Australian Government
Office of the Australian Information Commissioner

OAIC Submission

Senate Community Affairs References Committee - Inquiry into the My Health Record system

oaic.gov.au

OAIC

Contents

Inquiry into the My Health Record system

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide this submission to the Senate Community Affairs References Committee's inquiry into the My Health Record system.

The My Health Record system commenced in 2012 as an opt-in express consent based model where an individual needed to register in order to get their My Health Record.[1] Since the Government decision to move to an opt-out approach was made,[2] the OAIC has emphasised the need for individuals to be informed in order to make a proactive decision about whether they wish to opt-out of the system, are otherwise well-informed about the operation of the system, and know how they can exercise the various privacy-enhancing controls available to them.

The OAIC recognises the benefits that are expected to accompany an effective digital health record system in Australia. These benefits may include better health outcomes arising from the improved availability and quality of health information, fewer adverse medical events, and procedural and economic efficiency through reduced duplication of treatment. Realising these benefits is dependent upon ensuring that the sensitive health information is protected and held securely.

This submission provides some general background information in relation to the My Health Record system and the OAIC's regulatory role within the system, a high-level overview of the OAIC's regulatory experience since the commencement of the system in 2012, together with information on community privacy concerns for the Committee's consideration.

Background

The OAIC's regulatory role

The OAIC is the independent regulator of the privacy aspects of the My Health Record system. The OAIC has performed this regulatory role since the system commenced operation in 2012.

The privacy framework for the My Health Record system is currently set out in the *My Health Records Act 2012* (My Health Records Act) and the *Privacy Act 1988* (the Privacy Act). The OAIC has a range of regulatory functions and enforcement powers under both the Privacy Act and My Health Records Act to ensure compliance with these privacy requirements. The *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* outline how the Information Commissioner will approach enforcement issues under both of these Acts.

The OAIC has also entered a Memorandum of Understanding (MOU) with the Australian Digital Health Agency (Agency), the My Health Record System Operator, in relation to the OAIC's delivery of independent regulatory services in relation to the My Health Record system. In addition to exercising the regulatory and enforcement functions mentioned above, the OAIC also performs a

[1] The OAIC's view was that this represented best practice and provided a higher degree of privacy protection, by giving consumers the ability to decide upfront whether or not to participate. The OAIC's views on this matter have previously been set out in detail in its submission to the Senate Community Affairs Legislation Committee's inquiry into the Health Legislation Amendment (eHealth) Bill 2015.

[2] The decision implements one of the recommendations made in the Report into the Personally Controlled Electronic Health Record in December 2013, which was followed by opt-out pilots in Nepean Blue Mountains and Far North Queensland in 2016. In the 2017 Budget, the Australian Government announced the national expansion of the opt-out participation model for the My Health Record (MHR) system, following an evaluation of the opt-out pilots. The national opt-out expansion was authorised under Schedule 1 of the *My Health Records Act 2012* and the *My Health Records (National Application) Rules 2017*.

number of other activities under this MOU. This includes responding to enquiries and requests for advice on My Health Record privacy compliance obligations, and developing written guidance materials on privacy for users of the system.[3]

As part of the exercise of its regulatory responsibilities, the OAIC has also produced a range of digital health guidance for various stakeholders. This includes multimedia and written resources for healthcare providers, a series of factsheets for consumers and the Guide to mandatory data breach notification in the My Health Record system.

In response to the commencement of the My Health Record opt-out period on 16 July 2018, the OAIC also made comprehensive updates to the consumer factsheets, published new Frequently Asked Questions (FAQs) for consumers, and made consequential updates to other relevant website material, to assist in ensuring consumers have clear and up-to-date information about the My Health Record system and their ability to opt-out if they choose to do so.

The My Health Record privacy framework

The My Health Records Act, and the regulations and rules made under that Act, regulate the collection, use and disclosure of health information contained in a healthcare recipient's My Health Record. In addition to the requirements in the My Health Records Act, the System Operator is subject to the Privacy Act and other participants in the My Health Record system are subject to the Privacy Act and relevant State and Territory privacy laws.

These frameworks are in place to ensure that only members of the patient's healthcare team who are treating a person are able to access a record in the context of providing them healthcare. Consequently, unauthorised collection, use or disclosure of My Health Record information is prohibited. A breach of the My Health Records Act in connection with health information included in a healthcare recipient's digital record or a provision of Part 4 or 5 is an 'interference with privacy for the purposes of the Privacy Act', meaning the Australian Information Commissioner and Privacy Commissioner (the Commissioner) may investigate the act or practice under the Privacy Act. The Commissioner also has the discretion to conduct an investigation under subsection 73(4) of the My Health Records Act. The OAIC has a wide range of functions and enforcement powers available under the My Health Records Act and Privacy Act.[4] It is open to the Commissioner to use a combination of enforcement powers to address a particular matter.

