Review of the My Health Records Legislation

Final Report

Professor John McMillan AO

1 December 2020

Contents

List of acronyms

Acronym	Definition
AAT	Administrative Appeals Tribunal
ABS	Australian Bureau of Statistics
ACPA	Advance Care Planning Australia
ADF	Australian Defence Force
ADSP	Accredited Data Service Provider
Agency	Australian Digital Health Agency
Agency Rule	*Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016*
AHPRA	Australian Health Practitioner Regulation Agency
AIHW	Australian Institute of Health and Welfare
AMA	Australian Medical Association
ANAO	Australian National Audit Office
APF	Australian Privacy Foundation
APPs	Australian Privacy Principles
Assisted Registration Rule	*My Health Records (Assisted Registration) Rule 2015* (Cth)
CDR	Consumer Data Right
DAT Bill	Data Availability and Transparency Bill
Defence	Department of Defence
ePIP	Practice Incentives Program eHealth Incentive
FOI	Freedom of information
FOI Act	*Freedom of Information Act 1982* (Cth)
HI	Healthcare Identifier
HI Review	Healthcare Identifiers Act and Service Review
HI Act	*Healthcare Identifiers Act 2010* (Cth)
HI Service	Healthcare Identifiers Service
HPI-I	Healthcare Provider Identifier – Individual
HPI-O	Healthcare Provider Identifier – Organisation
IHI	Individual Healthcare Identifier
MADIP	Multi-Agency Data Integration Project
MBS	Medical Benefits Scheme
MHR	My Health Record
MHR Act	*My Health Records Act 2012* (Cth)

Acronym	Definition
MHR Rule 2016	*My Health Records Rule 2016* (Cth)
MIGA	Medical Insurance Group Australia
MLC	MLC Life Insurance
NHMRC	National Health and Medical Research Council
OAIC	Office of the Australian Information Commissioner
PCEHR	Personally Controlled Electronic Health Record
PBS	Pharmaceutical Benefits Scheme
RACGP	Royal Australian College of General Practitioners

List of recommendations

Recommendation 1

The Australian Government review the current Budget funding arrangements for My Health Record (MHR) system activity and, in particular, review the desirability of:

- moving the current annual budgetary funding arrangement for the role of the Australian Digital Health Agency, as the System Operator for MHR, to a new arrangement of an annual appropriation tied to a forward estimate
- direct appropriation to the Office of the Australian Information Commissioner for its privacy oversight work in relation to MHR, to replace the current arrangement of an appropriation to the Australian Digital Health Agency that is transmitted to the Office of the Australian Information Commissioner under a memorandum of understanding between both agencies.

Recommendation 2

The Department of Health review the principles for incentive payments being made under the Practice Incentives Program eHealth Incentive (ePIP) to general practices that participate in My Health Record. The review should examine whether:

- the current practice of tying incentive payments to the upload of shared health summaries to MHR is achieving the objectives of MHR
- incentive payments should instead be made for other general practice activities that can support the security, integrity or effectiveness of MHR.

Recommendation 3

The Australian Government initiate a review of practical incentives that could be adopted to support 3 strategic objectives for MHR stated in the National Digital Health Strategy – 'increased consumer participation', 'increased core clinical content', and 'extensive adoption by healthcare providers'. The review should examine options for tying eligibility criteria for specific government health benefit payments to those strategic objectives.

Recommendation 4

The Australian Digital Health Agency develop and publish a series of 'roadmap' or strategic planning documents as the basis for consultation with stakeholders on the future planning directions for MHR. The roadmap documents should deal as specifically and discretely as possible with special interest topics raised by stakeholders, including as part of this review. Examples include:

- education programs that illustrate the benefits of MHR for consumers and that could stimulate active participation by consumers
- strategies for encouraging participation in MHR by groups or cohorts that are presently under-represented, such as specialists, allied and community health, and aged care
- consumer options for accessing MHR through platforms other than myGov, including through mobile devices
- adjustments that could be made to MHR operating principles in response to distinctive issues in areas such as mental health or hospital emergency clinics
- strategies for facilitating participation in MHR by large employers such as the Australian Defence Force.

