placed to defend and advance our professions.

Through our work with members we aim to strengthen the contribution of nursing and midwifery to improving Australia's health and aged care systems, and the health of our national and global communities.

Background

The ANMF welcomes the opportunity to provide a submission to the Senate Community Affairs References Committee My Health Record system inquiry and the related My Health Records Amendment (Strengthening Privacy) Bill 2018 inquiry. This submission addresses both inquiries.

The ANMF has consistently taken a leadership role for the nursing and midwifery professions by participating in the development of policy and legislation relating to the implementation of a national digital health system. The ANMF considers the My Health Record (MyHR) system will assist our members to deliver safe, timely and competent quality care in their practice.

In the past the ANMF has made a significant contribution to the work of the National E-Health transition Authority (NEHTA), to the development of the Personally Controlled Electronic Health Record (PCEHR) system and the National Digital Health Strategy, through written submissions and personal representation, including participation in relevant committees. This commitment continues with the Australian Digital Health Agency. The investment in time and effort has been made by the ANMF because we maintain there are enormous benefits to be gained by the community, our nursing and midwifery members and other health practitioners, through an information system which delivers timely and consistent digital communication on a person's health status.

Since the commencement nationally from 16 July 2018 of the opt-out MyHR system, concerns have been raised about the effectiveness of the roll-out of the system, access to records and privacy and security of records. It is the ANMF's view that with continuing community and health professional education, training, awareness and strengthening of provisions of the MyHR Act, that those concerns can be addressed. The ANMF continues to support the opt-out system as the best method to ensure maximum engagement with the system and as a means to deliver optimal ongoing health benefits to both individuals and the Australian community.

a. The expected benefits of the My Health Record system

The ANMF considers there will be enormous benefit from the MYHR system, which will emerge over time and in line with the uptake and acceptance of the system. Amongst those benefits will be:

- enabling a person to have control of their healthcare
- enabling a person to control access to their health information
- enabling more informed decisions on treatment
- streamlining care management
- reduction in duplication of treatment, medication and diagnostic testing
- improved medicines reconciliation
- co-ordination, information sharing and connectivity between healthcare services
- improved health outcomes for individuals and communities
- increased administrative efficiency for healthcare providers
- healthcare providers, including nurses and midwives, becoming leaders in promoting, understanding and delivering digital healthcare

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

Since the Australian Government first proposed moving to a digital health system, the ANMF has advocated for an opt-out system.

When the PCEHR was first introduced in 2012 it was an opt-in system for both registered healthcare providers and individuals. Since its introduction, the PCEHR system and then renamed MyHR system have been subject to a number of reviews and inquiries. There has been a consistent finding that the system will achieve greater results if an opt-out approach is adopted.

An evaluation trial of the MyHR system was conducted in 2016. The findings of the participation trials were published in November 2016. Key findings were:

- the opt-out approach to increase both individual and healthcare provider participation and use is the preferred option
- the opt-out trial sites achieved better outcomes, in terms of participation, understanding and some aspects of the use of the MyHR system
- a national opt-out approach is not only acceptable to individuals, healthcare providers, participating health services and health department managers, it is seen by these participants as the only sustainable scalable approach.[1]

The ANMF supports the findings of the trial and the subsequent decision to move to a nationwide opt-out system. However, as discussed below, in response to terms of reference c, the move to opt-out, has demonstrated that there is still essential work to be done to ensure public confidence in the system. Such confidence is critical to the success of the system.

c. Privacy and security, including concerns regarding:

i. The vulnerability of the system to unauthorised access

Cyber-security

The system itself must have the highest possible privacy and security standards and continuous monitoring to ensure those standards are met. Over time, this responsibility will become increasingly demanding, as the MyHR system expands in uptake and use. Potentially, the MyHR may contain the personal and health data/information for every person in Australia. This rich data source will be increasingly attractive to IT hackers, whether individually, corporately or criminally motivated and resourced. Foreign government interests may also be a threat.

