



AUSTRALIAN MEDICAL  
ASSOCIATION

ABN 37 008 426 793

T | 61 2 6270 5400

F | 61 2 6270 5499

E | [info@ama.com.au](mailto:info@ama.com.au)

W | [www.ama.com.au](http://www.ama.com.au)

42 Macquarie St Barton ACT 2600

PO Box 6090 Kingston ACT 2604

---

# AMA submission to the Standing Committee on Community Affairs Legislation Committee Inquiry into the My Health Records Amendment (Strengthening Privacy) Bill 2018

## Committee Secretary

## Senate Standing Committees on Community Affairs Legislation

### Committee

PO Box 6100

Parliament House

Canberra ACT 2600

[community.affairs.sen@aph.gov.au](mailto:community.affairs.sen@aph.gov.au)

### Overview

The AMA welcomes the opportunity to provide a submission to the Standing Committee on Community Affairs Legislation Committee Inquiry into the *My Health Records Amendment (Strengthening Privacy) Bill 2018* (the **Bill**).

Following the shift to My Health Record opt out arrangements there was considerable concern the *My Health Record Act 2012* authorised the System Operator to release My Health Record information to law enforcement agencies and other government bodies without the patient's consent and without the need of a court order.

The amendments proposed in the Bill substantially reduce any discretion that the My Health Record System Operator has to disclose health information in the My Health Record. In particular, the Bill:

- ) Amends section 65 so that the ability to disclose where “authorised or required by law” only applies to four laws.
- ) Introduces a new section 69A which overrides any other Commonwealth, State and Territory laws that allow police or other government bodies to access records. Any such requests must be personally endorsed by a judicial officer and can only be directed to the System Operator.

Australian Medical Association

---

- ) Deletes sections 70(1) and (2) (being the provisions which allowed access by law enforcement); and
- ) Subjects section 70(3) to additional protections

These controls are substantially tighter than the controls that apply under the Privacy Act 1988 (Cth) to patient data stored in the clinician's own patient records. They also impose greater restrictions on the government's and courts' powers to require production than apply to data held by the patient outside the My Health Record system.

The requirement for a court order, a coroner's direction or a direction by a judicial officer should also ameliorate public concern that by virtue of the delegation powers in Section 98 of the My Health Records Act 2012, My Health Record data could be disclosed by a junior public servant or *any other person with the consent of the Minister*. Any delegate would be subject to the same stringent restrictions that apply to the System Operator.

A different privacy and security concern for some consumers is the retention of archived patient data in their My Health Record after they opt out. The Bill amends section 17 to provide for a 'hard delete' option; The System Operator is now required to permanently destroy all clinical information in a patient's My Health Record, if they request their Record to be cancelled.

Another area of public concern is the use of My Health Record data in relation to employment health checks. As discussed further below, the Bill generally prohibits a doctor from accessing a person's record for purposes that do not relate to the provision of healthcare to that patient. In addition, subsection 14(2) of the *Healthcare Identifiers Act 2010* expressly prohibits the use of healthcare identifiers for employment health checks. Use of My Health Record information is similarly prohibited in relation to a contract of insurance that covers the individual.

The AMA submission to the Senate Community Affairs References Committee Inquiry into the My Health Record System is at **Attachment A**. This provides the broader policy context of the My Health Record, and its system design, in which to consider the AMA's comments on the amendment Bill.

The remainder of this submission considers the technical issues associated with the *My Health Records Amendment (Strengthening Privacy) Bill 2018*.

The focus of this paper is on the legislative controls set out in Part 4 of *My Health Records Act 2012* and the further tightening of those controls set out in the Bill. These legislative controls supplement the technological and other controls that have been put in place to protect My Health Record.

As is illustrated by the examples given in this paper, the proposed legislative controls:

- ) are substantially tighter than the controls that apply to existing records; and
- ) recognise that the primary source of information will continue to be the medical practitioner or hospital's own records.

---

Australian Medical Association

---

In the AMA's view, assuming the Bill is passed, the remaining circumstances where the legislation allow disclosure strike an appropriate balance between:

- ) protecting patients' privacy; and
- ) allowing access in appropriate circumstances.

Of course, the AMA recognises that the Committee may identify other areas of the legislation which it may wish to examine. The AMA is happy to discuss these with the Committee.

### **Key protection – section 59(2)**

Section 59(2) provides that:

A person must not use or disclose health information included in a healthcare recipient's My Health Record if:

- (a) the person obtained the information by using or gaining access to the My Health Record system; and
- (b) the use or disclosure is not authorised under Division 2, and the person knows or is reckless as to that fact.

Section 59(2) effectively 'covers the field' in relation to the use of information contained in a My Health Record. This means that no one – including the patient themselves – can legally download information from a person's My Health Record unless it is expressly authorised by Division 2 of the *My Health Record Act 2012*.

Unlike some other provisions of Part 4, section 59(2) does not refer to a "registered" healthcare recipient. This means it applies equally to unauthorised access to the My Health Records of persons whose registration has been cancelled because they have died (section 51(6)). (This is different from the 'hard delete' that occurs when a person opts out.)

Section 71 confirms that section 59(2) does not apply to the medical practitioner's or patient's own records – even if they contain information downloaded from the patient's My Health Record.

### **Download and use by patients**

Section 67 provides that:

A healthcare recipient is authorised to collect, use and disclose, for any purpose, health information included in his or her My Health Record.

The main purpose for which a healthcare recipient will disclose their My Health Record is to obtain healthcare. However, a healthcare recipient may use their record for any other purpose. For example, a patient could choose – but is not required – to produce their My Health Record in legal proceedings.

