REVIEW OF THE MY HEALTH RECORDS LEGISLATION

Consultation Paper

September 2020

1. ABOUT THIS REVIEW

My Health Record (MHR) has evolved over more than a decade as a unique national digital health records scheme. As of August 2020:

- More than 90% of eligible Australians have an individual MHR – 22.82M in total, of which over 19.68M have health data entered in the record.
- A high majority of healthcare providers are registered in the system – 94% of general practitioners, 99% of pharmacies, and 95% of public hospitals.
- Over 2.24B documents have been uploaded to MHR, including almost 2B Medicare documents, 158M uploaded by healthcare providers and 328,000 by consumers.
- MHR includes immunisation data for nearly 15M people, and organ donor directions for over 1.6M.

The design and implementation of the MHR system requires Government to make choices that have been of public interest. Two significant examples are the switch from an opt-in to an opt-out scheme that occurred in 2019, and the design of the scheme rules that enable consumers to set access controls of different kinds.

To encourage continued discussion and public engagement, the *My Health Records Act 2012* (MHR Act) requires an independent review of the scheme to be undertaken by December 2020. Public consultation is an integral element of the review. The review report will be tabled in the Parliament, after being endorsed by the Minister for Health and shared with state and territory health ministers.

This consultation paper identifies key issues being considered in this review. They are drawn from the Terms of Reference for the review, and from early discussions held with government agencies and professional and consumer organisations.

Comments are invited on these and any other issues that relate to the operation of the MHR Act. As outlined in the Terms of Reference, a central focus of the review is whether the MHR Act supports the policy objectives of the MHR system to:

- improve continuity and coordination of health care for healthcare recipients who are accessing multiple providers
- reduce duplication of treatment and avoid adverse events through enhanced availability and quality of health and medicine information
- enable consumers to participate more actively in their own healthcare.

Maintaining public trust and confidence in the MHR system is a Government priority. As such, the review is particularly interested to hear whether revisions to the Act would enable better MHR use by consumers and health service providers, and improve the delivery of healthcare services in Australia.

2. AN OUTLINE OF MY HEALTH RECORD

MHR is a consumer-controlled national system for digitally storing key health information about individuals and providing controlled access to that information for healthcare purposes.

MHR is managed by the Australian Digital Health Agency (the Agency) – which is described in the MHR Act as the 'System Operator'.

A record is created within the MHR system for everyone who has been assigned an Individual Healthcare Identifier (IHI) – a unique 16 digit number that identifies a healthcare recipient. An IHI is assigned by the Healthcare Identifier Service (HI Service), which is operated by Services Australia, for every person who is enrolled in Medicare or is registered with the Department of Veterans' Affairs. An IHI is different to a consumer's Medicare number.

A consumer can cancel or suspend their MHR registration at any time. If a person cancels their record, their health information is deleted and the content can no longer be retrieved.

A consumer's MHR can include a comprehensive range of personal health information that is uploaded by Medicare, by healthcare providers (such as medical practitioners, specialists, nurses, pharmacists and dentists) and by health provider organisations (such as hospitals, medical practices, pharmacists and pathology and radiology services).

A consumer's MHR may include hospital discharge summaries, electronic referrals, a shared health summary prepared by a clinician, specialist letters, advance care plans, event summaries, pathology reports, diagnostic imaging reports, pharmaceutical prescriptions and dispense records, medical and pharmaceutical benefit claims, a consumer's organ donor registration status, immunisation information, and pharmacist shared medicines lists. A record holder can also upload health information to their own MHR (such as consumer-only notes).

To participate in the MHR system a healthcare provider or organisation must obtain a healthcare identifier from the HI Service – either a Healthcare Provider Identifier-Individual (HPI-I) or a Healthcare Provider Identifier-Organisation (HPI-O).

The identifier enables the provider or organisation both to upload health information to a consumer's MHR, and to access health information in their MHR. The default setting is that a provider or organisation can, without a consumer's express consent, upload or access their personal health information for the purpose of providing healthcare to them.

An MHR record holder can override those default settings. The person may advise the provider or organisation that a specified document is not to be uploaded. A person can also set access controls that prevent a provider organisation from viewing or having access to their health information, either generally or subject to limitations the person has specified. Another option is that the record holder can remove a document that has been uploaded.

There are other specific features of the MHR system that are explained later in this paper. Among them are that the MHR legislation contains special rules regarding the MHR of a minor, the appointment of a representative who may act on behalf of an MHR record holder, the use of MHR personal health information for insurance or employment purposes (called 'prohibited purposes'), and the use of MHR records for research and public health purposes.

The MHR Act requires the Office of the Australian Information Commissioner (OAIC) to oversee and report on how the privacy safeguards in the MHR legislation are being met. The

MHR Act also imposes criminal and civil penalties for the unauthorised collection, use, and disclosure of a healthcare recipient's MHR.