Recommendation 5

The Department of Health consider the desirability of amending the *My Health Records Act 2012* (MHR Act) to provide more explicitly that the functions of the System Operator listed in s 15 of the Act include:

- using health information from the MHR system for the purpose of performing a function or exercising a power under the Act (and, in particular, to perform the function of establishing and maintaining a reporting service in s 15(d))
- establishing and conducting testing in both a test environment and the MHR system (or live environment)
- testing MHR system data to assess if it conforms to specifications and standards for the MHR system
- undertaking analysis of clinical governance and clinical safety in MHR system data and in the MHR system
- notifying registered healthcare recipients and registered healthcare provider organisations of any matters arising from or connected to the operation of the MHR system.

Recommendation 6

The Department of Health consider the desirability of amending the MHR Act to:

- authorise the System Operator to impose a charge for specified activities
- extend the terms of s 6(1A)(b) to the circumstances of any healthcare recipient – that is, to authorise the System Operator not to recognise a person as an authorised or nominated representative of a healthcare recipient if doing so is likely to put at risk the life, health or safety of the healthcare recipient or another person
- authorise the System Operator to initiate action to remove a representative's access to a person's MHR if the System Operator has reason to believe that the representative is unable or unwilling to act in a way that promotes the personal and social wellbeing of the healthcare recipient; or, in the alternative, to make a representative's obligation under s 7A of the MHR Act to act in accordance with a healthcare recipient's will and preferences an eligibility requirement for a person to have access to the healthcare recipient's MHR
- provide that the System Operator must be satisfied that all representatives of a healthcare recipient are in agreement before the System Operator is required to act on the instructions of any one representative to cancel a person's MHR registration and destroy health information in their record
- consolidate and revise the provisions of the MHR Act that authorise the System Operator to manage and control the upload, removal and destruction of records in the MHR system.

Recommendation 7

The Department of Health review (and prepare a report on) Commonwealth, state and territory laws and administrative protocols that regulate the capacity of government entities to provide information to the System Operator that may be relevant to the responsibilities of the System Operator under the MHR Act to take action to protect the life, health or safety of a healthcare recipient.

Recommendation 8

The MHR Act s 75 be amended to introduce data breach notification requirements that are, to the extent practicable, similar to those in Part IIIC of the *Privacy Act 1988*.

Recommendation 9

The Department of Health consult with state and territory health agencies as to the options for applying the Australian Information Commissioner's functions and powers under the MHR Act to the actions of state and territory authorities.

Recommendation 10

The MHR Act s 73 be amended to include compliance by the System Operator with a provision of Part 3 of the Act as a matter that can be investigated by the Australian Information Commissioner under s 73 of the Act.

Recommendation 11

The MHR Act s 73A be amended to confer a more general authority on the Australian Information Commissioner to disclose information or documents to the System Operator, the Department of Health and Services Australia for the purpose of the commissioner exercising powers or performing functions or duties under the Act.

Recommendation 12

The Department of Health consider the desirability of amending the *Healthcare Identifiers Act 2010* (Cth) s 14(2) to take account of any changes that may be made to the provisions of the MHR Act relating to prohibited purposes, in response to Recommendation 18 in this report.

Recommendation 13

The Department of Health consult with the Australian Digital Health Agency (as System Operator for the MHR system) and Services Australia (as Service Operator for the Healthcare Identifiers Service) regarding the use of Healthcare Provider Organisation Identifier structures by healthcare provider organisations in a way that runs counter to the objective of transparency in revealing access events in the MHR system. The purpose of the consultation should be to resolve the question of whether there is a problem that should be addressed either by administrative compliance action by the System Operator and the Service Operator or by amendment of the MHR Act or *My Health Records Rule 2016.*

Recommendation 14

The Department of Health, in consultation with the Australian Digital Health Agency, review the pattern of decisions by the System Operator granting exemptions from the requirement to include an Individual Healthcare Provider Identifier in a clinical document that is uploaded to the MHR system. The purpose of the consultation should be to decide if the criteria for granting an exemption should be more strictly applied.