Australian Medical Association

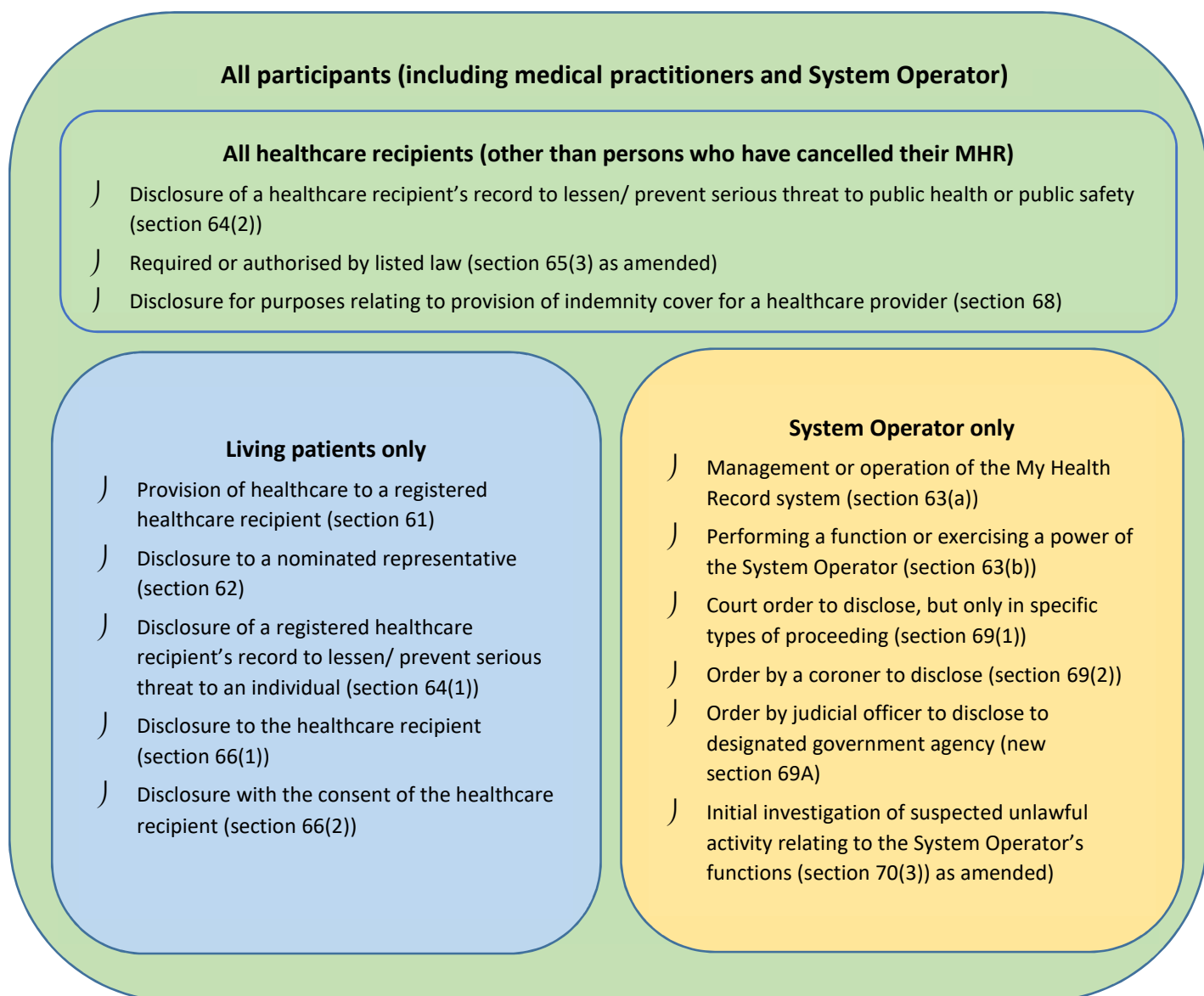
**Download and use by other persons**

The balance of Division 2 sets out the circumstances where persons other than patients are required or otherwise authorised to disclose a My Health Record. Diagram 1 divides these circumstances based on whether they apply:

- ) to all participants or only the System Operator; and
- ) to all healthcare recipients (other than persons who have cancelled their My Health Record) or only to living/ “registered healthcare recipients”.

Table 1 provides further detail in relation to section 65 and the System Operator’s other specific disclosure rights. These are the key items that have attracted media attention. Table 1 is drafted on the assumption that the Bill is passed.

*Diagram 1*



Australian Medical Association

Table 1

Provision	Authorises	Limitation	Reason for allowing disclosure
Section 63(a)	Collection, use or disclosure for the purpose of the management or operation of the My Health Record system	Only where the healthcare recipient would reasonably expect the participant to collect, use or disclose the health information for that purpose	This wording is consistent with Australian Privacy Principle 6.2(a) and recognises that the System Operator will necessarily use services of third parties (eg telecommunications providers) in operating the My Health Record System
Section 63(b)	Collection, use or disclosure in response to a request by the System Operator	Only where this is for the purpose of performing a function or exercising a power of the System Operator	This provision allows the System Operator to contact a healthcare practitioner about an apparent error or omission.
Section 65 (as amended)	Disclosure by participants [to the ANAO, Ombudsman or Privacy Commissioner]	Required or authorised by: <ul style="list-style-type: none"> <li>) the <i>My Health Records Act 2012</i>, the <i>Auditor-General Act 1997</i>, the <i>Ombudsman Act 1976</i>; or</li> <li>) laws supporting the Information Commissioner's functions in relation to My Health Record.</li> </ul>	The role of the ANAO, Ombudsman and Privacy Commissioner is to ensure compliance by government with legislation and other standards.
Section 69(1)	Disclosure by the System Operator to a court	Required by a court order but only where the proceedings relate to: <ul style="list-style-type: none"> <li>(i) the <i>My Health Records Act</i>;</li> <li>(ii) unauthorised access to information through the My Health Record system; or</li> <li>(iii) the provision of indemnity cover to a healthcare provider.</li> </ul>	Items (i) and (ii) are focused on ensuring the integrity of the My Health Records System. Item (iii) relates to indemnity cover. Indemnity cover is a key part of the Australian health care system. Insurers require full information about any issues in order to provide this insurance.
Section 69(2)	Disclosure by the System Operator to a coroner	Order or direction of a coroner.	It is in the interests of the public and the deceased patient to determine the cause of their death.
Section 69A (new provision)	Disclosure by the System Operator to a designated entity	Order by a judicial officer appointed under section 69B. The judicial officer must be satisfied that:	These provisions substantially override existing statutory provisions (in other legislation) which would otherwise allow

Australian Medical Association

Provision	Authorises	Limitation	Reason for allowing disclosure
		<ul style="list-style-type: none"> <li>) the designated entity would otherwise have statutory power to require production of the information; and</li> <li>) the other matters in section 69A(6) have been satisfied.</li> </ul>	<p>government agencies to request or require access.</p> <p>The judicial officer is required to consider the patient’s privacy and other sources of information before making any order.</p>
Section 70(3) as amended by section 70(3A)	Disclosure by System Operator to relevant persons or authorities	System Operator reasonably believes that disclosure is necessary to enable consideration of suspected unlawful activity that relates to the System Operator’s functions.	The System Operator needs to be able to involve the police or other relevant authorities if My Health Record is inappropriately accessed.

**Circumstances where My Health Record cannot be disclosed**

As noted above, section 59(2) prohibits use or disclosure of information obtained from My Health Record for any purpose that is not listed in Division 2.

The following sections provide examples of where information cannot be disclosed. These examples have been provided to illustrate how strictly the legislation (as amended by the Bill) controls the circumstances where the System Operator and medical practitioners can download records.

As noted earlier, the *Healthcare Identifiers Act 2010* also operates in addition to the My Health Records legislation (as amended by the Bill) such that particular types of unauthorised uses – such as pre-employment checks – will be a breach of both section 59(2) and the *Healthcare Identifiers Act 2010*.

**Circumstances where My Health Record cannot be disclosed – civil proceedings**

One illustration of where the legislative protections that apply to My Health Record are far more stringent than the protections that apply to other types of records (including records held by doctors and patients outside the My Health Record system) is civil proceedings.

For example, there is no ‘head of power’ that would allow the System Operator to comply with a court or tribunal order directing it to disclose a My Health Record for the purposes of:

- ) a divorce proceeding;
- ) child support matter;
- ) personal injury claim (unless it involved medical negligence); or
- ) proceedings to obtain an apprehended violence order.

Australian Medical Association

---

This is because these proceedings do not fall within section 69(1)(b). Section 69(4) provides that: Except as mentioned in subsection (1) or (2), the System Operator is not authorised to disclose health information included in a healthcare recipient's My Health Record to a court or tribunal unless the healthcare recipient consents.

The patient is unlikely to consent if the information incriminates them or is detrimental to their case.

The Explanatory Memorandum for section 69 noted that:

Clause 69 specifies the circumstances in which health information in a consumer's PCEHR may be collected, used and disclosed in response to subpoenas and other similar information gathering mechanisms, and in response to an order of a court or tribunal.