3. PERSPECTIVES ON THE OPERATION OF MY HEALTH RECORD

Several contrasting themes have emerged strongly in the early consultations undertaken for this Review. Some of the commentary was broader than this review, which focusses on whether the MHR Act supports the policy objectives of the MHR system.

With that limitation in mind, the themes raised in the early consultations are outlined below to invite further discussion and commentary. It is important to stress that the following summary does not evaluate or endorse the views expressed.

Strong cross-sectional support for My Health Record

There is widespread support for MHR and a belief that, intrinsically, a national digital health records system is essential.

MHR is seen as a necessary step in integrating health service delivery with technology. Appropriately, MHR seeks to overcome fragmentation and duplication of patient health information, to make patient information more readily accessible when healthcare services are being provided, and to aid the coordination and quality of healthcare provided to individuals.

MHR can offer practical benefits across the healthcare system. Healthcare recipients can benefit in many ways – by knowing where their health information can be accessed, by accessing that information to manage complex health conditions and to consult new healthcare providers, by avoiding duplicate testing, and through becoming more health literate and engaged. There can be similar practical benefits for healthcare providers in accessing reliable and current health information about new patients, dealing with unexpected or emergency visits, and validating the occurrence of tests and prescriptions.

The large number of public and private healthcare providers that operate across Australia and in different state and territory health networks is seen to be an added practical reason for integrating patient health information and making it accessible through common or linked platforms. Choice and mobility have become more important to healthcare recipients.

MHR is acknowledged to have compelling design features that differentiate it from some other health records systems. Three in particular are: consumer (rather than practitioner) control of the acquisition, use, and disclosure of personal health information; trusted independent oversight and auditing of how sensitive health information is managed; and infrastructure that is aligned to developments in Australia's broader digital health program.

My Health Record as a supplementary health record

It is recognised that MHR must be viewed in context in evaluating its purpose and strengths.

MHR operates alongside other health record systems, such as those maintained by hospitals, medical clinics, pathologists and pharmacists. In many instances, the healthcare recipient and provider can rely more simply on their localised record system. There may, for example, be little need for a patient who regularly visits the same practitioner to access MHR for healthcare purposes, or for the provider to do so. MHR will necessarily have greater utility in some situations than others.

Nor can MHR – or indeed any health records system – replace the need for normal clinical interaction between a patient and a clinician.

The benefit that MHR offers consumers of having an individual, permanent and accessible record of personal health information is also an important consideration. That benefit must be balanced against other options for designing a health records system.

Keeping this context in mind is integral to understanding the purpose of MHR and limitations on the currency and reliability of MHR content.

Mixed assessment of My Health Record performance

A view expressed is that MHR has not fully met the promise or the expectation that many held for it.

Two issues are highlighted. One is that there is limited or uneven content in many MHR records. A second is that there is insufficient involvement in MHR by healthcare providers, both in uploading personal health information to MHR and in accessing a patient's MHR when providing healthcare to them. These weaknesses can shake public and practitioner confidence in the utility of MHR and in that way be self-perpetuating.

A related concern is that of uneven MHR use across the health profession. Public hospitals, for example, have increased their upload and use of MHR health information, compared to areas of under-use that include specialists and allied and community health services. Similarly, there is variable participation in MHR by medical practitioners and pharmacists, and some have lessened their involvement over time.

It has been questioned whether many consumers are disinclined to make active use of their MHR. Contributing factors may be the need to link and access MHR through a MyGov account, a consumer may not understand the medical information in their record, or they may be aware that it is not up-to-date or contains gaps.

There are differing views on how to evaluate those weaknesses. One view is that MHR is still at an early stage and is evolving and its utility to healthcare recipients and providers will strengthen over time. Positive acceptance of MHR may have been held back by practical workflow obstacles that can be resolved by legislative and administrative reforms.

Possibly, too, the earlier and contentious opt-in/out privacy debate cast a long shadow, but that may be clearing gradually over time. Recent events such as the COVID-19 pandemic have led to an enhanced understanding – by consumers in particular – of the practical benefits that digital health practices can deliver.

A variation of that view is that the challenges facing MHR were understated or misunderstood. They include: the challenge of introducing a national health information system in a federal system comprising nine governments; community suspicion about a government managed database of personal health information; the inherent clash between an MHR principle of consumer control and an established medical tradition of clinical autonomy; and the health profession's preference to use alternative record databases that are practitioner-focussed and simpler to access – particularly those operated by public hospitals or by private diagnostic services.

This review will take account of those contrasting views, while focussing on the improvements and reforms that could be made to the MHR Act.

Linking My Health Record to other digital health initiatives

MHR is one of seven digital health priorities set down in *Australia's National Digital Health Strategy,* published by the Australian Digital Health Agency in July 2018 and endorsed by all Australian health ministers. Other strategic priorities include (but are not limited to): secure digital channels for communication between healthcare providers and with patients; standards to ensure interoperability between public and private healthcare services; electronic medicines; and program support for the development of accredited health apps.