[1]. Siggins Miller, November 2018. Final report - Evaluation of the Participation Trials for the My Health Record

The ongoing responsibility to ensure utmost cyber security rests with the relevant Australian Government authorities and agencies. Any security or data breaches must be investigated and appropriate action taken to mitigate future risk. The ANMF seeks ongoing engagement and assurance with respect to the measures implemented to protect the personal and health data of all Australians.

Access and use of digital devices

On the ground, for example in a hospital setting, there are concerns about access that will need to be addressed with education, practice guidelines and most importantly, sufficient funding to provide a secure digital information system.

Problems of unauthorised and/ or unidentified access can occur as a result of poor hardware security. Such risks could arise where shared computers on hospital wards or operating theatres are used, or where staff use unprotected passwords or logins to access computers. For instance, a MyHR may be open for a health recipient on a legitimate basis but not closed after access/use, or a shared password may make it easy to access already opened records. While the system provides for identification of the user who opens the record, there is no method to identify a person who might inappropriately access an already open record.

Any unauthorised access, even with no ill intent, is a breach of a health recipient's privacy. There are circumstances, however, where unauthorised access may result in a real risk of harm to the health recipient's health or safety. These may include:

- an employer gaining access to information about an employee that could be used to adversely affect the employee's employment
- in a situation of workplace conflict there is scope for inappropriate use of sensitive information
- in situations of family or domestic violence .

All such risks are amplified where a health recipient is also an employee of a healthcare service or is related to an employee of a healthcare service. To mitigate these risks, a number of measures to reduce the risks associated with unauthorised/unidentified access must be implemented:

- government and relevant agencies, must promote and where appropriate, fund, all healthcare providers to have secure information systems;
- organisational healthcare providers must be required to have digital policies that promote maximum security of digital records. Such a policy should include ensuring access to digital devices (log-ins and passwords) are ascribed to each individual user of the device and log-ins are set to time-out.

- education should be promoted to alert all registered individual and organisational users to the privacy and security risks of the system to minimise the risk of harm. Cyber-security training should be available to all users.

Identifying and prosecuting breaches

The MyHR Act provides that to be eligible to register as a healthcare provider a unique health-care identifier must have been assigned to the individual or organisation under the *Healthcare Identifiers Act 2010* (HI Act). Ongoing cross-referencing and auditing of unique identifiers under both the MyHR and HI Acts could also strengthen the security of the MHR system. The Government has yet to adequately explain to the public what mechanisms are in place, or will be in the future, to capture breaches of the Act with respect to unauthorised access. The ANMF seeks further clarity as to how the activities prohibited by the MyHR Act will be identified and prosecuted.

In summary, to mitigate against unauthorised and or unidentified access to the system, all possible measures must be taken to ensure both cyber digital security and best practice on the ground. In addition, there must be transparent mechanisms in place to identify and prosecute any breaches of the Act.

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

Third party access by law enforcement and government agencies

ANMF has significant concerns about s70 as it currently stands. The legislation allows the System Operator to disclose health information in MyHR to an 'enforcement body', as defined by the *Privacy Act 1988*. The ANMF considers both the definition of 'enforcement body' and the purposes for which records can be obtained to be too broad and to fail to protect the individual's rights to privacy and control over personal information.

The concern with the current s70, is however, met by the proposed Amendment Bill. The ANMF supports the proposed addition of sections 69A and 69B, which will result in MyHR's only being disclosed to designated entities when a judicial order has been obtained or the healthcare recipient has consented. Such consent must be informed and appropriate measures in place to ensure informed consent. Any consequential amendments are also supported, including the removal of the application and definition of 'enforcement body' in the MyHR Act.

The proposed amendment to s70 to limit disclosure of information to circumstances where the System Operator suspects unlawful activity with respect to its own functions is an appropriate amendment.

Third party access by researchers and commercial interests

The ANMF does not seek to respond to terms of reference with respect to researchers. With respect to organisations with a commercial interest in access to and use of data stored in the system, the ANMF opposes any use of material by commercial organisations, including research for commercial purposes, or for any commercial purpose. Such access and or use would significantly undermine public confidence in the system.