The decision to restrict the ability of courts and tribunals to access health information contained in a consumer's PCEHR has been made for a range of policy reasons:

- ) the PCEHR system, by drawing together health information about a consumer from many different sources, will create a much richer data source about consumers than any existing system. This warrants additional protections, including placing some restrictions on access to health information in the PCEHR system by way of subpoenas and other orders of courts and tribunals. Registration by consumers in the PCEHR system is voluntary, and consumers do not want the PCEHR system to be a source of health information that can be accessed for any court or tribunal purpose;
- ) health information in the PCEHR system will be available from other sources. For example, healthcare providers' local clinical records system will keep a copy of health information that is uploaded to the PCEHR system. Healthcare providers are also able to download copies of a consumer's PCEHR where authorised under Division 2 of Part 4 of the PCEHR Bill. Health information outside of the PCEHR system is subject to existing local laws and the provisions in the PCEHR Bill will not apply to the locally-held copy of the information or restrict access to such locally-held health information (see clause 71);
- ) the restrictions only apply to health information in a consumer's PCEHR. The restrictions under clause 69 would not prevent access to other information in the PCEHR system, for example, information about the operations of the PCEHR system generally; and
- ) the administrative burden on the System Operator of having to deal with unrestricted access to PCEHR-based health information by way of subpoena and other orders of courts and tribunals would likely be significant.

While the court could subpoena a party's medical practitioner, the medical practitioner would only be able to comply with the court order to the extent that it required production of the medical practitioner's own records. The medical practitioner could not download any additional material from the patient's My Health Record unless:

- ) the patient (or their nominated representative) consented (section 66); or
- ) the proceedings related to medical negligence (section 68).

This is because:

- ) section 69(2) (court orders) only applies to disclosure by the System Operator; and
- ) there is no other provision in Division 2 which authorises the medical practitioner to download and disclose a patient's My Health Record for this purpose.

---

Australian Medical Association

---

This is also emphasised by section 69(3). It provides that:

Except as mentioned in subsection (1) or (2), a participant in the My Health Record system, or a healthcare recipient, cannot be required to disclose health information included in a healthcare recipient's My Health Record to a court or tribunal.

In other words, a medical practitioner cannot be penalised for failing to comply with a court order requiring download of a patient's My Health Record as the medical practitioner is not authorised to produce this information for this purpose.

Similarly, a patient could not be required to download – and produce to the court – information which is contained in their My Health Record but is not otherwise in their care, custody or control.

### **Circumstances where My Health Record cannot be disclosed – executor of deceased patient**

The situations where a My Health Record of a deceased person can be disclosed are even more tightly confined. This is because a deceased person can no longer provide consent and a number of the other key 'heads of power' will also cease to apply.

For example, section 62 authorises a medical practitioner to provide health information from a My Health Record to a patient's nominated representative. However, section 7(1) requires that an agreement be in force between a nominated representative and a healthcare recipient. Accordingly, a person will cease to be a nominated representative if the healthcare recipient dies.

The practical implications of this are that a nominated representative that is caring for a person (eg a spouse) will be able to access their My Health Record while they are alive but will lose access if they die. This would include a scenario where their spouse dies unexpectedly (eg, in a car accident or during a procedure).

The Health Records (Privacy and Access) Act 1997 (ACT) and Health Records Act 2001 (Victoria) both include provision for a deceased's legal representative to request access to a deceased person's medical records. In other States and Territories, access is at the discretion of the medical practitioner.

Examples of why the deceased's representative may want to access their records include:

- ) to better understand how they died;
- ) to assist in taking legal proceedings on behalf of their estate (eg, where the deceased died in a car accident or had some other kind of civil claim);
- ) to assist in resolving a paternity or family provision claim; or
- ) to obtain information about any hereditary conditions.

There is no 'head of power' which authorises either the System Operator or the medical practitioner to provide this information. This means that, unless the claim involves medical indemnity cover, a medical practitioner would not be able to provide any information that is in the deceased's My Health Record but not in the medical practitioner's own files.



---

Australian Medical Association

---

This example has been provided to illustrate how strictly the legislation (as amended by the Bill) controls the circumstances where the System Operator and medical practitioners can download records.

### **Circumstances where My Health Record cannot be disclosed – coronial proceedings**

As noted above, the System Operator can be ordered by the coroner to disclose a deceased person's My Health Record.

However, there is no 'head of power' that would allow a medical practitioner to disclose information contained in a deceased patient's My Health Record to a coroner, unless that information is already contained in the medical practitioner's own records. This is because:

- ) section 69(2) (coroners) only applies to disclosure by the System Operator; and
- ) there is no other provision in Division which authorises the medical practitioner to download and disclose these records.

### **Circumstances where My Health Record cannot be disclosed – criminal proceedings**

As noted above, the System Operator can be ordered by a court or tribunal to disclose a person's My Health Record but only where the proceedings relate to:

- (i) the *My Health Records Act*;
- (ii) unauthorised access to information through the My Health Record system; or
- (iii) the provision of indemnity cover to a healthcare provider.

Unless the patient consents, there is no 'head of power' that allows the System Operator to comply with a court order issued as part of other types of proceedings.

If the patient is dead, they cannot consent. This means that, for example, the System Operator could not give evidence in an assault trial about the My Health Record of a victim who has subsequently died from their injuries.

While the court could call the victim's or the defendant's medical practitioner, the medical practitioner would only be able to comply with the court order to the extent that it required production of the medical practitioner's own records. This is because there is no provision in Division which authorises the medical practitioner to download and disclose additional information from the victim's My Health Record for this purpose.

New section 69A would allow the police to apply to a judicial officer for an order that the System Operator disclose the victim's My Health Record. This would be on the basis that:

- ) in all the circumstances, the particular disclosure of the particular information to the [police] is reasonably necessary;
- ) there is no effective means for the [police] to obtain the particular information, other than an order under [section 69A]; and

Australian Medical Association

---

- ) the disclosure of the information would not, on balance, unreasonably interfere with the privacy of the healthcare recipient.

**Circumstances where My Health Record cannot be disclosed – other proceedings**

As noted above, section 69 relates to disclosures to a court or tribunal. Section 69A relates to disclosures to other bodies.

Previously section 65 allowed participants (including medical practitioners) to download and disclose a person’s My Health Record where required or authorised by law.

For example, currently the Chief Executive Medicare has the power to issue a Notice to Produce to the System Operator or a medical practitioner under section 129AAD of the *Health Insurance Act 1973*. Notices cannot be issued to the patient directly (section 129AAD(7)).

Similarly, section 106B of the *Health Insurance Act 1973* provides that a member of a Professional Services Review Committee may issue a summons requiring any person (other than the person under review) to produce documents. This could be the System Operator, the patient or another medical practitioner.

Section 65(3) now restricts section 65 to use or disclosure required or authorised by:

- ) the *My Health Records Act 2012*;
- ) the *Auditor-General Act 1997*;
- ) the *Ombudsman Act 1976*; and
- ) laws supporting the Information Commissioner’s functions in relation to My Health Record.

New section 69A overrides all other Commonwealth, State or Territory laws that would otherwise provide an agency or a State or Territory authority (other than a court or tribunal) with the power to request or require the System Operator, a medical practitioner or another participant to produce information contained in a My Health Record.

The terms “agency” and “State or Territory authority” are defined in the *Privacy Act 1988* (Cth). The term “agency” is quite broad. It includes:

- ) Ministers
- ) a body (whether incorporated or not) ... established or appointed for a public purpose by or under a Commonwealth enactment, not being an incorporated company, society or association; or
- ) a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment.

Under the proposed approach, the entity requesting the information (ie, the Chief Executive Medicare or Committee member in the examples above) would be required to satisfy a judicial officer that:

Australian Medical Association

---

- (a)(iii) in all the circumstances, the particular disclosure of the particular information to the designated entity is reasonably necessary for the purposes of a thing done by, or on behalf of, the designated entity; and
- (a)(iv) there is no effective means for the designated entity to obtain the particular information, other than an order under this section; and
- (b) the disclosure of the information would not, on balance, unreasonably interfere with the privacy of the healthcare recipient.