There is strong backing for viewing MHR as an important element of a broader digital healthcare program. The importance of doing so has been affirmed by recent incidents in which there was greater reliance on technology to deliver health services. Examples in 2020 are the Australian bushfires and the COVID-19 pandemic. In both there was a marked increase in the use of telehealth services, e-prescribing, electronic messaging, emergency clinics and non-standard consultations.

Another way of viewing MHR in the context of other digital health initiatives is to regard it as more than a digital filing cabinet or drop box. In short, the creation of the record should not be seen as the end in itself. Though an aim is that all Australians should have the option of a digital health record that they control, the overarching MHR objective is to improve the quality and efficiency of healthcare. This can only be fully met if the purpose of MHR is understood broadly and it is linked to other digital health initiatives.

Looking ahead, new technology interface challenges will arise. An example is the issue of whether MHR should be re-platformed to apply artificial intelligence (AI) software. The benefit of so doing is that static MHR content could be curated or atomised and be presented and used differently.

A change of that kind may become a functional necessity. The content volume of individual records will enlarge over time and key 'real-time' information may become less identifiable and accessible. Intelligent software applications also raise larger issues about whether MHR can or should be re-platformed as a decisional support tool, for example, to issue reminders or alerts or co-ordinate health care treatments for individuals.

Laying out a My Health Record roadmap

There is a call for a futures roadmap to explain the direction that MHR is expected to take in coming years.

One purpose of a roadmap would be to elaborate on the priority outcomes and principles set out in *Australia's National Digital Health Strategy*. The Strategy states that the benefits of MHR will be realised through the delivery of three strategic objectives – 'increased consumer participation', 'increased core clinical content' and 'extensive adoption by healthcare providers'. A roadmap could provide additional detail on how those objectives are expected to be realised.

Another purpose of a roadmap would be to refine how MHR can interact with other health record systems to form a national health database. This is important to state and territory health planning, for both budgetary and strategic policy planning reasons. There is said to be a similar practical need for a long-term strategic plan on MHR interaction with separate record systems created for a special purpose, such as those for immunisation, cancer screening, allergies, renal failure and diagnostic imaging.

Another dimension that some would like spelt out more is the role that industry can play in adding value to the MHR system. There is industry interest in developments that could

provide better personalised health support to individuals, for example, through apps and mobile device options that integrate MHR data with other personal health information.

An underlying concern in some commentary is that uncertainty remains about the purpose and objectives of MHR. One source of uncertainty is that the process of defining MHR objectives was overwhelmed by the priority earlier given to implementing the opt-out model and reaching out to consumers. Uncertainty is also a product of fluidity in digital health strategies, given the rapid pace of change in this relatively new domain.

An analogous recommendation for development of a futures roadmap was made in the 2018 *Healthcare Identifiers Act and Service Review – Final Report*. The Report recommended that the Agency develop a strategy and roadmap for the HI Service that covered matters such as the alignment of HI business architecture and future uses, the projected impact of new digital initiatives on the HI Service, and strategies to extend uptake and participation in areas of under-representation in the HI Service. Specific issues concerning the interaction of the HI Service and the MHR system are discussed below.

Ensuring the My Health Records Act supports digital health innovation

The operation of the MHR system and the direction it may take in future are tied to the requirements of the MHR Act. The next section of this paper discusses several specific issues that have been raised about the suitability of the present legislative framework, as well as noting broader themes that bear on the specific issues.

One broader question is whether the complexity of the MHR legislative framework is impeding greater participation by healthcare providers. A criticism is that providers encounter difficulty in registering, keeping their registration current and managing MHR patient information in a clinical setting. An individual provider may weigh those difficulties against the benefits they derive from participating in MHR or instead using an alternative system or arrangement to access consumer health information.

An added disincentive for healthcare providers is that the MHR Act imposes criminal and civil penalties for the unauthorised collection, use and disclosure of an individual's MHR health information. While penalties are a customary method of buttressing privacy and security safeguards, a provider may be discouraged from using MHR if there is a possibility of a penalty applying to conduct that was not intended to be antagonistic to a consumer's health interests.

Another feature of the MHR privacy framework that has been questioned is the data breach notification obligation (discussed below). The notification obligation applies to any participant in the MHR system. There is keen interest in reviewing whether the obligation is appropriately framed so that it is not incompatible with the fluidity that can be a feature of digital health research and innovation.

The privacy and security safeguards in the MHR legislation can also be relevant in other ways. For example, the way the safeguards are framed will be relevant to the use of MHR data for public health research, or in digital health innovation work by software app developers. The issues those examples raise are multi-faceted, traversing law, policy and community interest.

Responses to general themes

1. Is MHR providing important practical healthcare benefits to consumers and providers? Could more be done to improve the benefits that are provided? Could more be done to generate better public understanding of the healthcare benefits of MHR?

