Australian Government

Department of Health

Submission to the Senate Standing Committee on Community Affairs: My Health Records Amendment (Strengthening Privacy) Bill 2018

14 September 2018

1. Introduction

Purpose of the Act

The *My Health Records Act 2012* (MHR Act) provides for the establishment and operation of the My Health Record system which will help address the fragmentation of health information in Australia by allowing a healthcare recipient and their healthcare providers to more easily access their key health information. This will result in:

- improved continuity of care for healthcare recipients accessing multiple healthcare providers by enabling key health information to be available when and where it is needed for safe ongoing care;
- access to consolidated key health information about a healthcare recipient's medicines, leading to safer and more effective medication management and reductions in avoidable medication-based adverse events;
- enabling healthcare recipients to participate more actively in their own healthcare through improved access to their health information;
- improved diagnostic and treatment capabilities through enhanced access to health information; and
- improved care coordination for healthcare recipients with chronic or complex conditions by enabling the healthcare recipient's healthcare team to make better-informed decisions at the point of care.

The MHR Act establishes:

- the role and functions of the System Operator (the Australian Digital Health Agency since July 2016);
- a registration framework for healthcare recipients, and entities including healthcare provider organisations, to participate in the My Health Record system; and
- a privacy framework, which draws heavily on the use and disclosure provisions of the *Privacy Act 1988* (Privacy Act), specifying which entities can access and use information in the system, and a penalty regime that can be imposed as a result of improper use of this information.[1]

Legislative framework

The MHR Act operates alongside numerous other Australian laws to support the My Health Record system, and was developed to work together with state and territory

[1] Penalties for misuse of health information under the MHR Act are already significantly tougher than those in the Privacy Act.

privacy and information laws as much as possible.[2] Subsection 41(4) and subclause 9(3) of Schedule 1 provide for certain state and territory laws to continue to have effect regarding uploading of certain health information onto the My Health Record system.

Information stored in the My Health Record system is protected under the MHR Act, including strong civil and criminal penalties for misuse. Information stored outside of the My Health Record system – for example, information that has been downloaded from the system – is subject to existing state and territory laws and, in some cases, the Privacy Act.

The *Healthcare Identifiers Act 2010* regulates the handling of healthcare identifiers, which are a foundation of the My Health Record system.

The Privacy Act regulates the handling of personal information, including access to and correction of that information, and the Australian Information Commissioner has various enforcement and investigative powers in respect of the My Health Record system.

Each of these Acts imposes serious penalties for the unauthorised collection, use or disclosure of information.

The My Health Record legislative framework also comprises a range of subordinate legislation:

- The *My Health Records Regulation 2012* specifies additional details regarding the operation of the My Health Record system including preserved laws, and prescribes the Australian Digital Health Agency as the System Operator.

- The *Healthcare Identifiers Regulations 2010* specify additional operational details regarding the assignment, collection, use, adoption and disclosure of healthcare identifiers.

- A suite of My Health Records Rules (*My Health Records Rule 2016, My Health Records (Assisted Registration) Rule 2015*, *My Health Records (National Application) Rules 2017* and *My Health Records (Opt-out Trials) Rule 2016)* provide additional requirements for participation in the My Health Record system, further prescribe how the system should operate, and provide for opt-out participation arrangements.

[2] While the MHR Act normally overrides a state or territory law that cannot operate concurrently with the MHR Act, some of those laws have been prescribed to remain in force (referred to as 'preserved laws'). Those preserved laws relate to the disclosure of a healthcare recipient's identity or confidential information in connection with certain notifiable diseases, and require a healthcare recipient's consent to be obtained in a particular manner in order for the information to be uploaded to the My Health Record system.

- The *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* set out the Information Commissioner's general approach to the exercise of enforcement powers and investigative powers under both the MHR Act and Privacy Act.

The Australian Digital Health Agency, which is the System Operator, was established by the *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016* as a corporate Commonwealth entity which is legally separate from the Commonwealth.