In addition, section 69A(9) also requires that the order:

- (a) identify the healthcare recipient; and
- (b) specify the particular information to be disclosed; and
- (c) specify a purpose and an expiry date. (The expiry date must be no more than 6 months.)

While not expressly stated, to satisfy (b), the government entity will need to justify why it needs the System Operator to provide the information without notifying the patient or obtaining their approval. As noted above, one scenario where it is not possible to obtain consent is where the patient is dead. There may also be scenarios (such as section 129AAD(7)) where the government agency is not authorised to request the information from the patient directly.

The procedure in section 69A only allows judicial orders to be made to the System Operator. It does not authorise disclosure by any other participants. This means that, unless the patient consents, a medical practitioner cannot download a person's My Health Record in order to comply with:

- ) a Notice to Produce issued under section 129AAD of the *Health Insurance Act 1973*;
- ) a summons to produce documents to a Professional Review Committee under section 106B of the *Health Insurance Act 1973*; or
- ) another form of statutory notice to produce.

This is because there is no 'head of power' that would authorise the medical practitioner to provide this information.

This is also emphasised by section 69A(2). It provides that:

Except as mentioned in subsection (1) or in accordance with a law covered by subsection 65(3), a participant in the My Health Record system, or a healthcare recipient, cannot be required to disclose health information included in a healthcare recipient's My Health Record to a designated entity.

In other words, a medical practitioner cannot be penalised for failing to comply with a statutory notice to produce information contained in a patient's My Health Record as a medical practitioner is not authorised to download this information for that purpose.

Similarly, a patient could not be required to download – and produce to a government agency – information which is contained in their My Health Record but is not otherwise in their care, custody or control.

Australian Medical Association

---

**Conclusion**

The purpose of the above examples is to highlight that:

- ) the legislative controls on My Health Record (as amended by the Bill) are extremely tight; and
- ) the circumstances in which persons other than patient can download information are very limited.

Similarly, the circumstances where the patient can be required to produce information contained in their My Health Record are extremely limited.

**14 SEPTEMBER 2018**

**Contact**

Luke Toy  
Director  
Medical Practice Section  
Australian Medical Association

## Attachment A



AUSTRALIAN MEDICAL  
ASSOCIATION

ABN 37 008 426 793

T | 61 2 6270 5400

F | 61 2 6270 5499

E | [info@ama.com.au](mailto:info@ama.com.au)

W | [www.ama.com.au](http://www.ama.com.au)

42 Macquarie St Barton ACT 2600  
PO Box 6090 Kingston ACT 2604

---

# AMA submission to Senate Community Affairs References Committee Inquiry into *the My Health Record System*

**Committee Secretary**  
**Senate Standing Committees on Community Affairs**  
PO Box 6100  
Parliament House  
Canberra ACT 2600  
[community.affairs.sen@aph.gov.au](mailto:community.affairs.sen@aph.gov.au)

As the peak professional organisation representing medical practitioners in Australia, the Australian Medical Association (AMA) welcomes the opportunity to provide a submission against the terms of reference for this *Inquiry into the My Health Record system*.

## Executive Summary

Treating clinicians need to have access to a detailed and accurate clinical patient history to provide the best possible care. The siloed nature of the Australian healthcare system and the localised storage of patient records in their doctor's own patient records, compromises the flow of patient information between health care settings, and between health care practitioners. Many of the greatest failures in patient care and safety result when patients are required to move across the health system but their clinical information does not follow them.

The My Health Record (Record) has the potential to circumvent these limitations to ensure clinically important patient information is available at the point of care, irrespective of the health care setting and the location of the treating doctor. The result is better connected care, reduced medical harm from avoidable medication complications and allergic reactions. As the My Health Record matures and patient participation levels increase, the Record may also generate health system efficiencies by eliminating diagnostic and pathology tests currently duplicated because test results are not available to the treating doctor. Not only is duplication wasteful, it is detrimental to the patient as duplicated tests expose them to additional radiation from X-rays and CT Scans.

---

Australian Medical Association

---

Increased patient engagement in their own healthcare is another way the My Health Record can improve quality of care. Research indicates 40-80 per cent of medical information provided by healthcare practitioners is forgotten immediately by patients. If patients have access to their clinical data in their My Health Record, they are more likely to understand their health conditions, adhere to treatment advice and engage more actively with their treating clinicians in their ongoing care. This will also assist in increasing overall patient health literacy which will improve long term health outcomes and indeed improve prevention and education activities. The inclusion of patient nominated advanced care planning documents in the My Health Record increases the likelihood emergency treatments will align with patient preference if they have lost the ability to speak for themselves. It will increase the chance that a patient who has lost decision-making capacity will receive treatment that they *do* want, and reduce the chance that they receive treatment that they *don't* want, at a time when they are vulnerable and when their doctor might otherwise be “flying blind” in deciding on how to act.

If the benefits of My Health Record are to be fully realised, the My Health Record system will need to become self-sustaining. The Northern Territory experience and opt out trials suggest a participation rate of around fifty percent achieves this threshold and is more likely to occur under opt out arrangements. Opt out removes the burden on patients to initiate the effort to register, but public acceptance of opt out is predicated on the patient's confidence their health data in the My Health Record is secure and their privacy will be protected.

There was a momentum of negative media at the start of the opt out period. In order to restore public confidence in My Health Record, it is critical the privacy issues raised in the media are addressed.

The AMA notes the additional privacy protections set out in the proposed *My Health Records Amendment (Strengthening Privacy) Bill 2018* (Bill) go a long way towards achieving this. The Bill substantially reduces any discretion that the My Health Record System Operator has to disclose health information in the My Health Record. The limits are substantially tighter than the controls that apply under the *Privacy Act 1988* (Cth) to patient data stored in the clinician's own patient records. For example, Australian Privacy Principle 6.2(b) allows a record holder to produce a patient's record where this is “required or authorised by or under an Australian law or a court/tribunal order”. The equivalent provisions of the *My Health Records Act* – sections 65 (as amended) and 69 – only authorise or require access in very limited circumstances.

A different privacy concern for some consumers is the retention of their My Health Health Record data after they opt out. This is also resolved in the Bill by providing for a ‘hard delete’ if a patient cancels their Record. The AMA is satisfied the permanent deletion of a Record after it is created, provides citizens with a genuine choice as they can retain the Record created by Government on their behalf, or withdraw completely by exercising the choice.

Above and beyond the amendments proposed in the Bill, the existing privacy and security protections in the My Health Record design are also substantial. For example any software that connects to the My Health Record system must be secure, encrypted and certified as conformant. The software is subject to automated checks to ensure it maintains conformity standards.

## Australian Medical Association

---

Conformant clinical software also assigns unique staff member identification codes and records each time a staff member accesses the My Health Record system. A log is automatically generated to record each time the My Health Record is accessed by a health provider *organisation*. These logs mean Record owners can see which organisations have accessed their Record in real time and the System Operator can drill down to identify which staff member Individual Healthcare Identifier was used to sign into the Record. The AMA considers this level of transparency combined with criminal penalties for unlawful access equal to up to two years in prison and up to \$126,000 in fines, act as robust, meaningful deterrents.