2. Are there any particular features of MHR that make healthcare recipients or providers reluctant or disinclined to use it? Is there unnecessary complexity in MHR legislation?

3. Is the scope and purpose of MHR clear? Is there a need to define or explain MHR more clearly, and how it relates to other health information systems and practices?

4. Should the future direction of MHR be spelt out more than at present? What issues should be covered in a futures roadmap or strategic plan?

4. PROMINENT ISSUES REGARDING THE MY HEALTH RECORDS ACT

This section discusses issues that were frequently raised during the early consultation sessions for this review, and also in the Terms of Reference. Most of these issues have been prominent topics of discussion in the design and operation of the MHR system.

Prohibition on using My Health Record-sourced information for insurance and employment purposes

A central principle of the MHR system is that an individual's MHR information is made available to others only for the purpose of providing healthcare to the relevant person. To strengthen that principle, the MHR Act was amended in 2018 to restrict use of an individual's MHR information by insurers and employers. This was done to allay concern that insurers and employers would have growing interest in accessing client MHR records after the opt-out period concluded and MHR content volume would increase.

The MHR Act provides that an individual's MHR information cannot be used for a 'prohibited purpose'. This includes deciding whether a contract of insurance applies to a particular event, or making an employment decision relating to a healthcare recipient.

The prohibition can apply not only to an insurer or employer, but also to a health practitioner who uses an individual's MHR in preparing a report for an employer or insurer. Breach of the prohibition can be both a criminal offence and attract a civil penalty.

The prohibition has been criticised as being unnecessarily broad and imprecise. The new offence provision may deter a health practitioner from accessing or using a consumer's MHR record if the information accessed may be used in a document that could be relied on by an insurer or employer. The prohibition can also inhibit a practitioner from assisting a patient who seeks a report for an insurer or employer that outlines the patient's medical history.

The prohibition can also throw up special problems – for example, for a health practitioner who is supported by an employer to provide health services in a remote mining town.

Control of a minor's My Health Record

A person aged under 18 (a minor) may have an MHR, usually through Medicare registration after birth. Since 2018, the MHR rules applying to the control of a record differ according to whether a child is aged 0-13 or 14-17.

The MHR of a child aged 0-13 is controlled by a person who has parental responsibility for them (called an 'authorised representative').

A child aged 14-17 controls their own MHR and can, for example, set privacy access controls that regulate which healthcare provider organisations can view either the record or specific documents. A parent or guardian cannot access the child's record unless appointed

with the child's concurrence as an authorised representative (who substitutes for the child) or a nominated representative (who may exercise concurrent powers).

The 2018 changes have introduced some anomalies into the MHR scheme. There is no clear procedure for managing the MHR of a child aged 0-13 who does not have an authorised representative.

Nor is there a procedure for a third party to apply to be an authorised representative of a child aged 14-17 who has impaired decision-making capacity due to a disability or complex health condition. Such a procedure applies for adults. Overall, there does not appear to be a strong rationale for applying different MHR rules to adults and to minors aged 14-17.

There are also different age settings for information access and control in MHR and in other systems. For example, the age a child can obtain a separate Medicare card is 15. Some states and territories upload medical history information for minors into MHR, but have separate local laws that govern access to that information in the possession of the state or territory.

Healthcare recipient controls in My Health Record

Consumer control is a foundation principle of the MHR system, as reflected in many features – the 'My Health Record' title; individual participation in MHR is voluntary and can be reversed; a person controls the personal health information uploaded to their MHR, and can remove a record; and they can set access controls on who can access that information.

While there appears to be general acceptance of the principle of consumer control, questions have nevertheless been raised about whether some adjustments could be made as to how that principle applies. This may benefit healthcare recipients, and also make healthcare providers more inclined to use MHR.

One issue is that documents can be 'hidden' or concealed by the record holder. A healthcare professional will not know if a document has been concealed, which may undermine practitioner confidence in the reliability of MHR and encourage scepticism. One option may be to note in MHR that a document is hidden, but not reveal anything further about that document. The countervailing view is that this may be awkward for a healthcare recipient when speaking to a clinician, and that all patient interactions should in any case be approached afresh and with a questioning and open mind to elicit relevant information.

Another issue has to do with the option available to a healthcare provider to override a consumer's access controls when consent cannot readily be obtained and MHR access is reasonably necessary to prevent a serious threat to the person's life, health or safety. Use of this power triggers a reporting and auditing process. However, the provider may not know if there was an access control in place and whether reliance on this override power was necessary. The suitability in a clinical setting of the demanding 'serious threat to life, health or safety' standard has also been questioned.

A similar issue that has been raised is whether there should be a special authorisation for a hospital emergency department to access a consumer's MHR without having to explore other access options with the individual. The viability of this option could depend on whether suitable criteria could be devised to control when and by whom this override option could be used.