The *My Health Records Rule 2016* also sets out a number of security requirements that the System Operator, healthcare provider organisations, contracted service providers and registered operators must comply with.[5]

In addition to the protections provided by the legislative framework, individuals also have a number of options in how they personally manage their privacy and exercise choice and control over their record. Specifically, individuals can do this by:

---

[3] The OAIC's full range of digital health regulatory activities is set out in the MOU.

[4] These include investigating and conciliating complaints, accepting enforceable undertakings, making determinations, seeking an injunction to prohibit or require particular conduct, seeking a civil penalty from the Courts, and accepting mandatory data breach notifications from the System Operator (the Australian Digital Health Agency), health care provider organisations, repository operators and portal operators.

[5] For example, registered healthcare provider organisations must have, communicate to employees and contractors, and enforce, a written policy that reasonably addresses security matters, such as the process for identifying a person who requests access to a healthcare recipient's My Health Record; the physical and information security measures that are to be established and adhered to; and mitigation strategies to ensure My Health Record system-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation's management.

- placing a Record Access Code on their record so that they have to provide a healthcare provider organisation with the code before the provider can access the record
- placing a Limited Document Access Code to restrict access to specific documents relating to visits to healthcare providers, or medicines they are taking, so that they have to provide the code for the healthcare provider organisation to access the document
- choosing to be notified via an SMS alert or email in real time when their record is accessed for the first time by a health care provider organisation, or when other actions occur such as a shared health summary being uploaded or where emergency access has been made
- asking a healthcare provider to not upload information and the healthcare provider must comply
- removing documents from view from the system
- viewing a full history of all access to their record, and seeking more information about these accesses if required
- cancelling their record at any time which ensures that healthcare providers can no longer access the information in the record.

The OAIC also welcomes the Government's decision to introduce the My Health Records Amendment (Strengthening Privacy) Bill 2018, which aims to strengthen the existing privacy protections in the My Health Records Act. Further, on 10 August 2018, the Government extended the opt-out period for the My Health Record system by an extra month to 15 November 2018. The OAIC is supportive of these privacy-enhancing measures, which provide individuals with further time to consider their options, and greater certainty and control over how their My Health Record information will be handled.

The OAIC's regulatory experience since 2012

As the privacy regulator for the My Health Record system, the OAIC is responsible for responding to enquiries and requests for advice on the appropriate handling of My Health Record information, responding to complaints received relating to the privacy aspects of the My Health Record system, receiving mandatory data breach notifications and conducting assessments of the My Health Record system.

Since the My Health Record system commenced in July 2012 (until 30 June 2018), the OAIC has:

- responded to 80 My Health Record enquiries
- received 11 My Health Record complaints
- received 88 My Health Record mandatory data breach notifications, and
- conducted 14 assessments (audits) of the My Health Record system and Healthcare Identifier service.

From 1 July 2018 to 13 September 2018, the OAIC has also:

- responded to 98 My Health Record enquiries
- received 29 My Health Record complaints
- received 11 mandatory data breach notifications.

The mandatory data breach notifications received have generally involved incorrect information being uploaded to a My Health record. Specifically:

- intertwined Medicare records of individuals with similar demographic information, resulting in Medicare providing data to the incorrect individual's My Health Record, and

- findings under the Medicare compliance program that certain Medicare claims were made in the name of a healthcare recipient, but not by that healthcare recipient, were uploaded to their My Health Record.

Under its MOU arrangements with the Agency (and previously the Department of Health), the OAIC has conducted a number of assessments of the My Health Record system and participants in the system. The assessments have considered how a range of privacy requirements (including governance, policies, notice, collection, use, disclosure and security) have been applied by participants in the system. The assessments were conducted with a view to identifying risks and suggesting mitigation strategies regarding the handling of personal information held in the My Health Record system. The complete list of assessments conducted by the OAIC in relation to the My Health Record system is available on the OAIC's website.

Further information and statistics are available in the Annual reports of the Australian Information Commissioner's activities in relation to digital health.

Community concerns raised during the opt-out period

The OAIC has been actively monitoring community concerns raised with the My Health Record system, particularly since the commencement of the opt-out period on 16 July 2018. A number of issues have been raised in various channels, including directly with the OAIC and through the media. The extended opt-out period provides an opportunity to address these matters and build confidence in the My Health Record system. To address these, the OAIC has been responding to enquiries about the My Health Record system, and has published a series of FAQs to assist in informing individuals about their choice to opt-out, and how to take other steps to protect their health information. The OAIC has also updated previously published fact sheets covering different aspects of the system, to help consumers understand how information in the My Health Record system is handled and what they can do to help protect their information. These were published on 16 July 2018 to coincide with the commencement of the opt-out period.