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

Section 5 of the MyHR Act defines 'healthcare' by reference to the definition of health service in the Privacy Act 1988.

Section 6FB of the Privacy Act 1988 defines a health service as follows:

"6FB Meaning of health service

(1) An activity performed in relation to an individual is a health service if the activity is intended or claimed (expressly or otherwise) by the individual or the person performing it:

(a) to assess, maintain or improve the individual's health; or

(b) where the individual's health cannot be maintained or improved—to manage the individual's health; or

(c) to diagnose the individual's illness, disability or injury; or

(d) to treat the individual's illness, disability or injury or suspected illness, disability or injury; or

(e) to record the individual's health for the purposes of assessing, maintaining, improving or managing the individual's health.

(2) The dispensing on prescription of a drug or medicinal preparation by a pharmacist is a health service.

(3) To avoid doubt:

(a) a reference in this section to an individual's health includes the individual's physical or psychological health; and

(b) an activity mentioned in subsection (1) or (2) that takes place in the course of providing aged care, palliative care or care for a person with a disability is a health service.

(4) The regulations may prescribe an activity that, despite subsections (1) and (2) is not to be treated as a health service for the purposes of this Act.

The definition is broad and has an element of subjectivity allowing for interpretation as to whether a service is intended or claimed to be a health service. The definition includes the activity of assessing health. Without addressing each section of the MyHR Act that refers to healthcare and healthcare providers, it is clear that by virtue of providing 'healthcare' within the meaning of the Act, healthcare providers can access individual MyHR information. The MyHR Act does not as it currently stands provide any barrier to healthcare providers engaged by employers or insurers to gaining access to MyHRs.

For employment and insurance purposes, there are many instances where an assessment of health may occur. These may include:

- pre-employment health checks
- ongoing employment health checks,
- work cover related health assessments
- superannuation insurance claims
- health insurance applications and claims
- travel insurance applications and claims
- statutory body assessment of fitness to practice, via independent medical examination

Currently, an individual recipient can only control third party access to his or her MyHR by varying access codes. This requires the individual to have a sound knowledge of the system, sufficient literacy and to be in a position to withstand pressure from an employer or insurer to grant access. This may expose an employee to discrimination in employment, adverse action or limit employment opportunities. For individuals seeking insurance or to make a claim on insurance, unlimited access to MyHR information may result in a refusal or reduction of insurance cover and increased litigation. In both instances, individuals may be subject to an unjustified loss of privacy.

The current system is overly dependent on the capacity of the individual, who may be vulnerable in a range of ways, to navigate the system. The ANMF seeks to ensure individuals' rights, particularly with respect to employment and insurance are protected, while also balancing the benefits of the scheme.

Section 14(2) of the HI Act provides some protection around use and access to records. The HI Act makes it illegal to collect, use or disclose the healthcare identifier of a healthcare recipient for the purpose of communicating or disclosing health information for the purpose of:

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

Relying on these restrictions to access and use of health information is not sufficient to address all of the concerns about insurers and employers' use of such information. Firstly, the HI Act restriction only relates to use of a person's healthcare identifier. It does not extend to access gained via a Medicare or veteran's affair number. Secondly, with respect to employment it does not extend beyond the process of employing a person.

The ACTU has proposed including a clause similar to s14(2) of the HI Act into the MyHR Act with some modification and extension of scope. If a clause similar to s14(2) were to be included in the MyHR Act, it would need to extend to all individual forms of identification that can be used to access the record, including personal information, Medicare and Veteran Affairs numbers. In addition, the scope of unauthorised purposes should extend to access in connection with the employment of the healthcare recipient, including in connection with any worker's compensation claim. The ANMF consider this is an appropriate proposal that addresses the concerns raised above.

Such an amendment would work in conjunction with a healthcare recipient's ability to modify access to his or her records.