2. Background

Changes to the Act

The Personally Controlled Electronic Health Records Bill 2011 was introduced into Parliament on 23 November 2011 and was soon after referred for an inquiry by the Community Affairs Legislation Committee. The report of that inquiry recommended several changes to the Bill which were largely made before the Bill was passed.[3] These changes were:

- to specify that the statutory review include consideration of the opt-in design and the feasibility and appropriateness of transitioning to an opt-out system;
- to make clear that rules could be made to enhance healthcare recipient privacy;
- to require community consultation in determining default access controls; and
- to explicitly specify that a function of the System Operator is the use of de-identified information for research and public health purposes.

The Bill was enacted on 26 June 2012.

The Health Legislation Amendment (eHealth) Bill 2015 was introduced into Parliament on 17 September 2015 to amend the *Personally Controlled Electronic Health Records Act 2012* to implement the recommendations of reviews of the Personally Controlled Electronic Health Record and the Healthcare Identifiers Service. These amendments included enabling opt-out participation arrangements to operate in future and changing the system's name to My Health Record.

This Bill was referred for an inquiry by the Community Affairs Legislation Committee. The report of that inquiry recommended the Department consider recommendations made by the Office of the Australian Information Commissioner regarding privacy in developing the public awareness campaign about the opt-out trials in 2016. The Bill was subsequently passed and enacted on 26 November 2015,

[3] The change recommended but not adopted related to the inclusion of preventative health in the definition of "healthcare" – changes were subsequently made to this definition in 2015.

and the Commissioner's recommendations informed the development and implementation of the participation trial communications in 2016.

Following commencement of the national opt-out period on 16 July 2018, some stakeholders expressed concerns about the privacy of information in the My Health Record system, particularly the ability for law enforcement agencies to obtain this information and the requirement to retain information regardless of whether a healthcare recipient chooses to cancel their My Health Record. The Minister for Health, the Hon Greg Hunt MP, addressed these concerns by consulting with the Australian Medical Association, Royal Australian College of General Practitioners, Office of the Australian Information Commissioner and Human Rights Commissioner, and then introducing the My Health Records (Strengthening Privacy) Bill 2018 on 22 August 2018. The proposed changes would see the My Health Record privacy protections strengthened by further restricting the circumstances in which information can be disclosed, and requiring the destruction of information in the National Repositories Service of healthcare recipients who choose to cancel or have already cancelled their My Health Record.

3. Retention of information

Current retention arrangements

The My Health Record system is a distributed system – it draws information from participating repositories[4] (such as that operated by the Chief Executive Medicare) to compile a healthcare recipient's My Health Record. It also draws information from the National Repositories Service which is operated by the System Operator to ensure a minimum critical set of health information is available for a My Health Record, such as shared health summaries, event summaries, discharge summaries and specialist letters, and to hold information not stored elsewhere, such as a healthcare recipient's own health summary and health notes.

Section 17 of the MHR Act currently specifies the retention arrangements for information in the National Repositories Service. The System Operator must retain records uploaded to the National Repositories Service from when the record is first uploaded until 30 years after the death of the healthcare recipient. If the date of death of the healthcare recipient is unknown, the record must be retained until 130 years after the date of birth of the healthcare recipient.

This retention requirement applies whether or not a healthcare recipient remains registered, that is, if they've elected to cancel their My Health Record the System Operator is still required to retain the information already uploaded. When a healthcare recipient cancels their My Health Record, their My Health Record

[4] A repository is essentially a store of information. Health information is held in many repositories around Australia, operated by a mix of public and private sector organisations. An operator of a repository can register their repository to participate in the My Health Record system, thereby making information in that repository available for inclusion in a healthcare recipient's My Health Record (if they have one).

information is no longer available to any entity other than in specific circumstances (such as to lessen or prevent a serious threat to public health).

The retention requirement was implemented in this manner for a range of reasons, including to:

- provide for medico-legal needs, such as if a clinical decision is made on the basis of My Health Record information and the decision is being legally challenged;
- provide a long-term source of information that could be used to inform and improve health services (largely in de-identified form; only in identified form if consented to by the healthcare recipient); and
- provide that if a healthcare recipient changed their mind and decided to re-register for a My Health Record, they would have access to the information that existed before they previously cancelled it.

