Australian Government

Office of the Australian Information Commissioner

Legislation review of the My Health Records Act 2012 - Submission to the Department of Health

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

26 October 2020

OAIC

Overview

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Consultation Paper for the Review of the My Health Records Legislation (the Review). The Review is required under s 108 of the *My Health Records Act 2012* (MHR Act) and aims to ensure the legislation underpinning the My Health Records (MHR) system is effective.

The Consultation Paper outlines a number of key issues being considered as part of the Review and seeks specific input on 19 discussion questions which were largely drawn from the early consultation sessions that were conducted for the Review and from the Review Terms of Reference. The OAIC considers this Review to be an important evaluative measure and an opportunity to ensure that the privacy and security of health information continues to be a central focus of the design and functionality of the MHR system.

The protection and security of MHR information underpins public confidence in the system and is crucial to realising the benefits that are increasingly expected to accompany an effective digital health record system in Australia. This review provides an opportunity to re-assess the MHR system legislative framework and current privacy and security safeguards to ensure they remain current in an evolving digital landscape. Achieving the appropriate balance between clinical utility and privacy and security is critical to ensuring ongoing trust in the system and realising public health benefits.

Through our role as the independent privacy regulator for the MHR system, the OAIC is in a unique position to identify and understand MHR privacy and security risks. The OAIC conducts assessments (audits) to proactively identify and make recommendations to mitigate risks to privacy. The OAIC's MHR assessment program and other regulatory activities have highlighted some areas where we consider the privacy protections and regulatory oversight provided by the current legislative framework warrant further consideration and strengthening.

This submission outlines the risks identified by the OAIC and makes recommendations for legislative amendment.

About the OAIC and our role in the MHR system

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

The privacy framework for the MHR system is currently set out in the MHR 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 MHR 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.

In addition to the exercise of its regulatory responsibilities, the OAIC proactively develops digital health guidance for various stakeholders. This includes new guidance for healthcare providers on Rule 42 (security policy requirements), 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.

The OAIC is currently funded through a Memorandum of Understanding (MOU) with the Australian Digital Health Agency (Agency), the MHR System Operator, in relation to the OAIC's privacy regulation

in relation to the MHR system. The MOU provides funding for the OAIC to exercise its regulatory and enforcement functions as well as other activities, such as responding to enquiries and requests for advice on MHR privacy compliance obligations. Direct appropriation for the OAIC's base funding would provide greater certainty to support longer term planning of its privacy oversight role in the MHR system.

Response to general themes

Digital innovation in the health sector has the power to improve health outcomes for Australians. The recent COVID-19 pandemic has demonstrated the practical benefits that digital health practices can deliver, for example, through the rapid adoption of telehealth services, e-prescribing, electronic messaging, emergency clinics and non-standard consultations. However, as digital health initiatives necessarily involve the management of large amounts of sensitive health information, privacy must be a central consideration. Some of the ideas for improving the value and utility of the MHR system that have been raised in the Consultation Paper have the potential to significantly increase privacy risks associated with the MHR system, such as re-platforming to apply artificial intelligence (AI) software and interaction with other health record systems.

The OAIC welcomes the development of a 'futures roadmap' or strategic plan for the MHR system as a way for stakeholders, including the OAIC, to understand how the system is intended to operate going forward. The OAIC is aware that the Agency is prioritising the development of a strategic plan for the MHR system, including how the MHR system could better integrate into the broader digital health landscape. The OAIC continues to engage with the Agency on their work in this area.

It is important that any roadmap or strategic plan builds privacy protections into future planned uses of the MHR system at an early stage and has the flexibility to accommodate privacy protections into novel uses of the MHR system. Expansion of clinical uses of the system has the potential to significantly increase privacy risks, particularly where health information in the MHR system is shared more widely and used for more varied purposes. The Agency is required by the Privacy (Australian Government Agencies – Governance) APP Code 2017 to undertake a Privacy Impact Assessment (PIA) for any high risk privacy projects, such as integration of the MHR system with separate record systems or other significant expansion of the MHR system. A PIA is a systematic assessment of a project to identify the impact it might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact.