Recommendation 15

The MHR Act s 45 be amended to provide that it is a condition of registration for a healthcare provider organisation that it will not *knowingly* upload to a repository a record that was prepared by an individual healthcare provider who did not meet the requirements specified in s 45.

Recommendation 16

The Department of Health consider whether amendment of s 64 of the MHR Act is desirable:

- to specify less demanding criteria for emergency record access
- to remove the requirement that every use of the power be notified individually to the System Operator
- to provide that s 75 of the MHR Act (data breach notification) does not apply to an action taken under s 64.

The review of s 64 by the Department of Health should be undertaken after completion of any action currently being taken by the department and the Australian Digital Health Agency, in consultation with the Office of the Australian Information Commissioner, in response to Recommendation 2 of the report of the Australian National Audit Office, *Implementation of the My Health Record system* (2019).

Recommendation 17

The *My Health Records Rule 2016*, rr 7 and 8, be amended to require that the Record Access Code and Limited Document Access Code are displayed in clinical software only where a healthcare recipient has applied an advanced access code.

Recommendation 18

The provisions of the MHR Act relating to prohibited purposes be amended to exclude their application to:

- use by a healthcare provider of health information included in a registered healthcare recipient's MHR if the use:
  - is in a report to an insurer or employer relating to the healthcare recipient
  - the report was prepared by the healthcare provider at the request of the recipient (or their representative)
  - the healthcare provider is reasonably satisfied that the use of the health information is in the recipient's best interests and the recipient was not subject to any pressure by the insurer or employer to allow the use of the information
- use by an insurer or employer of health information included in a registered healthcare recipient's MHR if:
  - the information is included in a report prepared by a healthcare provider
  - the healthcare provider has confirmed in writing that he or she is satisfied that use of the health information is in the recipient's best interests and the recipient was not subject to any pressure by the insurer or employer to allow the use of the information.

Recommendation 19

The Department of Health consider the desirability of amending the MHR Act to exempt some employment categories from the scope of the prohibited purposes provisions, such as employment in the Australian Defence Force or Defence Reserves.

Recommendation 20

The MHR Act s 6(1)–(2) be amended to provide that a healthcare recipient aged under 14 may take control of their own MHR by establishing to the satisfaction of the System Operator that the recipient wants to manage his or her own record and is capable of making decisions for himself or herself.

Recommendation 21

The Department of Health consult with states and territories on any concerns they may hold that safety net powers in the MHR Act are ineffective in ensuring that the life, health or safety of a child is not put at risk by an unsuitable person being eligible to be a representative of the child under the Act.

Recommendation 22

The MHR Act be amended to apply the provisions of the Act that relate to healthcare recipients aged 18 or above to healthcare recipients aged 14–17 (and thereby removing the provisions of the Act that separately relate to healthcare recipients aged 14–17).

Recommendation 23

The MHR Act be amended to provide that the System Operator may recognise the appointment of a person aged under 18 as an authorised or nominated representative of a healthcare recipient if the System Operator is satisfied that the person would be an appropriate person to perform that role.

Recommendation 24

The Department of Health consult with the Chief Executive Medicare and the Australian Digital Health Agency on administrative changes that could be implemented to resolve any inconsistent practices that may exist between Medicare and MHR regarding access by a child age 14 above or their representative to Medicare claims information relating to the child.

Recommendation 25

The Department of Health consider whether amendments should be proposed to the provisions of the MHR Act and MHR Rule 2016 that deal with managing and accessing the MHR of a deceased person, with particular reference to:

- whether an authorised or nominated representative should have continued access to the MHR of a deceased person and can request the System Operator to cancel the record or destroy information in the record
- the conditions that should apply to any access that an authorised or nominated representative has to a deceased person's MHR
- the criteria to be applied in releasing health information from a deceased person's records for matters such as public health research, clinical review of death and ascertaining organ donor consent
- access to and use by a nominated healthcare practitioner to the MHR of a deceased person
- the provisions of the Act that may result in an offence being committed by a healthcare provider who has accessed the MHR of a deceased person
- the length of the period (between 30 and 130 years) for which the record of health information of a deceased person is retained in the National Repositories Service.