While the System Operator must comply with this retention requirement, the requirement does not apply to other repositories participating in the system – those repositories are already subject to Commonwealth, state or territory health information retention requirements.

Proposed changes

The My Health Records (Strengthening Privacy) Bill 2018 proposes to amend section 17 so that the System Operator would no longer be required to retain a healthcare recipient's health information which is in the National Repositories Service if the healthcare recipient has cancelled their My Health Record, and would in fact be required to promptly destroy that information.

This change would align the treatment of people who choose to opt-out of having a My Health Record with the treatment of people who get a My Health Record but decide at any time to cancel it – namely, that the System Operator will not hold any health information about them.

There are exceptions to this requirement to destroy information, specifically if the information is being lawfully obtained by an entity under amended section 65, section 69 or new section 69A – that is, the System Operator has received a court order or an order by a judicial officer for the disclosure of that information, or a request by the Australian Information Commissioner, Ombudsman or Auditor-General for the information, or a court order instructing the System Operator not to destroy the information (for example, until certain related legal proceedings have ended). If one of these exceptions applies, the System Operator would be required to destroy the information promptly after that matter has concluded (for example, after the information has been disclosed as ordered).

This requirement would not apply to any other repositories participating in the My Health Record system. Those entities are holding the healthcare recipient's

information for other purposes, such as to operate the Pharmaceutical Benefits Scheme or to provide a prescription exchange service, and they would continue to retain that information in accordance with their own retention requirements. This means that if a healthcare recipient subsequently changes their mind and decides to get a My Health Record, some information may still be available from those other repositories to include in the healthcare recipient's new My Health Record (if those other repositories haven't already destroyed the information in accordance with their own retention requirements).

The System Operator would be required to destroy all of the healthcare recipient's health information that is held in the National Repositories Service, with the exception of some minimal information required for basic operational and audit purposes – specifically, the System Operator could only retain the healthcare recipient's name and healthcare identifier, the name and healthcare of the healthcare recipient's authorised representative if they requested the cancellation, and the date the My Health Record is cancelled. This would ensure that, for example, if the System Operator is audited, it can identify why information has been destroyed and the person who requested cancellation of the My Health Record (and triggered the destruction of information).

What does this mean?

If a healthcare recipient (or their authorised representative) requests that their My Health Record be cancelled, the System Operator would be required to promptly destroy any health information uploaded to the National Repositories Service about that healthcare recipient. In practice, this destruction would occur 24 to 48 hours after the My Health Record is cancelled (to allow for system functionality). This requirement would apply to any healthcare recipient who has cancelled their My Health Record since it began operating on 1 July 2012 (excluding those who previously cancelled but have re-registered before the amended section 17 takes effect).

The System Operator would continue to be required to retain information uploaded to the National Repositories Service about a registered healthcare recipient (i.e. someone who has not cancelled their My Health Record) until 30 years after the healthcare recipient's death (or if the date of death is not known, for 130 years from the healthcare recipient's date of birth).

Commencement

The changes would come into effect the day after the My Health Records Amendment (Strengthening Privacy) Bill 2018 receives Royal Assent. This would mean that anyone who has ever cancelled their My Health Record (and not changed their mind and re-registered) would have their health information permanently deleted from the National Repositories Service within a matter of days of Royal Assent.

The Australian Digital Health Agency has advised the Department that it is preparing the functionality to effect these deletions to be in place in early December 2018. If the Bill is passed during the 2018 Spring sitting, the requirement would be in place in advance of the creation of My Health Records on 13 December 2018 resulting from opt-out implementation – that is, if anyone has a My Health Record created and doesn't want one, they would able to immediately cancel it and any health information that has been uploaded to the National Repositories Service (if any) would be deleted permanently.

Implications

Given the distributed nature of the My Health Record system, much of the information available in a My Health Record is a copy of information held in other repositories and in clinical systems, but not all of it. As noted previously, the National Repositories Service holds information which is not stored elsewhere, such as a healthcare recipient's own health summary and healthcare recipient-only notes.

This means that when a healthcare recipient cancels their My Health Record, any original information held only in the National Repositories Service would be destroyed and therefore lost.