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

Neither the Commonwealth *Privacy Act 1988* nor the MHR Act provide comprehensive guidance as to the information governance rules applying to the personal information of a deceased person.

The MHR Act requires the Agency to cancel the registration of a healthcare recipient upon being notified of the person's death. However, 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).

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 MHR Act states that it is 'a national public system for making information about a healthcare recipient available *for the purpose of providing healthcare to the recipient*' (s 4). It is manifest that a deceased person can no longer receive healthcare. However, section 15 of the MHR Act also gives the Agency (as System Operator) functions that extend beyond the provision of healthcare – for example, providing data for public health and research purposes.

A record of a deceased person can be accessed or used under the MHR Act for some purposes. For example, the MHR Act provides in general terms that a coroner can direct the Agency to disclose health information in the record. A court or tribunal can also order disclosure, but for limited purposes.

However, the MHR Act is less clear on other issues that have arisen, such as 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? Or, can documents be added to the record after death, such as an autopsy report or a death certificate?

A variation of those issues is that a healthcare provider who is unaware of a person's death may have accessed their record in the period between death and cancellation of the person's registration by the Agency. Again, the MHR Act provides that a registered provider is authorised to access a person's record 'for the purposes of providing healthcare' to that person (s 61). Unauthorised access is an offence.

Concern has also been raised regarding the record of a deceased child. While the child is alive their record can be cancelled by their authorised representative (usually a parent) and all information in the record is then deleted. After death, the authorised representative can no longer cancel the record and health information in the record is retained for 30 years (or longer). The authorised representative cannot access the record at that time.

There is no consistent approach in Australian privacy law as to the records of deceased persons. The Commonwealth *Privacy Act 1988* does not apply to the personal information of a deceased person, whereas some state privacy laws do.

Facilitating use of My Health Record patient data for research and public health purposes

Privacy law differentiates between the primary and secondary use of data that has been collected by government. Different legal rules and administrative arrangements may apply to ensure that a secondary use is appropriate and that privacy and security safeguards are properly met.

The primary use of MHR data is to provide healthcare to individuals. Use of that data for public health research would be a secondary use.

The MHR Act recognises that public health research would be an appropriate secondary use of MHR data. A function of the Agency is to prepare de-identified data, with the consent of the record owner, for research and public health purposes; and the MHR Act empowers the Health Minister to publish a Rule to prescribe a framework for that to occur.

Individuals with a MHR can choose not to share their data for public health and research purposes. They can log into their MHR and update their MHR settings and choose not to participate.

A *Framework to guide the secondary use of My Health Record system data* (the Framework) was developed in close consultation with stakeholders in 2017.

Key features of the Framework's governance structures include establishing a Data Governance Board to assess applications to use patient data; a public register of research approvals; a preservation of the MHR principle that an individual could restrict access to their record and deny use of personal data in research; a prohibition against use of MHR data solely for commercial purposes or by insurers; and oversight by the Information and Privacy Commissioner.

Elements of the Framework were legislated as part of the government's 2018 amendments to the My Health Records Act 2012. They include identifying the Australian Institute of Health and Welfare (AIHW) as the data custodian; authority to establish a Data Governance Board (the Board) which will consider applications for data; and authority to develop a Rule that will impose requirements on persons handling My Health Record information for research and public health purposes.

There is a strong trend in government to increase the availability and productive use of de-identified data by researchers and policy planners. A guiding principle is that data held by government is a valuable national asset that should be used more strategically to improve service design and delivery, inform and better plan government programs, and support research and innovation. The Government has signalled its support for this approach in releasing in September 2020, through the Office of the National Data Commissioner, an exposure draft Data Availability and Transparency Bill.

The use of MHR-sourced health information for research or public health purposes could assist in identifying priority health issues for different age, community and geographic cohorts, lead to new health treatments and strategies, and make healthcare delivery more efficient and accessible.

The Department of Health (the Department) continues to progress the implementation of the Framework's governance structures in collaboration with the Agency and the AIHW.

Privacy settings in the My Health Records Act

Protection of individual privacy has been a major topic of discussion and planning in the development of the MHR system. This is reflected in the submissions to and consideration of issues by the Senate Community Affairs Reference Committee's 2018 Inquiry Report into the *My Health Record system*. The management of privacy issues was likewise a central issue in a 2019 report of the Auditor-General, *Implementation of the My Health Record System.* Health privacy issues were also at the fore once again in public discussion in 2020 of the Government request that all Australians download the COVIDSafe app.

A common view is that privacy protection has been well-managed in the design of the MHR system. Individuals can choose whether to have an MHR and can control the content of and access to their record. Healthcare providers must be registered to participate in MHR and their transactions in the system are recorded and can be audited. The Information Commissioner has oversight of whether privacy requirements are being observed, through functions such as complaint handling, own motion investigations, compliance assessments, receipt of data breach notifications, and by access to enforcement powers that include determinations, enforceable undertakings, injunctions and civil penalties. A range of criminal and civil penalties apply to the unauthorised collection, use and disclosure of MHR patient information.