However, since the commencement of the opt-out period, the OAIC has also identified a number of more specific matters which require further consideration. These specific issues have been raised with the Department of Health and the Agency and are under active consideration. They are set out for the Committee's further consideration below.

Communications campaign

The OAIC considers that it is of critical importance that every Australian understands that they have a choice about whether they want to have a My Health Record created for them, or opt-out. Importantly, under the previous opt-in arrangements, individuals had to make an active decision to have a My Health Record and so were more likely to be engaged users of the system. By contrast, with the move to opt-out, there is a risk that individuals will be unaware that their sensitive health information is to be collected, used and disclosed for the purposes of their My Health Record. Further, they may be unaware of the general privacy implications associated with the handling of information in their record, or how to make use of the privacy safeguards available to them. The ability of individuals to make an informed choice about the way their health information is collected, used and disclosed by the My Health Record system will be heavily dependent on the existence of an effective awareness campaign.

The OAIC is aware that there have been some concerns raised in the community regarding the ability of all people to be reached by the current media campaign, or whether additional education or assistance is needed to support the community (or specific sections of the community).

The OAIC considers that the communications campaign should enable individuals to make a proactive decision about whether to opt-out of the system, as part of encouraging good privacy practice. Specifically, the OAIC's position is that individuals should be made aware of:

- how the My Health Record system operates
- the risks and benefits of the system
- their right to opt-out
- how to opt-out (whether by phone, online, or post), and
- how to exercise the privacy and security controls of their My Health Record.

The OAIC will develop further guidance and resources for consumers to be published at the end of the opt-out period and into 2019, to inform consumers about how to manage their My Health Record, what to do if they decide they no longer want a record, and how to exercise the privacy and security setting available to them.

Default privacy settings

With an opt-out participation model, the onus lies with the individual to set the access controls for their My Health Record. The default settings are set out in the *My Health Records Rule 2016*, and were developed in the context of an opt-in model. For example, the current default access arrangement is that all healthcare providers using the system will be able to view an individual's My Health Record who is in their care (unless the individual has set up their access controls to prevent this). Recent debate has focussed on whether the default settings are still appropriate, in light of the shift to opt-out.

The OAIC notes there may be alternative options to retaining the existing default settings - for example, the default settings could allow health information to be uploaded to an individual's record, but require an active step by individuals to adjust the settings, prior to any healthcare providers being able to access the record.

Alternatively, a healthcare provider wishing to access an individual's record could be required to go through a process similar to assisted registration[6] to gain access, thereby notifying the affected individual of the existence of the record, and that the healthcare provider wants to access the record.

Such a model would not prevent information being included in an individual's My Health Record. However, it would prompt the individual to exercise control over who could view the information. Accordingly, it may assist in mitigating the privacy risks associated with individuals being unaware of the fact that a My Health Record has been created for them, and of the record being used and viewed by their treating practitioners in this context.

The OAIC encourages further consideration of this issue, noting the need to consider privacy alongside the overarching policy objective and utility of the system.

[6] Assisted registration occurs where a healthcare provider assists an individual to register for a My Health Record with the individual's consent. It is permissible under the *My Health Records (Assisted Registration) Rule 2015*.

Young people

The Agency's current policy is to allow parents or guardians to have access to their child's My Health Record aged between 14 to 18 years, unless the young person changes that setting. It has been suggested that in light of the context of an opt-out participation model, this policy position may need to be reconsidered. The OAIC notes that this policy diverges from the policy applied in relation to Medicare information, whereby parents and guardians must obtain their child's consent to view their information once the child turns 14.

The OAIC encourages further consideration of this issue, noting the need to balance privacy concerns, parental access and clinical safety and quality concerns.

Automatic upload of Medicare information

According to the *My Health Records (National Application) Rules 2017*, two years' worth of Medicare information (for example, information about Medicare benefits scheme claims, pharmaceutical benefits scheme (PBS) claims) will be uploaded to My Health Records that are automatically created after the opt-out period closes. This will be triggered when a healthcare provider accesses an individual's My Health Record, unless the individual has adjusted their settings beforehand, to 'opt-out of' that upload process.

The OAIC understands that this default setting was implemented at the request of consumer groups before the system was first launched, as a way to bring some data into a newly created record, so that the record would have some immediate clinical value for a healthcare recipient. We also acknowledge this element of the My Health Record system is intended to deliver benefits to consumers, by allowing clinicians to access information on the medicines that have been prescribed to people with a My Health Record.

The OAIC encourages further consultation on this issue, including with privacy advocates, as well as organisations that represent vulnerable groups within the community.