Responses to specific issues

Privacy oversight by the Office of the Australian Information Commissioner

The Information Commissioner has various enforcement and investigative powers in relation to the MHR system, under both the MHR Act and the Privacy Act. The Information Commissioner has power under subsection 73(4) of MHR Act to do all things necessary or convenient to investigate an alleged contravention of MHR Act in relation to the MHR system, either in connection with health information in a healthcare recipient's digital record or as a result of a breach of a civil penalty provision.

The Information Commissioner may also choose to investigate the act or practice under the Privacy Act because a contravention of the MHR 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.

Effective regulation is dependent on a clear and comprehensive legislative framework. The review is an opportunity to ensure that the Information Commissioner's role in assessing, investigating and enforcing the MHR Act fully extends to all participants in the system. For example, consideration should be given to the Information Commissioner's general investigative powers under s 73 of the MHR Act to ensure their application in relation to State and Territory authorities' handling of information contained in an individual's MHR.

Recommendation 1

The OAIC recommends consideration is given to legislative amendments required to ensure the application of the Information Commissioner's role in assessing, investigating and enforcing the MHR Act fully extends to all participants in the MHR system.

Oversight of registration process

The OAIC has an important audit role in the MHR system, that could include all aspects of the governance of the system which may impact the privacy and security of the system. However, the Information Commissioner's regulatory remit does not include oversight of the way in which the System Operator satisfies itself that an applicant healthcare provider organisation has and will comply with the requirements of the My Health Records Rule 2016 (MHR Rules) in order to register to use the system.

Under s 73 of the MHR Act, the Information Commissioner has the power to investigate acts or practices that contravene that Act in connection with health information included in a healthcare recipient's MHR, or a provision of Part 4 or Part 5. The act of registering a healthcare provider organisation sits within Part 3 of the MHR Act. The act of registering does not have a connection with health information included in a healthcare recipient's MHR.

The effect of this limitation is that the Information Commissioner cannot consider the conduct of the System Operator in registering healthcare provider organisations under the MHR Act. There is no clear intent evident in the MHR Act which would allow the Information Commissioner, in the exercise of their regulatory functions and powers under the Privacy Act, to direct or provide guidance to the System Operator in determining whether to register healthcare provider organisations. Further, no other body appears to have regulatory oversight of the registration process. This appears to be a regulatory gap in overseeing the manner in which healthcare providers should demonstrate compliance with relevant privacy obligations in order to become registered to use the system.

Recommendation 2

The OAIC recommends a mechanism for external oversight of the healthcare provider registration be established.

Limitations on sharing information with the System Operator regarding risks to the MHR system

The OAIC is uniquely positioned to identify privacy and security risks to the MHR system as a result of its regulatory oversight role, however, due to current statutory limitations on the OAIC's ability to disclose information, the OAIC is unable to advise the System Operator of certain risks in the absence of an investigation.[1] For example, absent an investigation, documents that relate to particular healthcare providers cannot be shared with the System Operator to inform its forward assurance program.

As with the State and Territory jurisdiction issue raised above in relation to recommendation 1, the recently introduced COVIDSafe regulatory framework provides a useful model that could be reflected in the MHR Act to expand the Information Commissioner's information sharing powers to also address this issue. Under this framework, the Information Commissioner is specifically permitted to share information or documents with a State or Territory privacy authority for the purpose of:

- exercising powers, or performing functions or duties under the Privacy Act in relation to public health contact information, or
- for the purpose of the State or Territory privacy authority exercising its powers, or performing its functions or duties.

The Information Commissioner must also be satisfied on reasonable grounds that the State or Territory privacy authority has satisfactory arrangements in place for protecting the information or documents (s 94W of the Privacy Act).

Recommendation 3

The OAIC recommends that the permitted disclosure regime is expanded to allow disclosures of certain risks identified through the OAIC's regulation of the MHR system to the System Operator, including bodies delegated to undertake System Operator functions. This will facilitate a more cohesive and effective mitigation of those risks. This may involve information sharing between the OAIC, the Agency and Services Australia in relation to the MHR system.