A corresponding view is that privacy protection has also been well-managed in the operation of the MHR system. The Agency reported in 2019 that there have been no purposeful or malicious attacks that compromised the integrity or security of the system. The OAIC annual report for the same reporting year listed 69 data breach notifications to the OAIC, of which most were attributable to administrative error (such as intertwined records), 3 involved unauthorised access to a consumer's record, and 7 involved suspected Medicare fraud that was logged in information uploaded to MHR.

The majority of enquiries and complaints received directly by the Agency and externally by the Information Commissioner were related to the transition in the reporting year to an opt-out system and to a record holder's ability to delete a record. The Agency received 304 complaints in the 2018-19 reporting year, and 10,000 enquiries. The Information Commissioner received 57 complaints and 145 enquiries.

The 2019 Auditor-General report found that MHR privacy and security risks were 'largely well managed', and were appropriately informed by privacy risk assessments and cyber security measures. The Auditor-General's five recommendations, accepted by the Agency and the Department, were for the Agency to update the risk management framework after conducting an end-to-end privacy risk assessment of MHR; for the Agency and the Department to review monitoring procedures for the use of the emergency access function and reporting that use to the Information Commissioner; for the Agency to develop an assurance framework for connecting third-party software to MHR; for the Agency to develop a strategy for monitoring compliance by external parties with legislative requirements relating to security; and for the Agency to develop and implement a program evaluation plan for MHR, including forward timeframes and sequencing of measurement and evaluation activities across the coming years, and report on the outcomes of benefits evaluation.

Any change to the MHR Act or operating procedures may require a fresh consideration of privacy safeguards. Examples discussed above would be changing the access control procedures for concealed records and the use of the emergency access function, and allowing accredited researchers to use de-identified MHR patient data for public health research.

Privacy issues similarly arise in relation to any change to allow third party software developers to connect to MHR. Among the issues that would require consideration are the adequacy of existing privacy safeguards, the reach of the Information Commissioner's remit to examine privacy compliance, and the current prohibition in the MHR Act against taking MHR health information outside Australia.

Two other specific privacy issues discussed below are the jurisdictional range of the Information Commissioner's oversight role, and the data breach notification requirements in the MHR Act.

Privacy oversight by the Office of the Australian Information Commissioner

The oversight jurisdiction of the Information Commissioner under the Privacy Act is extensive. It extends to all Australian Government agencies and ministers, contracted service providers, health service providers, credit reporting bodies, and any business that trades in personal information (which could include an app developer). That extensive jurisdiction enables the Information Commissioner to oversight most activities occurring under the MHR Act.

The Information Commissioner does not have jurisdiction over state authorities – in line with Australian federalism. In all but two states (South Australia and Western Australia) there are state privacy or health information laws that apply to state authorities. Administrative arrangements also exist in all states to monitor privacy compliance.

The limitation on the Information Commissioner's jurisdiction has mainly been an issue when the OAIC is undertaking an assessment of whether there has been adequate privacy compliance in using MHR patient information in a health facility or program that is operated jointly by a state authority and a private sector body. The OAIC is required to conduct between 4-6 assessments each year, pursuant to a memorandum of understanding with the Agency. The OAIC can assess the activities of the private sector body but not the state authority. There is a potential blank spot if it is unclear whether an activity was undertaken by a state or private sector staff member, their interaction was fluid, or the staff member is unclear about which privacy rules apply.

A similar issue arose in relation to the Information Commissioner's role in monitoring privacy compliance with the COVIDSafe app. The Privacy Act was amended in May 2020 to protect data collected or generated through the app, including information given to a state or territory health authority for contact tracing. Information collected locally by the state or territory authority is subject to state/territory law only, and not to the Commonwealth Privacy Act or the Information Commissioner's oversight jurisdiction.

The Privacy Act enables a state or territory to request the Commonwealth to make a regulation that extends the Act to the activities of a state or territory authority. However, the discretion rests with the state or territory to initiate that coverage.

Another privacy protection measure that may be adaptable to the MHR setting is the new Consumer Data Right (CDR) introduced in 2020. To bolster consumer choice, the CDR enables a person to direct an organisation (such as a bank) to share their data via a secure online system with a competitor organisation accredited by the Australian Competition and Consumer Commission. The OAIC has a role in monitoring whether the accredited recipient complies with privacy safeguards and security requirements. The *Competition and Consumer Act 2010* (Cth) s 56EY also provides a new right of action for damages against an organisation that breaches the privacy safeguards applying to the CDR.

The CDR privacy protections may be adaptable, for example, to MHR patient information that is shared with a third party such as a software developer.