The privacy protections available to patients add further security to patient data. Patients can instruct their health provider at the point of care, not to upload information they consider sensitive. They can put a Record Access Code across their whole record or an individual document so only the providers who have been given the access pin number can see them. Record owners can also set up alerts to receive a text or email notification if their Record is accessed by a new health provider. Record owners can remove documents from their Record or opt out at any time. See ADHA information on [My Health Record Access Controls and 'How to'](#) instructions. These privacy controls are extensive and would appear to provide a greater level of privacy protection than paper based patient files and the common practice of faxing health information.

Fundamental to the public acceptance of the My Health Record opt out arrangements is a long term, well-funded, public education campaign to rebuild public confidence and a deeper understanding of how the My Health Record works, and the benefits and the privacy levers available to patients to boost their privacy settings to suit their own circumstance. It is a difficult public communication challenge but unless it succeeds, a sustainable level of participation may not be achieved. This includes the participation of doctors.

Trust is the basis of the doctor patient relationship and some doctors, if not many, will balk at adopting the My Health Record if they have concerns about the privacy of their patients. The Australian Digital Health Agency's (ADHA) reliance on training Primary Health Networks to provide My Health Record information and assistance to health providers (mostly general practitioners) on their behalf has so far, been patchy. The Government's reliance on this model to reach out to health providers needs to be reconsidered. Likewise, there are costs for doctors associated with participation and compliance that must be recognised by Government.

The AMA is updating a My Health Record Guide for medical practitioners. It is, however, a practical guide to help doctors use the Record as part of their patient consultation workflow. Assistance for medical practitioners to meet their legal compliance requirements is a separate piece of work that needs to be addressed urgently.

Government must also be more proactive in working with specialist software providers to update their proprietary systems to achieve full interoperability with the My Health Record. Lack of interoperability that limits the functionality of the Record and requires time wasting work arounds is a deterrent for specialist participation.

Australian Medical Association

---

Finally, there is an opportunity to ensure that the existing, but temporary arrangements to exclude private sector and for profit entities (such as insurers) is made permanent. The current arrangements are for two years only, and outlined in a Framework, not the legislation.

The AMA would like the My Health Record to succeed because the clinical benefits are considerable. It has the capacity to save lives, to promote a more efficient and more effective health system, and to provide the information our world class medical practitioners need to better care for their patients. But the AMA recognises that no system is perfect. And systems will need to continue to improve and evolve. To that end, the AMA continues to support the My Health Record, and the proposed legislative amendments, while calling for a program of ongoing improvement. Our submission below expands on the points raised in this summary.



---

Australian Medical Association

---

The AMA's response to the Terms of Reference is set out below.

### The My Health Record

My Health Record (Record) is a secure national online repository (not unlike systems such as Dropbox) of patient clinical information. Each patient's individual record is essentially a digital folder which contains copies of already existing clinical documents which are prepared and uploaded by the patient's treating healthcare practitioners, sourced from current registers and information added by the patient. The clinical documents and data in a patient's My Health Record can include:

- ) shared health summaries (a medical summary uploaded by the doctor who provides ongoing care to the patient - usually a general practitioner);
- ) hospital discharge summaries;
- ) event summaries (information about specific patient encounters uploaded by health practitioners);
- ) specialist letters;
- ) eReferral letters;
- ) pathology and diagnostic imaging reports;
- ) prescription and dispense records; plus
- ) data auto uploaded from the Australian Immunisation Register, Australian Organ Donor Register, MBS/DVA and PBS;
- ) advance care planning documents; and
- ) details of a patient's emergency contacts.

It is important to emphasise that the original clinical documents and the doctor's own detailed notes continue to be stored in the doctor's own clinical practice software systems.

A patient's My Health Record can be accessed securely by another registered health practitioner at a future time and place, such as in an emergency. This creates the potential to improve the patient's care and safety given that access to this information might previously have been confined to the originating doctor's clinical system.

In addition, and unlike electronic health record systems existing in some countries, My Health Record also allows the patient to *access* to their record, giving them *choice* and *control* in their participation- the basis of the "My" in My Health Record.

Following largely negative media following the start of the three month opt-out period, the AMA President met with the Minister for Health on 31 July 2018 to call for the following four changes to help address the struggling My Health Record communication campaign, and implementation issues:

1. an extensive Government run education and communication campaign, aimed at the general public;

---

Australian Medical Association

---

2. changes to allow Record owners to cancel their Record permanently and delete all clinical content;
3. an extension of the opt-out period by one month to give citizens more time to make a considered decision about participating in the My Health Record; and
4. changes/deletions to Section 70 of the *My Health Record Act 2012* to require a warrant/court order before Records are disclosed by the System Operator to law enforcement bodies.

The Minister for Health agreed to all four AMA recommendations. The changes to s70 of the *My Health Record Act 2012* and the ability to cancel a Record permanently are given effect in the *My Health Records Amendment (Strengthening Privacy) Bill 2018*.

### **Expected benefits of the My Health Record system**

#### Better connected care

If healthcare was simple and predictable and if a patient only ever needed clinical treatment from a single, regular clinician, we would not need a My Health Record system. The patient's doctor would have all the patient's clinical history in their own clinical software on their desktop.

But patient's lives are more dynamic than this, and the Australian health system is more complex than this. Emergencies happen, patients will require medical treatment from different doctors for different reasons, at different times in different settings across the siloes of the Australian health system. As well as their GP, a patient might be treated by specialists, require hospital admissions, prosthetic implants, and be referred to different pathology labs and diagnostic imaging providers. Many patients will also be prescribed medications from one or more doctors.

Unfortunately, for all of the excellent care that is provided by each health practitioner, and in each health care setting. Communication and access to clinical information across health care settings, and between health care practitioners, remains slow, poor and often lacking in "interoperability". While the Record does not replace direct handovers or existing communication channels between clinicians, the clinical information in the Record can be accessed securely when it is needed most – at the point of care. The Record makes it easier to track the patient's journey through the health system- with the potential to improve their care. Many of the greatest failures in patient care and safety result when patients are required to move across the health system.

So, for example, a hospital emergency doctor will not have immediate access to critical information about a patient's medical history, including their medications and allergies, which is essentially trapped in the GP's clinical system. While the emergency doctor may attempt to contact the GP to ask them to fax (with all of its own privacy vulnerabilities) a copy of the patient's medical history, this becomes impossible after hours. The potential delay or lack of access to this critical information will mean that the emergency doctor will be "flying blind". These situations potentially compromise patient safety and care.

## Australian Medical Association

---

### Reduced medical harm

Areas where My Health Record has the potential to improve patient safety include:

#### *Medication related harm*

The Australian Commission of Safety and Quality in Health Care estimates medication related hospital admissions account for around 230,000 avoidable hospital admissions in Australia per annum. This is four times the number of admissions to hospital per annum due to motor vehicle accidents (57,000) and costs the health system around \$1.2b per annum<sup>1</sup>. Many of these admissions are caused because prescribers lack information about a patient's current medications and allergies at the point of care. Without a Record, prescribing doctors have no way of confirming the name and dose of medicines prescribed by the patient's other treating doctors. Many patients, especially the elderly, struggle to recall the name of their prescription medicines – particularly if they switch between a generic and an originator medication.

The Record, and in particular the "Medicines View" (a compilation of prescribed and dispensed medications) has the potential to reduce patient harm by allowing a prescriber a clearer view of the patient's medications and allergies.