Recommendation 26

The Australian Government appoint as early as practicable – and, if appropriate, on an interim basis – the members of the Data Governance Board established in Part 7 of the MHR Act.

Recommendation 27

The Minister for Health make a Rule under the MHR Act s 109(7A) to prescribe a framework to guide the collection, use and disclosure of MHR patient health information for research or public health purposes. The Rule should take account of the data sharing frameworks outlined in the *Framework to guide the secondary use of My Health Record system data* (2018) and the Data and Transparency Bill 2020.

Recommendation 28

The Department of Health consider the desirability of amending the MHR Act ss 15(ma), 82–96J, 109(7A) and 109A to ensure consistency with the provisions and terminology in the Data and Transparency Bill 2020.

Recommendation 29

The MHR Act be amended to merge the provisions in Schedule 1 of the Act (introducing the opt-out model) with other provisions in the Act dealing with the same issues.

Recommendation 30

The *My Health Records (Assisted Registration) Rule 2015* be repealed for the reason that it is redundant following the implementation of the opt-out model. Consideration should be given to preserving r 8 of the Rule, which requires a healthcare provider organisation to exercise reasonable care in making a declaration to support a healthcare recipient's assertion of parental responsibility for a person.

Recommendation 31

The Australian Digital Health Agency consider publishing more extensive guidance on how the terms 'security' and 'integrity' may be applied in the different contexts in which those words are used in the MHR Act.

Recommendation 32

The MHR Act ss 5 and 10 be amended to provide that the System Operator may publish guidelines that prescribe which registered healthcare providers may prepare a shared health summary and the procedure to be followed to upload the shared health summary to a healthcare recipient's MHR.

Recommendation 33

The Department of Health consider the desirability of amending the MHR Act to:

- exclude de-identification of health information in a healthcare recipient's MHR from the definition of 'use' in s 5 of the Act
- clarify the roles of the System Operator and the Australian Information Commissioner in exercising powers listed in the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)
- authorise the System Operator to delegate relevant powers to the data custodian (the Australian Institute of Health and Welfare) and the Australian Commission on Safety and Quality in Health Care
- provide that an authorisation that can be exercised under the MHR Act by a contractor can also be exercised by a subcontractor, and (in like circumstances) it can also be exercised under a memorandum of understanding as well as under a contract
- provide that the obligation of the System Operator under s 53 of the MHR Act to notify a healthcare recipient of a proposed decision to cancel, vary or suspend their MHR registration is an obligation to take such steps as are reasonably necessary in the circumstances to notify the proposed decision
- provide immunity in civil proceedings for healthcare providers in respect of action taken by a provider under the MHR Act to collect, use or disclose health information in a healthcare recipient's MHR for the purpose of providing health care to the recipient
- clarify the meaning of the reference in s 68 of the MHR Act to 'the provision of indemnity cover for a healthcare provider'
- provide that a healthcare provider organisation is in breach of the non-discrimination condition in s 46 of the Act only if the organisation unreasonably refuses to provide healthcare services to a person when an access control is in place
- exempt personal and health information in the MHR system from a request for access under the *Freedom of Information Act 1982* (Cth)
- resolve the statutory anomalies in the MHR Act as listed above.

Executive summary

The development of Australia's MHR system

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

MHR is a secure national system for facilitating consumer-controlled access to key health information about individuals for healthcare purposes. Using a federated model, the MHR system draws health information from repositories that are independently managed and makes it accessible to consumers through the myGov platform and to registered healthcare providers through secure portals.

The policy objectives of the MHR system are 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 health care.

MHR began in 2012 as an opt-in system, titled the Personally Controlled Electronic Health Records system (PCEHR). It transitioned to an opt-out model in July 2018. Participation in the scheme remains voluntary for healthcare consumers and healthcare providers.