Data breach notification under My Health Records Act

The MHR Act contains a data breach notification (DBN) scheme that differs from the DBN scheme introduced into the Privacy Act in 2018.

The notification obligation in the MHR Act applies to the Agency, to registered healthcare providers, registered portal and repository operators, and to contracted service providers. They must notify the OAIC of an actual or possible unauthorised collection, use, or

disclosure of MHR patient information, and of any event (whether or not a contravention of the MHR Act) that may compromise the security or integrity of the MHR system.

The notification obligation in the Privacy Act applies to entities that are subject to that Act, and requires notification to the OAIC of a loss or unauthorised access to or disclosure of personal information that could result in serious harm to an individual.

The justification for a separate MHR notification scheme is that MHR contains a large and growing volume of sensitive personal health information that should be protected by a tailored scheme.

Two criticisms have nevertheless been made of the MHR notification scheme. One is that it is confusing for organisations that are subject to both the MHR Act and the Privacy Act to work under two different sets of DBN rules. This can be another practical disincentive for an organisation to use MHR. Harmonisation of DBN requirements would be a sensible and welcome option.

A second criticism is that the MHR Act requirements are more demanding and indeterminate than the Privacy Act requirements. The key criterion in the Privacy Act is that a data breach could result in 'serious harm' to an individual. That aligns with a central purpose of a DBN obligation – to notify individuals who may be affected by a data breach so that they are properly informed and can if necessary take precautionary action.

By contrast, it may be unclear or speculative whether an event may compromise the 'security or integrity' of the MHR 'system'. Nor is there any requirement that the matter being notified to the OAIC posed any risk to a healthcare recipient. It is said that many MHR matters notified to the OAIC posed no such risk and were inconsequential so far as personal privacy protection risks were concerned. Examples are an incorrect Medicare data entry that was promptly rectified, and an unauthorised but unsuccessful attempted data entry on an administrative support system.

My Health Record business participation rules

Several business architecture features of the MHR Act and Rules have been singled out as being anomalous or problematic.

One is the authority to author and upload a shared health summary that can be consulted by other healthcare providers who have access to a consumer's MHR. The MHR Act makes special mention of shared health summaries, in anticipation of this being a key document that provides a holistic health overview at a particular point in time of a consumer's medical conditions, medications, immunisations and allergies and adverse reactions.

The authority to author a shared health summary is limited, consistent with its importance. Those who can author one are a medical practitioner, a registered nurse or an Aboriginal or Torres Strait Islander health practitioner with a specified qualification.

It has been suggested that the category of authorised people should be widened to include midwives who are not registered nurses. They are a large and growing profession, represented by the Australian College of Midwives, and provide an essential health maternity service to many women.

Another aspect of the shared health summary framework that has caused difficulty is that the summary must have been prepared by a healthcare recipient's 'nominated healthcare provider'. This in turn is defined in the MHR Act as being a provider that has an agreement in force' with the healthcare recipient. That is a cause of uncertainty in the absence of a formal

agreement, which may not be typical in many clinical practices. The assumption too that there can only be one nominated provider may be at odds with the healthcare consultation patterns of many individuals.

Another framework concept in the MHR Act is the phrase 'participant in the MHR system'. This includes the System Operator, registered healthcare provider organisations, repository and portal operators and contracted service providers. Many of the compliance obligations in the MHR Act are imposed on participants.

A group that may not presently come within that defined grouping are software developers. This will be relevant if the MHR system evolves to facilitate their capacity to provide a more personalised health service through functions such as smartphone apps.

Interaction of the Healthcare Identifiers Act and the My Health Records Act

The interaction of the MHR Act with the *Healthcare Identifiers Act 2010* (Cth) occurs at several levels.

The most important is the operational or functional level. Healthcare identifiers are assigned by the HI Service to healthcare participants (an IHI), individual healthcare providers (HPI-I) and healthcare provider organisations (HPI-O). Each identifier is unique and enables registration and participation in MHR.

At the next level up, the healthcare identifier supports monitoring and auditing activity within MHR. Entry to and activity within the system by an individual provider or healthcare organisation can be traced as their HPI-I/O will leave an audit log.

Another interaction level relates to the evolution of Australia's *National Digital Health Strategy*. There are additional uses of healthcare identifiers that are being rolled out – for example, e-prescribing. Others have been suggested – for example, using an HPI-I for secure messaging, and for other government business such as MBS claiming. Operational links can be established between those digital processes and MHR.

There have been criticisms that are relevant to MHR about healthcare identifier practices at each of those levels. These matters are covered in the 2018 *Healthcare Identifiers Act and Service Review – Final Report*.

Another operational issue has to do with the range of healthcare providers or ancillary support services that are eligible to be assigned an HPI-I/O. Two examples where doubt exists are sonographers and primary health networks. Generally, an expansion of the range of those eligible for an identifier could lead to more and diverse health information being uploaded to MHR.