[1] See section 29 of the *Australian Information Commissioner Act 2010* and section 73A of the *My Health Records Act 2012*.

Access to MHR information for insurance and employment purposes

The possible use of MHR information by health insurers, or for the purposes of employment checks was a major concern for consumers identified in the lead up to the transition to an opt-out model. The OAIC supported the legislative amendments made through *My Health Records Amendment (Strengthening Privacy) Act 2018*, in recognition of these serious privacy concerns.

The OAIC understood that MHR information was never intended to be used for these purposes, and that the 2018 amendments strengthened the existing prohibitions for insurers and employers. Any proposal to weaken these protections could impact the privacy of healthcare recipients and public confidence in the system, leading to possible reduced participation.

Control of a Minor's MHR

Amendments to the MHR Act were introduced in December 2018 regarding the arrangements for young people aged 14–17. Since then, the MHR Act provides for young people aged 14–17 to have control over their own MHRs (s 6). They may however choose another person (such as a parent) to be their 'authorised representative' or 'nominated representative', which allows that person to control or view their MHR. These changes were introduced to give young people more control over their own health information and to prevent the parents of 14 to 17-year-olds accessing their child's MHR without explicit consent. Prior to these amendments, parents of young people under 18 automatically became 'authorised representatives' and generally had control over a young person's MHR.

The OAIC supported the 2018 amendments to the extent that it meant that young people could feel confident that their sensitive health information, would remain private between themselves and their treating healthcare providers. However, the OAIC is aware that the amendments have since created challenges around the handling of MHR information whereby:

- children under 14 years of age can no longer manage their own MHR where they are capable of making decisions for themselves (and have no authorised representative, such as a parent or guardian), and
- there is no provision for a person to be an authorised representative (without nomination) for a person who does not have capacity to make decisions for themselves where that person is 14–17 years of age.

The OAIC welcomes further consideration of the issues raised above in relation to the existing framework for the handling of the health information of minors.

Recommendation 4

The OAIC recommends that the following changes may resolve these issues:

- the MHR Act be amended to include provisions for a child under 14 years of age to manage their own MHR where the Agency is satisfied that the child is capable of making decisions for themselves, in terms such as the previously repealed s 6(3) or similar.
- the MHR Act be amended so that a third party may apply to be an authorised representative for a healthcare recipient aged 14 or over who has impaired decision-making capacity.

Healthcare recipient controls in My Health Record

The OAIC strongly supports the ability of consumers to be able to control access to their MHR information, including through the ability to 'hide' documents. The default settings established in the MHR Rules allow all healthcare providers using the system to view an individual's MHR who is in their care unless the individual has set up access controls to prevent this. There are two ways an individual can control access to specific health documents in their MHR:

1. Restricting access to a document, which will limit access by an individual's nominated representatives and healthcare providers, except in the case of an emergency.
2. Removing a document, so that it cannot be viewed by anybody, even in an emergency.

It is an important system feature that a consumer may limit access to health information they consider to be sensitive from particular healthcare providers. For example, a person may wish to limit access to their mental health plan to their GP and psychologist and restrict access to other providers such as their dentist or podiatrist.

Healthcare providers may use an 'emergency access' override function to access MHRs in limited circumstances involving 'serious threat' to individuals or public health/safety where it is unreasonable or impracticable to obtain the individual's consent. This overrides any access settings set by healthcare recipients. The OAIC recognises that the 'emergency access' function is an important system feature, which could give potentially life-saving information to healthcare providers in situations where, for example, an individual is unconscious or otherwise unable to communicate their medical history. However, when this feature is not used appropriately, this could constitute an interference with privacy and undermine the purpose of allowing a consumer to control access to their record.