Effect of opt-out model on individuals at risk from family violence

The OAIC is aware that concerns have been raised in relation to how My Health Records may impact individuals who may be experiencing family violence. Some of these concerns already existed within the opt-in system. For example, a non-custodial parent may be able to create a My Health Record on their child's behalf, without the consent or knowledge of their former partner. That parent's access to the record in those circumstances could be inappropriate, and risk revealing the child's location or movements in an unintended way.

However, some of the concerns raised would appear to be exacerbated in the context of an opt-out model. Privacy risks would be increased where an individual is not aware that a record has been automatically created for them and hence they may not be aware of steps they can take to protect their information in their My Health Record. Concerns have also been raised about how the Agency will mediate the rival claims of parents seeking to create or delete children's My Health Records.

The OAIC understands that these privacy risks are not limited to the My Health Record system, and may exist in other systems such as Medicare online. However, the My Health Record system offers an increasingly rich source of sensitive information that could be open to misuse in family violence or child custody situations.

We would encourage further consideration and consultation on this issue, to ensure that appropriate solutions are devised to minimise any privacy risks for individuals experiencing family violence.

Access to My Health Record information by third parties

At present, there are limited circumstances where health information may be accessed by healthcare providers, the Agency or other registered entities for non-healthcare reasons, including:

- for the management of the My Health Record system
- where it is necessary to lessen or prevent a serious threat to an individual's life, health or safety and it is unreasonable or impracticable to obtain consent
- where it is necessary to lessen or prevent a serious threat to public health or public safety (such as in an emergency, for more information see: Privacy fact sheet 23: Emergency access and your My Health Record).
- where it is required or authorised by law
- for purposes relating to a healthcare provider's indemnity cover
- to comply with a court or tribunal order, or
- for law enforcement purposes.

As noted above, the My Health Records Amendment (Strengthening Privacy) Bill 2018, will further limit the possible access to My Health Record information by third parties by removing the ability for the System Operator to disclose health information to law enforcement agencies and government agencies without an order by a judicial officer (or the healthcare recipient's consent), and specifying the limited laws which may authorise the collection, use and disclosure of My Health Record information. The OAIC is supportive of these proposed amendments.

The OAIC is aware that particular concerns have been raised regarding access to My Health Records by health insurers, or for the purposes of employment checks. However, we note that only approved healthcare providers are able to access information in the My Health Record system, and insurers are specifically prohibited under section 14(2) of the *Healthcare Identifiers Act 2010* from having a healthcare identifier, which is a pre-requisite for access to the system.

Access history

We understand the My Health Record system is able to provide individual users with information about which healthcare providers have viewed their record. However, the OAIC understands that the information available to an individual in the My Health Record 'Access History' is at the organisational level, rather than individual practitioner level. Where an individual wants to know which individual practitioner has accessed their record, we understand that they can request this information by contacting the healthcare provider organisation or the Agency directly. The My Health Record Act and supporting rules require systems to be in place at the organisational level to be able to ascertain who has accessed the record from within an organisation.

The OAIC understands that many healthcare provider organisations have implemented measures which will allow the System Operator to 'track' access to the individual practitioner level, using 'Healthcare Provider Identifiers – Individual' (HPI-Is). This will mean that individual practitioners are identified in the System Operator's audit log.

However, some notable exceptions are state and territory healthcare providers, which have advised that they are currently unable to implement real-time tracking of HPI-Is to the System Operator at a state-wide level. In these instances, the OAIC understands that the System Operator

contacts the healthcare provider organisation to obtain the name of the individual from the local audit log, where a healthcare recipient contacts them to request this. While current processes are compliant, ideally over time, all individual clinicians should be able to be identified in the System Operator's audit log to allow for more seamless oversight of the system.

Secondary use of information in the My Health Record system

Some concerns have also been raised in relation to other possible secondary uses of both identifiable and de-identified data sourced from the My Health Record system. By default, de-identified information extracted from a My Health Record may be provided to certain third parties, such as medical researchers, for purposes other than providing healthcare. However, individuals can choose not to have their de-identified data used for secondary purposes by selecting the 'withdraw participation' function in their My Health Record or contacting the System Operator.

Identified personal information in a My Health Record can only be used for secondary purposes, such as research or public health purposes, with the individual's consent. The Department of Health has published the Framework to guide the secondary use of My Health Record system data (the Framework), which provides guiding principles for the use of My Health Record information for secondary purposes and specifically states that system data cannot be used solely for commercial and non-health-related purposes.

The OAIC made a public submission to HealthConsult on the Consultation Paper on the Development of a Framework for Secondary Use of My Health Record Data, and welcomes further engagement with the Department of Health and the Agency on the implementation of the framework and privacy matters.