Questions have also been raised about whether there is a need to tighten the criteria for the Agency to grant an exemption from the requirement that an HPI-I be included in a clinical document uploaded to MHR. Exemptions have been granted widely to public and private sector healthcare providers, for practical workflow reasons to support document uploading.

An issue regarding MHR monitoring and auditing is that those processes can be blunted when a single HPI-O is granted (as it has been) to an entire state or health organisation that operates multiple sites. It may not be possible to ascertain which organisation or facility has accessed a consumer's MHR. This may be a special concern to a consumer who has imposed access controls that allow limited access to their record.

Lastly, there is a view that more active use of healthcare identifiers beyond MHR (and the HPI-Is in particular) would reinforce the evolution of a dynamic and integrated digital health

system in Australia. This explains the recommendation of the 2018 HI review that the Agency develop a future roadmap and health technology strategy to encourage broader adoption and use of healthcare identifiers.

Another healthcare identifier dimension that is under-developed is the adoption by states and territories of the commonwealth identifier. There are understandable reasons why another jurisdiction may develop a separate identification system that is tailored to its own health framework and information technology platforms and software. However, the adoption of common or interoperable identifiers can make it easier to upload to MHR a greater range and volume of patient health information.

Revising and updating the My Health Records Act

This review has been informed of a range of specific aspects of the MHR Act that warrant reconsideration and possible amendment. Many of these are technical in nature and are more suited to targeted consultation rather than a public submission process through this issues paper. Any issues that are taken up will be dealt with in the published report from this review, when there is likely to be a further opportunity for public comment.

It is nevertheless appropriate to note, by way of illustration, a few issues that have been raised regarding the suitability of the statutory provisions relating to the System Operator's (the Agency's) powers, functions and responsibilities:

- The lack of definition of the terms 'security' and 'integrity' in the MHR Act causes uncertainty as regards the System Operator's responsibility to safeguard those values, for example, by cancelling the registration of a healthcare provider organisation, notifying a data breach to the OAIC, or suspending access by a consumer or participant.
- The functions of the System Operator could be extended to expressly cover activities such as removing or deleting a wrong record, undertaking data analytics or clinical safety analyses, or adopting a more proactive role such as sending vaccination reminders to consumers.
- The System Operator does not have explicit authority to undertake testing in the live MHR environment, for example, by creating a 'test' patient or IHI independently of privacy requirements.
- The System Operator is hampered in identifying who within an organisation has accessed MHR, for example, because multiple state health facilities may be covered by the same HPI-O.
- The System Operator has limited authority to resolve a dispute between the authorised representatives of an MHR record holder regarding the cancellation of the record.
- The System Operator does not have a straightforward power to remove a document from a consumer's MHR, for example, because it is in the wrong record.

Responses to specific issues

5. Should the prohibited purpose provision in the MHR Act be amended to reduce the adverse impact on health practitioners? How could this best be done – for example, by excluding specific conduct from the scope of the prohibition, or removing the penalty for a breach of the prohibition?

6. Should the MHR Act provisions relating to managing the health information of minors be revised? For example, should the MHR age category of 14-17 be combined with the age

category 18 and above? Have the age settings for information access and control under MHR that are different to those in Medicare or in state and territory laws given rise to any issues that should be addressed?

7. Should adjustments be made to how the principle of consumer control is embodied in MHR legislation? Is it appropriate to have a category of hidden documents? Should the emergency override function be reformulated?

8. Should the MHR Act contain more comprehensive guidance regarding access to and use of health information in the MHR of a deceased person? What rules would be appropriate?

9. What key factors should be taken into consideration during the development of the Rule that will support implementation of the *Framework to guide the secondary use of My Health Record system data*, to ensure there is a robust legal framework for that to occur?

10. Should any aspects of the privacy protections in MHR legislation be revisited and possibly altered – either to ensure better privacy protection, or to facilitate digital health innovation?

11. Has the Office of the Australian Information Commissioner been given an appropriate role and powers to oversight the privacy and data handling aspects of the MHR system?

12. Should the data breach notification scheme in the MHR Act be revised and possibly harmonised with the data breach notification scheme in the Privacy Act?

13. Are appropriate arrangements in place for handling complaints about MHR matters?

14. Should the category of people authorised to author and upload a shared health summary be widened, and in particular, to include a midwife who is not a registered nurse?

15. Should the MHR Act provisions relating to nominated healthcare providers be revised to make it easier to identify who is the nominated provider?

16. Should changes be implemented that provide better support for MHR by the Healthcare Identifiers Act?

17. Are the criminal and civil penalty provisions in the MHR Act appropriate, or do they act as a practical deterrent to the more effective operation of MHR? If so, what changes should be made?

18. Are the functions, powers and responsibilities of the System Operator adequately and suitability defined in the MHR Act?

19. Are there any particular aspects of the MHR Act that should be reconsidered and possibly amended to better support the policy objectives of the MHR system?