4. Disclosure of information

Current disclosure arrangements

The My Health Record system is likely to be a richer resource for health information than other systems in Australia given that it is drawing information together from various repositories. For this reason, the My Health Record privacy framework was developed to be stronger than other laws that apply to health information – for example, unlike the Privacy Act, the MHR Act imposes criminal penalties for the misuse of health information.

The privacy framework was developed to reflect the same handling of personal information permitted by the Privacy Act with some additional limitations to reflect the unique nature of the My Health Record system and the sensitive information that can be held in a My Health Record.

A person or organisation can only collect, use or disclose health information in a healthcare recipient's My Health Record if they are authorised to do so by Division 2 of Part 4 of the MHR Act. The authorisations provided by the MHR Act include permitting:

- a participant in the My Health Record system (i.e. System Operator, registered healthcare provider organisation, registered contracted service provider, registered portal operator and registered repository operator) to collect, use and disclose information if required or authorised to do so by another Australian law (section 65);

- the System Operator to disclose information if ordered to do so by a court or tribunal if the proceedings relate to the MHR Act, to unauthorised My Health Record access or to healthcare provider indemnity cover, or with the consent of the healthcare recipient – in this case the System Operator is required to comply with the order (section 69);

- the System Operator to disclose information if ordered to do so by a coroner – in this case the System Operator is required to comply with the order (section 69);

- the System Operator to use or disclose information if he or she considers it is reasonably necessary for an enforcement body to undertake prescribed enforcement activities[5] (section 70); and

- the System Operator to use or disclose information if he or she suspects unlawful activity in relation to the System Operator's functions and reasonably believes that use or disclosure of the information is necessary for investigation or reporting the activity to authorities (section 70).

Proposed changes

The My Health Records (Strengthening Privacy) Bill 2018 proposes to amend some of the authorisations provided at Division 2 of Part 4 of the MHR Act to further limit the circumstances in which health information in a healthcare recipient's My Health Record may be collected, used or disclosed.

Under the changes proposed to section 65, it would generally no longer be sufficient for a participant in the My Health Record system to rely on other state, territory or Commonwealth laws to access health information in a healthcare recipient's My Health Record. The purpose of this amendment is to restrict, as far as if practicable and in accordance with good governance, the other laws that are able to require or authorise access to health information stored in the My Health Record system. State and territory laws will no longer be able to be relied upon to require or authorise access. Only a very limited range of Commonwealth laws will be able to require or authorise access to health information – that is, laws which are necessary for the proper administration and oversight of the system. Amended section 65 would not override the laws governing the Auditor-General, the Ombudsman and the Australian Information Commissioner (where in the latter case the law requires or authorises the collection, use or disclosure of information for the purposes of

[5] The prescribed enforcement activities are:
(a) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
(b) the enforcement of laws relating to the confiscation of the proceeds of crime;
(c) the protection of the public revenue;
(d) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
(e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

performing the Information Commissioner's privacy functions in relation to the My Health Record system), which means that their statutory powers would remain in effect authorising them to collect health information in a healthcare recipient's My Health Record. These entities are critical for appropriate oversight of government functions and transparency, in particular the Information Commissioner which is the regulator of the My Health Record system.

Under amended section 65, bodies which previously relied on section 65 to access health information in the My Health Record system (other than the Auditor-General, Information Commissioner and the Ombudsman) would need to instead rely on the other authorisations in Part 4 of Division 2 of the MHR Act if they wish to continue accessing information – for example, they would need to rely on section 69 or on new section 69A.

Section 69 already enables a court to require health information in a healthcare recipient's My Health Record to be disclosed by the System Operator under an order. New section 69A would enable entities with statutory powers (to require or collect information from another entity) to take steps to obtain the information by applying to a judicial officer for an order for the production of the information.