The Australian National Audit Office's (ANAO) performance audit of the MHR system, published in November 2019, found that the Agency did not have sufficient assurance arrangements to satisfy itself that all instances of emergency access by healthcare provider organisations did not constitute a breach of privacy. Additionally, the ANAO noted that the Agency has not notified the Information Commissioner of any of the potential contraventions of the MHR Act related to use of the 'emergency access' function.

The OAIC's view is that the existing provisions in the MHR Act that establish the 'emergency access' function appropriately balance privacy and clinical needs. The OAIC is not aware of evidence that would warrant their expansion to allow, for example, "a special authorisation for a hospital

emergency department to access a consumer's MHR without having to explore other access options with the individual" as suggested in the Consultation Paper. The OAIC's view is predicated on upholding the important principle that, where possible, an individual's consent is obtained before overriding any access controls they have put in place.

However, as identified in the ANAO audit, there may be practical challenges associated with implementation of the 'emergency access' function and compliance with the legislative provisions in the MHR Act. The OAIC acknowledges that the Agency has responded to the ANAO audit with an Implementation Plan, which proposes steps to address this issue. The OAIC continues to engage with the Agency to ensure that suitable measures are in place to regulate use of the emergency access function and that the Implementation Plan is carried out.

Status of a My Health Record upon a person's death

Under the Privacy Act, information about deceased persons is generally not considered to be 'personal information'. Personal information is information about an individual, which means a natural person and does not include a deceased person. As noted in the Consultation Paper, the MHR Act requires the Agency to cancel the registration of a healthcare recipient upon being notified of the person's death. The health information in the record is retained for 30 years after death (or for 130 years if the date of death is not known). However, it is not otherwise made expressly clear in the MHR Act what action can be taken in relation to the record after a person's death.

The Consultation Paper raises a number of questions around a person's MHR after death, including:

- can the record be used to support clinical review of the cause of death (an autopsy)?
- can it be accessed to ascertain if there is an organ donor consent?
- can documents be added to the record after death, such as an autopsy report or a death certificate?

Given the issues raised in the Consultation Paper, it may be appropriate for the MHR Rules to specifically deal with this issue in relation to the MHR system. The OAIC would welcome further consideration and consultation on this issue. The OAIC also recommends reconsideration of the necessity and proportionality of the requirement to retain records 30 years after death (or for 130 years if the date of death is not known).

Recommendation 5

The OAIC recommends that the MHR Rules deal with the status of a person's MHR upon death and that the necessity and proportionality of the requirement to retain records 30 years after death (or for 130 years if the date of death is not known) be reconsidered.

Secondary use of MHR information

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.

Data breach notification under the My Health Records Act

The MHR Act makes it mandatory for certain entities to notify the OAIC and the System Operator of a data breach involving the MHR system. Under s75(2)(c) of the MHR Act, State and Territory authorities, and instrumentalities of State and Territory authorities, are only required to notify data breaches to the System Operator, which limits the oversight role of the OAIC. The MHR Act requires relevant entities to take a number of steps as soon as practicable after becoming aware of a MHR data breach.

From 22 February 2018, a wider Notifiable Data Breaches (NDB) scheme has also applied in Australia under the Privacy Act. This scheme applies to all private sector healthcare providers and requires organisations covered by the scheme to notify particular individuals and the OAIC about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

Broadly, the NDB scheme requirements sit alongside the data breach reporting requirement for the MHR system, but they do not overlap. So, while there are similarities between the reporting requirements of both schemes, there are some important differences. Firstly, data breaches notified under the MHR Act do not need to be reported under the NDB scheme, and this is to prevent duplication of reporting. Another key difference is that entities must report every MHR data breach that has or may have occurred, whereas under the NDB scheme, only data breaches that are likely to result in serious harm to affected individuals need to be reported. Thirdly, breaches must be reported as soon as practicable under the MHR Act, even when remedial action to mitigate the likelihood of harm arising as a result of the data breach is in progress or has already been taken.