#### *Anaphylaxis and allergic reactions*

Anaphylaxis and serious allergic reactions would be easier to avoid if details regarding patient allergies are documented in the patient's Record. During a previous Senate Finance and Public Administration References Committee Hearing on 15 September 2017 an AMA member, who is a general practitioner (GP), provided an excellent example of a life saved because his patient had a Patient Controlled Electronic Health Record (the precursor to the My Health Record). Quote from Hansard;

*'.. the hospital was able to access the information that was in that electronic record and not give a patient diabetic in a coma the usual antibiotic that would have been administered for sepsis. This person had a severe anaphylactic allergy to that antibiotic, and, if it had been given, would have been killed<sup>2</sup>.*

#### *Lack of access to hospital discharge letters*

Lack of timely access to clinical information by the health practitioners that treat a patient after hospital discharge is a well-known cause of serious harm to patients. Currently, discharge letters are usually only sent to the treating patient's GP by direct communication methods: post, fax or secure messaging. These forms of communication can be slow or fail to reach their intended recipient due to an incorrect address. In addition, if the next health practitioner the patient sees post discharge is not their usual GP, there is a heightened risk of harm because the alternative health provider has no way of knowing the clinical detail of the patient's recent hospital treatment.

---

<sup>1</sup> Australian Commission on Safety and Quality in Health Care (2013), Literature Review: Medication Safety in Australia ACSQHC Sydney

<sup>2</sup> Senate Finance and Public Administration References Committee, *Protection of personal Medicare information* Hearing 15 September 2017, Hansard [Proof Copy] p3

---

Australian Medical Association

---

In 2010 a WA Coronial inquest found that the inability of a remote community nurse to access critical information contained in a discharge letter was a factor in the death of a five-month-old boy from the Kimberly from meningitis. The boy had recently been admitted to a Perth hospital and had an identified immune deficiency. While a copy the discharge letter had been sent to the boy's paediatrician, the nurse, who was from a nearby clinic and had not until then been caring for the patient, responded in a less urgent manner to the child's initial symptoms partly because of her inability to access a discharge summary from Perth which should have greatly increased her level of concern<sup>3</sup>.

The upload of a discharge summary to My Health Record at the point of discharge allows immediate access to not only the usual GP, but also other doctors, health practitioners and health services who the patient may see, thereby increasing the probability that the patient will receive appropriate information and care.

#### Patient engagement in their own healthcare

AMA members report their patients often struggle to accurately recall important details about the nature and timing of medical treatments they have received. 40-80% of medical information provided by healthcare practitioners is forgotten immediately by patients. These include the names of specialists they have consulted, the name and doses of medicines prescribed, details about allergies, vaccination dates, health screening test dates, the name and location of diagnostic imaging and pathology providers, date of service and results.

Gaps in accurate treatment recall is not isolated to the elderly, and it increases greatly for patients who require complex treatments, multiple medicines, or have low literacy levels, English as a second language, or impaired memory.

Patient access to this information after they obtain care can contribute to their understanding of their health conditions - a key aspect of health literacy - and can increase treatment adherence and motivation to attend follow-up<sup>4</sup>. The Record will also empower patients to engage more actively with their treating clinicians about their own healthcare in ongoing interactions.

In addition, the Record allows patients to upload advance care planning documents and emergency contacts. In the event the patient presents in an emergency with impaired decision-making capacity (e.g. due to delirium, severe mental illness, or near death), treating doctors will have digital access to the patient's Record with details of their nominated substitute decision makers and wishes (including any refusal of care). Digital access to their advance care directives significantly increases the likelihood the emergency treatments aligns with their preferences when they have lost the ability to speak for themselves. It is a vast improvement to current paper based advanced care planning documents that are, for the most part, not available to a treating ambulance officer or emergency doctors.

---

<sup>3</sup>WA Department of Health *From death we learn 2014* Perth 2015, p 7-9

<sup>4</sup> Roy, PC & Kessels PhD JR, *Patients' memory for medical information*, Journal of Social Medicine Vol 96, no. 5, 2003, pp 219-222

---

Australian Medical Association

---

### Reduced duplication

The creation of a reliable digital patient history should also reduce the need to duplicate diagnostic imaging and pathology tests which a doctor is unable to access at the point of care. For example, patients attending hospital often need to have tests repeated because the treating doctor cannot confirm the laboratory or practice that provided the original test. The repetition of tests is not only wasteful and costly<sup>56-7</sup> it is also potentially harmful with regard to, for example, radiation exposure due to X-rays and CT Scans.

### **Impact on health providers**

The My Health Record's initial benefits accrue to patients. For health providers, the initial impact of connecting to the My Health Record System is an increase in practice costs. These costs relate to technical My Health Record installation and connection processes and the development and implementation of many new My Health Record specific policies within the health provider's practice which are necessary to satisfy compliance requirements (a sample is [here](#)). On top of this there are ongoing costs to upload and contribute information to a patient's My Health Record and new time costs incurred because patients are likely to rely on their doctor to explain the Record and understand the options available to them to adjust the privacy access settings to match their personal circumstance.

The efficiency benefits for providers – less time required to find clinical information about a patient -are not realised until participation levels (patients and other healthcare providers) reach critical mass in an opt in model.

### **The shift to an opt out system**

The AMA considers a My Health Record opt out model is the most effective way to realise the substantial clinical benefits of an electronic health record in the Australian health system.

The My Health Record has had a long and difficult history and there is now considerable Australian evidence to show opt in arrangements are very *unlikely* to achieve high levels of participation – amongst citizens and clinicians. When the Personally Controlled Electronic Health Record was launched as an opt in model in 2012, uptake remained low. As at 19 August 2018, only 24 per cent of Australian citizens had opted in<sup>8</sup>.

The evaluation of the 2016 My Health Record trials found statistically significant<sup>9</sup> higher levels of participation and use of My Health Record system in the two opt out trial sites (Nepean Blue Mountains and North Queensland), compared to the two opt in trial sites (Ballarat Hospital and

---

<sup>5</sup>Treasury officials estimate the duplication of tests will cost around \$123m by 2020-21

<sup>6</sup> Health 2017-18 Budget at a Glance, Commonwealth Department of Health  
<http://www.health.gov.au/internet/budget/publishing.nsf/Content/budget2017-glance.htm>

<sup>7</sup> Health 2017-18 Budget at a Glance, Commonwealth Department of Health  
<http://www.health.gov.au/internet/budget/publishing.nsf/Content/budget2017-glance.htm>

<sup>8</sup> Australian Digital Health Agency 'My Health Record Statistics', 19 August 2018

<sup>9</sup> Siggins Miller 2016 Evaluation of the Participation Trials for the My Health Record Final Report, pv

---

Australian Medical Association

---

Perth Western Australia), plus the rest of Australia where opt in still applied. In both opt out trial sites only two (1.9) per cent opted out.

In the Nepean Blue Mountains opt out trial site, the proportion of computerised general practices registered to participate in the My Health Record system increased from 40 percent pre-trial to 80 percent. The proportion of general practitioners uploading shared health summaries increased from 15 percent to 70 percent<sup>10</sup>.

The majority of patients want their doctors to have access to their clinical information, so they can receive the best possible care. In an opt in system, adoption of the Record requires the patient to initiate the effort to register. The shift to opt out removes this registration burden from the patient.

If the switch to opt out arrangements creates a sustained increase in the My Health Record participation rate the incentive for clinicians to adopt the My Health Record also increases.

Evaluation of the NT electronic health record system (My eHealth Record)<sup>11</sup>, to some degree the prototype for My Health Record, found that:

*Achieving 50% registration overall appears to be associated with the tipping point at which the MyEHR service reached critical mass, and usage increased markedly...*

*Achieving critical mass has meant the MyEHR service has become embedded into routine clinical and administrative workflow.*

## **Privacy and Security**

Following the launch of the three month opt out period, the immediate media response was overwhelmingly negative. Many of the concerns and criticisms of the My Health Record were related to privacy and the vulnerability of the system to unauthorised or unanticipated access.