New section 69A would require the System Operator to disclose health information in a healthcare recipient's My Health Record to such an entity only if a judicial officer has issued an order requiring the disclosure of the information. An order of this type may only be issued if prescribed criteria are met – specifically:

- the entity has satisfied the judicial officer that the entity has a power under a Commonwealth, state or territory law to require a person to provide information, or its officers are authorised to execute warrants;

- the entity has satisfied the judicial officer that the entity has exercised or purported to exercise this power (while the effect of amended section 65 would be that the entity cannot obtain the information by exercising this power in the absence of new section 69A, there may be other obligations associated with the exercise of this power that should be satisfied, such as reporting requirements or due diligence);

- the entity has satisfied the judicial officer that the disclosure of information is reasonably necessary for the entity to carry out its functions;

- the entity has satisfied the judicial officer that the requested information cannot be obtained from another source;

- the judicial officer is satisfied that in considering the entity's need for the information and the healthcare recipient's privacy, the disclosure of information would not, on balance, unreasonably interfere with the healthcare recipient's privacy.

The judicial officer may seek additional information from the entity in order to make a decision, and is not under any obligation to issue such an order. If the judicial officer decides to issue an order, the order must be reasonably detailed in terms of the information it relates to and the healthcare recipient to which that information relates.

In effect, this new section 69A reflects the unique aspects of My Health Record (including it being a rich data source, but also one where much of the information it holds is also held by other entities), the objectives of the MHR Act and the need to engender trust in the system and its protection of sensitive information. The amendments ensure that disclosure of My Health Record information is an option of last resort and subject to meeting a high bar.

In keeping with the amendments proposed above, amended section 70 would provide the System Operator with authority to release a minimal amount of information only if he or she has reason to suspect that unlawful activity relating to the System Operator's functions (as specified by section 15) has been, is being or may be engaged in, and the System Operator reasonably believes that the disclosure is necessary for investigation or reporting purposes.

The information released would only be enough for the relevant person or authority (for example, the Australian Federal Police) to consider the activity and, if necessary, seek an order for the information under new section 69A.

The proposed changes would effectively oblige any entity that is not participating in the My Health Record system that would otherwise have powers to require disclosure of health information held in the My Health Record system to obtain an order by a judicial officer to collect that information.

The decision to adopt an order by a judicial officer as the vehicle for entities to obtain this information responds to public concerns raised since the commencement of the opt-out period on 16 July 2018. It also reflects the policy of the Australian Digital Health Agency and announcements by the Minister for Health,
the Hon Greg Hunt MP, that information would not be released without a court order. The proposed amendment ensures that the criteria described above can be applied to the judicial officer's decision-making process, without interfering with the exercise of judicial power by Commonwealth and state courts under the Constitution.

What does this mean?

The circumstances in which a participant in the My Health Record system may collect, use or disclose health information in a My Health Record, and in which an entity may be able to obtain this information, would be further restricted.

Entities with statutory powers outside of the MHR Act to require information for certain purposes would no longer be able to rely on those powers in respect of health information in a My Health Record. Instead, they would need to obtain an order

from a judicial officer under the MHR Act in order to obtain the information. These changes apply to participants in the My Health Record system and to other entities making requests of those participants. To the extent that participants are currently relying on section 65 to undertake certain activities, they would no longer be able to do so unless they obtain an order by a judicial officer. It should be noted that to date no My Health Record information has ever been released under section 65.

Similarly, enforcement bodies (as prescribed by the Privacy Act) would no longer be able to obtain health information in a My Health Record for the purpose of undertaking an enforcement-related activity unless they obtain an order by a judicial officer under new section 69A.

Further, the System Operator would no longer be able to disclose health information in a My Health Record if he or she considered it was necessary for the purpose of reporting an unlawful activity relating to the System Operator's functions. The System Operator could only disclose sufficient information to allow the relevant person or authority (to which it was reporting) to determine whether it needed to obtain the information to investigate the matter. If the person or authority determined that it did need to obtain the information, it would need to obtain an order by a judicial officer in order to obtain further information for that purpose.

The other authorisations set out in Division 2 of Part 4 of the MHR Act – such as collection, use and disclosure for the purpose of providing healthcare to the healthcare recipient, for the purpose of operating the My Health Record system or for any purpose with the consent of the healthcare recipient – are not affected by the changes proposed by the My Health Records (Strengthening Privacy) Bill 2018.

Commencement

The changes would come into effect the day after the My Health Records Amendment (Strengthening Privacy) Bill 2018 receives Royal Assent.