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

i. The public information campaign-

It has been apparent in the months since the system became opt-out that many issues have arisen that may have had less impact if broader understanding of the system had been provided prior to the move to opt-out. In addition, the move to opt-out has resulted in weaknesses in the legislation being identified. ANMF considers ongoing education, promotion and training about the system for both provider and recipient users is required. This in turn requires an ongoing commitment to funding being provided for these specific purposes.

ii. The prevalence of 'informed consent' amongst users

The ANMF considers that trust in the system will be enhanced if health recipients are conversant with their ability to exercise informed consent to access records. Health recipients should be aware that access and the ability to upload information can be granted or denied in each instance of use of the system (save for the exceptions provided in the Act). This awareness can be promoted through public education and when an individual accesses their record.

Health providers must also be educated around issues of consent and how to ensure health recipients have provided informed consent. Depending on the setting, this could involve asking a new patient to sign a consent form and could also include a discussion before material is uploaded to the system. Appropriate funding should be allocated for workforce education around understanding and obtaining informed consent.

Health recipients should be empowered to make informed decisions about the use of the system with respect to their own health. Ongoing surveying and collection of information about the prevalence of informed consent will be a valuable indicator of trust in the system.

e. Measures that are necessary to address community privacy concerns in the MyHR system

The ANMF considers that the measures put forward in the Amendment Bill should be adopted and that these will go some way to addressing privacy concerns. In addition, limiting or excluding access and use for third parties as outlined above will address concerns about information being used for purposes that may be adverse to the interests of the health recipient.

Ongoing education, training and awareness of the system is also essential for increased confidence in the system. This must be backed with transparency from Government agencies, in particular ADHA. Problems with the system must be dealt with expeditiously but must also be seen publicly to have been addressed and mitigated.

f. How MyHR compares to alternative systems of digitised health records internationally

The ANMF considers the MyHR system to be innovative and leading the move to digitised health systems. Comparison with other digitised health records internationally will provide opportunities to learn from other systems and to improve Australia's system. At present, ANMF does not seek to make any comment about comparison to other systems, but can see this forming part of future assessment and evaluation of the MyHR.

g. Any other matters

My Health Records Amendment (Strengthening Privacy) Bill 2018 Inquiry

With respect to the My Health Records Amendment (Strengthening Privacy) Bill 2018, ANMF supports the proposed amendments. The amendments with respect to s70 are addressed above.

Currently, if a registration is cancelled records remain in the system and could be accessed by some users. The second part of the Amendment Bill provides that where a health recipient decides to cancel their MyHR registration this will result in all records held within the system being destroyed, including those held in the National Repository Service.

The ANMF welcomes this change, which gives individuals greater control over and certainty about their records. The ANMF proposes however, that the amendment should go further and allow health recipients to cancel specific records resulting in those specific records being destroyed. For example, an individual with a MyHR that contains records about mental health in addition to other health material may wish to have records with respect to mental health destroyed but otherwise maintain a record.

Intersection of the MyHR system with other regulatory schemes

There are multiple other federal and state regulatory schemes that may intersect with the MyHR scheme. Of particular relevance are those schemes that require mandatory reporting or create obligations to share information. By way of example the Victorian Child Information Sharing Scheme and Family Violence Information Sharing Scheme are designed to ensure relevant agencies are communicating information between services to protect children or people experiencing family violence.

As outlined in this submission, security and privacy of information in the MyHR system is vital to the successful operation of the system. There is, however, a clearly identifiable risk to be managed in balancing the benefits of information sharing within and between schemes and ensuring the privacy and security of information contained within a system. What policies will be implemented to manage this risk and to inform the public of the way in which regulatory schemes interact with respect to sharing of information? What work will be done to manage the intersection between state and federal schemes that involve sharing of health information?

Conclusion

Thank you for the opportunity to contribute a submission to both the Inquiry into the My Health Record system and the Inquiry into the My Health Records Amendment (Strengthening Privacy) Bill 2018. The ANMF considers the ongoing successful implementation of the My Health Record digitised health system is critical to delivering high quality healthcare in the twenty-first century. The trust and confidence of both healthcare recipients and healthcare providers in the system, will be essential to that success.