The OAIC acknowledges that there are potential challenges for healthcare providers having to comply with two schemes with different reporting thresholds. While harmonising the reporting obligations under the MHR scheme with the Privacy Act NDB Scheme may address these challenges, the OAIC is concerned that:

- the lower data breach notification threshold required for information held in the MHR system was designed as a privacy enhancing measure, given that the MHR system is a searchable network of connected registered repositories storing sensitive personal information, and
- the lower threshold ensures data breach reporting that may not relate to incidents giving rise to serious harm, but which may point to systemic issues in the ecosystem.

For example, most notifications to the OAIC related to intertwined Medicare records. While a test of serious harm to affected individuals may not have been met, it did point to system faults that required remediation. The requirement to report these provides accountability of the System Operator in remediating these issues.

On balance, the OAIC recommends maintaining the existing MHR data breach scheme which captures a broader range of data breaches compared to the NDB scheme, in recognition of the sensitive information held in the MHR system. However, if in the future it was decided that the harmonisation of the schemes was considered necessary, the OAIC suggests that other measures would need to be established to counter any resultant risks.

The OAIC also recommends that consideration is given to the introduction of an 'accreditation' system. For example, in relation to the Consumer Data Right (CDR), providers are accredited by the Australian Competition and Consumer Commission (ACCC) as meeting particular security and privacy standards. This model builds in assurance up front in addition to a reactive breach reporting approach. The Agency could apply a similar approach for the accreditation of healthcare providers and other participants registering to use the MHR system in addition to meeting the eligibility requirements and any assurances required to be given during the registration process.

The OAIC considers that an accreditation program has merit generally and ought to be considered as a proactive safeguard.

Recommendation 6

The OAIC recommends:

- State and Territory authorities, and instrumentalities of State and Territory authorities, be required under Section 75(2) of the MHR Act, to also report data breaches to the OAIC;
- maintaining the existing MHR data breach scheme which captures a broader range of data breaches compared to the NDB scheme; and
- that consideration be given to an accreditation system to ensure that healthcare providers and other participants registering to use the MHR system meet minimum privacy and security requirements.

System Operator's powers, functions and responsibilities

Potential deficiencies in the registration process: Limited compliance/assurance checks concerning healthcare provider organisations

The System Operator of the MHR system has a statutory function to register healthcare provider organisations, and to manage and monitor on an ongoing basis the system of registration (s 15 and 56 MHR Act). Registration of healthcare provider organisations is necessary to ensure that healthcare provider organisations' collection, use, disclosure of health information from the MHR system is authorised (s 61-70 MHR Act).

The System Operator must register a healthcare provider organisation if it meets eligibility requirements, including that the healthcare provider organisation complies with the MHR Rules. The

System Operator is not obliged to register an organisation if it is satisfied that registration may compromise the security or integrity of the MHR system, having regard to any prescribed matters under the MHR Rules (s 44 of the MHR Act).

The Agency (as System Operator) has delegated its powers under s 44 of the MHR Act to Services Australia.

There is no positive obligation on the System Operator to take action in the event that the healthcare provider organisation does not comply with the MHR Rules at the time of registration, or has since become non-compliant with the MHR Rules. The System Operator 'may' decide to cancel or suspend the registration of an entity if, amongst other things, the System Operator is no longer satisfied that they are eligible (s 51(3) of the MHR Act).

In April 2019, the OAIC initiated a series of privacy assessments of emerging participants in the MHR system. Through these assessments it became apparent that numerous healthcare provider organisations did not comply with the MHR Rules and MHR Act at the time of registration and during their subsequent use of the system following registration. For example, assessed healthcare provider organisations did not have a Rule 42 (security) policy at the time they applied for, and were granted registration, which is required under the MHR Rules.

Recommendation 7

The OAIC recommends legislative amendments to sections 44 and 51(3) of the MHR Act to introduce positive obligations on the System Operator to:

- require a healthcare provider organisation to provide evidence that it meets the MHR Rules requirements during the registration process
- undertake checks to confirm the information provided by the healthcare provider organisation, and
- take action in the event that the healthcare provider organisation does not comply with the MHR Rules at the time of registration or has since become non-compliant with the MHR Rules.