The AMA notes doctors in private practice are already subject to the *Privacy Act 1988* and the Australian Privacy Principles, and professional standards. Healthcare organisations already set controls over access to patient information for individuals performing different roles within healthcare provider organisations. The My Health Record imposes security and privacy standards over and above these existing requirements.

Any software that connects to the My Health Record system must be secure, encrypted and certified as conformant. The software is subject to automated checks to ensure it maintains conformity standards. Authority to write in a Record is only available to health providers via approved, conformant clinical software.

---

<sup>10</sup> Nepean Blue Mountains Primary Health Network: *Learnings from the My Health Record Opt Out Trial* p4

<sup>11</sup> My eHealth Record to National eHealth Record, Transition Impact Evaluation Phase 1 evaluation report, 10 July 2015

---

Australian Medical Association

---

Conformant clinical software also assigns unique staff member identification codes and records each time a staff member accesses the My Health Record system. A log is automatically generated to record each time the My Health Record is accessed by a health provider *organisation*. These logs mean Record owners can see which organisations have accessed their Record in real time and the System Operator can drill down to identify which Individual Healthcare Identifier was used. The criminal penalties plus the ability to trace the Healthcare Identifier used each time a Record is accessed, will act as robust deterrents against unlawful access.

This level of transparency is arguably greater than current arrangements whereby a staff member in a medical practice can call a pathology provider and obtain copies of pathology tests for a particular patient of the practice. These current arrangements have no formal mechanisms to alert the patient their health information has been requested by, and provided to, a staff member in a medical practice.

Unauthorised access via cyber-attack is an undisputed risk for large health databases. Yet, so too is there risk of cyber-attack to the same health data stored in existing databases such as health insurers, large hospitals, MBS and PBS data. In 2018 we live in a digitised world.

In addition, although not generally acknowledged, paper-based files, and the common practice of faxing health information, are also subject to privacy failures – but because they are common practice in the current health system, this is generally not commented on by the broader media and public.

The privacy protections available to Record owners add further security to patient data. Individual Record owners can adjust these privacy settings to suit their data sharing risk profile.

Record owners can instruct their health provider at the point of care, not to upload information they consider sensitive. They can put a Record access code across their whole record or an individual document so only the providers who have been given the access pin number can see them. Record owners can also set up alerts to receive a text or email notification if their Record is accessed by a new health provider. Record owners can remove documents from their Record or opt out at any time. See ADHA information on [My Health Record Access Controls and 'How to' instructions](#).



### **Case Study**

A nurse who works in a large health organisation, such as a hospital, with many colleagues who are authorised My Health Record users, may wish to prevent the risk their record could be browsed by colleagues who are not involved in providing her with treatment. Even though this action is unlawful under the My Health Record Act 2012, and the individual responsible can be traced, the nurse can use the Advanced Access controls to reduce the perceived risk of unauthorised access to zero. For example, she can put an access code across her whole record to block access to all health providers other than her treating health practitioners to whom she gives the access pin.

A privacy concern for some consumers is the retention of their My Health Health Record data after they opt out. This is resolved in the *My Health Records Amendment (Strengthening Privacy) Bill 2018* by providing for a 'hard delete' if a patient cancels their Record. The AMA is satisfied the permanent deletion of a Record after it is created, provides citizens with a genuine choice -they can retain the Record created by Government on their behalf, or withdraw completely. The hard delete facilitates all the benefits of opt out (removing the administrative effort to create a Record) while giving citizens the option to withdraw completely at a future date with no retention of data. Although not yet widely understood, this is an important and reassuring change as it effectively removes the time pressure on citizens to reach an informed view about participating in the My Health Record before the end of the opt out period.

Some commentators consider there are patient privacy risks generated by the decision to use the default access settings for new Records created by Government in the shift to opt out arrangements. The AMA notes, a decision to impose maximum security settings as a default for all new My Health Records created by government under an opt out model, would mean all clinical information uploaded to the patient's My Health Record would remain invisible to the patient's treating healthcare providers unless the patient creates myGov account and *opts into* their Record to relax these privacy settings. The opt in approach has demonstrably failed in Australia to achieve a critical mass adoption necessary to create a self-sustaining My Health Record System with all the potential clinical benefits it offers.

### **Permitted disclosures by the System Operator to enforcement bodies or for enforcement related activities**

Another prevailing privacy concern raised in the media during the opt out period was the potential for law enforcement and other government agencies to access an individual's My Health Record data.



---

Australian Medical Association

---

The *My Health Records Amendment (Strengthening Privacy) Bill 2018* (Bill) also substantially addresses these concerns. In particular, the Bill:

- ) Amends section 65 so that the ability to disclose where “authorised or required by law” only applies to four laws.
- ) Introduces a new section 69A which overrides any other Commonwealth, State and Territory laws that allow police or other government bodies to access records. Any such requests must be personally endorsed by a judicial officer and can only be directed to the System Operator.
- ) Deletes sections 70(1) and (2) (being the provisions which allowed access by law enforcement).
- ) Subjects section 70(3) to additional protections.

These controls are substantially tighter than the controls that apply under the *Privacy Act 1988* (Cth) to patient data stored in the clinician’s own patient records. For example, Australian Privacy Principle 6.2(b) allows a record holder to produce a patient’s record where this is “required or authorised by or under an Australian law or a court/ tribunal order”. The equivalent provisions of the *My Health Records Act* – sections 65 (as amended) and 69 – only authorise or require access in very limited circumstances.

### **The administration of the My Health Record system roll-out**

The ADHA has developed extensive, informative guides for consumers and providers to explain what the My Health Record System is, how it operates, how it will affect individuals, and how they can use it. There are also helpful ‘how to’ videos to demonstrate the implementation of privacy settings.

For health practitioners there are simulations to demonstrate how the Record integrates with clinical software packages and high-level guides to assist health providers understand the My Health Record compliance standards. These resources are available on the ADHA website and easily located via an effective search function.

Health providers are at different stages of readiness to connect to the My Health Record and integrate it into the workflow of their practice. The ADHA has focussed on getting general practices connected to and using My Health Record through ePIP incentives. Specialists have not had access to similar support.

Many Specialists are still deterred from connecting to the My Health Record because their clinical software providers have not invested in the upgrades necessary to provide seamless interoperability with the My Health Record System. One AMA specialist who uses a leading software program and did try and connect to the My Health Record reported error rates of 32 per cent with event uploads to a patient’s Record. The program, and some other medical practice software products, do not provide the option to upload Specialist letters, despite this being a

---

Australian Medical Association

---

function that My Health Record is designed for.<sup>12</sup> To work around this limitation, the specialist would need to create an Event Summary to cover the issues summarised in the Specialist letter *and* write a separate Specialist letter required as part of her usual workflow. These time consuming workarounds deter Specialists from connecting to the My Health Record.

Government intervention is needed to break the catch 22 cycle where lack of functionality and usability deters Specialists from using the My Health Record, and low rates of use amongst Specialists deters proprietary software providers from investing in software upgrades. Specialists also need specific support and training from the ADHA to understand the My Health Record, connect to the My Health Record System and integrate it into their clinical workflow. It is unwise for ADHA to assume Specialists' participation will occur organically.

ADHA assume that doctors as a group, understand what the My Health Record is, it's capabilities, it's limitations, and the obligations. AMA members report that many blogs contain misinformation about the Record, and doctors are struggling to understand their legally binding compliance obligations once they connect to the My Health Record System. Much more direct assistance for doctors is required.

The ADHA strategy to tap into the wide network of government and non-government service providers to promulgate My Health Record information to the groups they service, will need more time and Government investment to succeed. The current use of non-traditional and social media to raise awareness – especially amongst 14-17 year olds - will also be important to get right.

While the networking approach might succeed in the longer term, it did not prepare the Australian public en-masse for the opt out announcement.

The overwhelming negative media response that zeroed in on every perceived risk of the My Health Record created a perception the My Health Record risk to privacy was too great compared to the benefits. The media response, however, was in some ways not surprising. The My Health Record privacy infrastructure is complex and too difficult to effectively communicate in a truncated manner in the immediate aftermath of the opt out announcement. Ironically, the Record is complex because this is necessary to protect patient privacy.

This is why the AMA always called for a more extensive public communications campaign on top of the current efforts to promulgate awareness and understanding via social media channels and health networks.

Government must do more to build the case for opt out in the mind of the citizens. It is their health data, and should be available for them to use for their benefit.

There may be an opportunity to reset the media campaign if the *My Health Records Amendment (Strengthening Privacy) Bill 2012* is passed by Parliament. One of the key amendments will allow My Health Records to be deleted permanently. This creates a de-facto unlimited opt out period

---

<sup>12</sup> At the time of writing the following software packages used by specialists, do not have the functionality to upload Specialist Letters - Genie Solutions, ZedMed, The Practice, Clarity. For a full list please see: [https://www.myhealthrecord.gov.au/sites/g/files/net5181/f/register\\_summary\\_10nov17\\_0.pdf?v=1522292447](https://www.myhealthrecord.gov.au/sites/g/files/net5181/f/register_summary_10nov17_0.pdf?v=1522292447)

## Australian Medical Association

---

in which a long-term public education campaign can explain the Record, the benefits, the privacy levers to control what is visible and who can access the Record.

Substantial parallel effort will be required to continue to build My Health Record knowledge and skills of first to know agencies who work with vulnerable groups in a 'train the trainer' model so they can assist their clients to manage the Record according to their circumstance and risk profile.

For example, young people 14-17 years become potentially vulnerable in an opt out environment. The AMA understands the My Health Record system allows young people to take control of their own Record from the age of 14 but this process does not occur automatically. The young person must find out this is an option and initiate it. Only then can they apply their privacy settings and decide if they want their parents to access their Record. If they remain unaware and don't take control of their Record, their Authorised Representative (parent or legally recognised carer) will continue to manage it on their behalf until they turn 18, although the record will not contain PBS or MBS data. See [OAIC fact sheet](#) for more details.

Individuals suffering domestic violence are another at risk group under My Health Record opt out arrangements – unless they understand the options available in the My Health Record to manage their risks and privacy. For example, if a woman lives with an abusive partner he may, either through threat or stealth, access her My Health Record against her wishes. In a different scenario, some media commentators have noted if a woman is in hiding and the abusive partner has non-custodial shared parenting responsibilities for their child(ren), he can access the child(ren)'s existing My Health Record or create a new Record for the child, as the child's Nominated or Authorised Representative. The location of the health services listed in the child's Record will then potentially expose the woman's area of residence.

The AMA understands at risk parents in these circumstances can call the System Operator and either opt out or immediately suspend a Record if the child has one. This suspends access to all Representatives. Parents can also request suspension during the opt out period to ensure a Record for the child is never created – even if the other parent requests one. These systems will, however, will be of little benefit if the people at risk are unaware or do not know how they can neutralise the potential risk to their privacy and personal security. There is a responsibility for government to reach this at risk group directly before the end of the opt out period to assist them remain safe.

The AMA has no expertise in the processes used by other government departments to keep individuals safe when they are at risk from violent ex-partners, but simply notes this problem is not new. The My Health Record should be, at minimum, consistent with the safeguards in place already for the same type of information (in this example, MBS/PBS) when it is stored and accessed via other government portals/initiatives (such as myGov or Medicare).

Australian Medical Association

---

## Further improvements to the My Health Record System

### Unstructured data

The lack of My Health Record data structure limits the integrity and searchability of important health information, in a patient's Record. Over time, the utility of the My Health Record will be considerably increased if this is addressed.

### Prostheses data

In the absence of a national prostheses registry, there is a need, and an opportunity to create a dedicated, searchable section in the My Health Record to record patient prostheses data. This facility would simplify prostheses recalls, and create routine efficiencies and improved patient care. For example, a radiologist could make a quick informed decision about whether it is safe to provide a patient with an urgent MRI. Surgeons would be able to pre-determine the type of prostheses screw-driver needed during a planned operation to remove screws from a prosthetic previously inserted into the patient by another doctor. This would avoid the waste and patient harm that could otherwise be created in situations where a patient is in theatre and under general anaesthetic but the correct prostheses screwdriver is unavailable.

### Disclosure of My Health Record data to researchers and commercial interests (Secondary Use Framework)

The AMA shares the media concern that health insurers should not have access to My Health Record data. Their interest in this data presents a clear conflict of interest between the financial benefit of avoiding fund members who are high risk claimants and their obligations to abide by the principles of community rating. The *My Health Records Amendment (Strengthening Privacy) Bill 2018* presents an opportunity for a further amendment to the Bill to to remove all doubt data sharing with health insurers will occur at some point in the future.

Although the AMA understands the *Healthcare Identifiers Act 2010* appears to prohibit health insurers from directly access to a patient's My Health Record, Section 15(ma) of the *My Health Record Act 2012* permits the ADHA, as the System Operator, to *prepare and provide de-identified data for research or public health purposes*. The first edition of the Secondary Use of My Health Record Framework was released in May 2018. Under this Framework de-identified data will not be released for commercial or non-health related purposes. Equally important, insurance agencies (including health insurers) are prohibited from accessing My Health Record data for secondary purposes.

It is, however, problematic that the Framework parameters are **short term**. The Department of Health has already foreshadowed their intention to review the Framework parameters two years after the first release of data, planned for 2020. Health insurer access has been identified as a priority in this first review. The frequency and type of amendments to the Secondary Use Framework in the future is not bound by any enforceable restrictions. It is effectively, at the Minister's discretion.

The AMA would be very concerned if health insurers obtained access to de-identified My Health Record data in the future – whether in the first Framework review or thereafter. The considerable membership data the health insurer already holds, will likely allow them to create a matched,

---

Australian Medical Association

---

identified data set covering all health services utilized by the patient (admitted/non-admitted). Existing protections to prevent unlawful discrimination based on health risk and claims history would be virtually impossible to enforce. This would be a very poor outcome for existing insured patients and those who apply for health insurance in the future, and the AMA view is that a more enduring and permanent solution is needed to address this issue, now. As the AMA outlined to the Committee, this could be a legislative amendment.

### **Conclusion**

The AMA welcomes the Committee's inquiry as an opportunity to talk about the substantial benefits that could result for patient and practitioner alike in the use of the My Health Record. It is also an opportunity to highlight the further improvements that can be made.

Likewise, the AMA welcomes the Senate Community Affairs Legislative Committee inquiry into the proposed amendments.

It is the view of the AMA that the proposed amendments must be read within the context of the My Health Record, its operation and system design and inbuilt protections – and that equally, any inquiry into the My Health Record at a broader level should consider the proposed legislative framework.

For that reason, the AMA has submitted both submissions to both inquiries and is happy to answer any questions the Committees may have.

14 September 2018

### **Contact**

Mr Luke Toy  
Director, Medical Practice Section  
Australian Medical Association