At October 2020, a total of 22.85 million eligible Australians had an individual MHR, and over 19.9 million had health data entered in the record. Over 2.38 billion documents have been uploaded to MHR, covering all major categories – Medicare documents, shared health summaries, pathology reports, discharge summaries, diagnostic imaging reports, advance care plans and pharmacist shared medicine list. Other information available through MHR includes personal vaccination and organ donor information.

There is active participation in the MHR system by all major healthcare sectors, including public and private hospitals, medical practices, general practitioners, pathologists and pharmacies.

Review of the MHR legislation and system

The *My Health Records Act 2012* (MHR Act) requires the Minister for Health to appoint an individual to review the operation of the Act and to report to the Minister (in effect) by 1 December 2020. Earlier reviews of the operation of the Act have been commissioned by government and undertaken by parliamentary committees, but this is the first independent statutory review of the Act that is framed around public consultation.

The Minister is required to table this report in both houses of Parliament within 15 sitting days of receiving it.

Terms of reference for this review were published in March 2020. Their central focus is whether the MHR Act supports the policy objectives of the MHR system – to coordinate healthcare services provided to people, reduce duplication of treatment and adverse events, and enable active consumer participation in self-care. The review was also to examine MHR issues of special importance such as privacy oversight, the interaction of the *Healthcare Identifiers Act 2010* (Cth) (HI Act) with other laws, and the use of MHR system data for public health research.

Consultation, both publicly and with key stakeholders, was a key activity in this review. The consultation was conducted in 2 stages (that were adapted in response to the COVID-19 pandemic pressures facing Australian governments, the health profession and the Australian community).

Phase 1 in May–August involved consultation with Commonwealth, state and territory agencies, professional and consumer organisations, and researchers.

Phase 2 followed the publication of a short consultation paper in September that presented themes and questions that were drawn from the Phase 1 consultations. Forty-one submissions were received from individual consumers, practitioners, professional organisations and government agencies. Most submissions have been published as attributed or anonymous submissions on https://consultations.health.gov.au/provider-benefits-integrity/legislative-review-of-my-health-record-act-2012/.

The structure of this report aligns with the topics presented in the consultation paper. The consultation paper was organised into 2 parts.

The first part presented 6 general themes (or perspectives) that captured a diversity of views on the MHR Act and system. These are covered in Chapter 3 of this report and are summarised below under the heading 'Perspectives on the operation of MHR'. These 6 themes and the submissions in response range more broadly than the narrower focus of the terms of reference for this review on the provisions of the MHR Act. The operation of the MHR system is a far larger public policy topic. However, these themes and the commentary provide an important perspective when examining the MHR Act, and they can help to shape future lines of inquiry on the Act and its operation.

The second part of the consultation paper highlighted key issues to do with the provisions of the MHR Act that were raised both in the terms of reference and in the Phase 1 consultation. These issues are covered in Chapters 4–12 of this report and are summarised below under the same titles as the chapter headings.

Perspectives on the operation of MHR

Following is a brief summary of the 6 themes outlined in the consultation paper and the comments that were made in response in submissions to this review. Three additional numbered topics (7–9) are added at the end of this section – to highlight some common themes that run through all other issues; to note relevant digital innovation and system projects that under underway within the Australian Digital Health Agency (the Agency); and to make 4 recommendations for government to act on the findings of this review.

1. Strong cross-sectional support for MHR

Support for MHR was expressed in 3 ways – there was endorsement of the contemporary need to integrate health service delivery and technology through a digital records system; examples were given of how individuals have benefited from being able to access MHR information for health consultation purposes; and there was acknowledgement of the compelling design features of MHR (such as consumer control, independent privacy oversight, and modern infrastructure). Many professional associations have published a statement of support on their website.

2. MHR as a supplementary health record

MHR operates alongside and does not aim to replace other health records systems maintained by hospitals, medical clinics / GPs, pathologists, pharmacists and others. Those systems adequately satisfy most record-keeping requirements. A challenge, consequently, is to convey a stronger understanding of where MHR has added value (often described as the challenge of spelling out 'the value proposition' of MHR for different sectors).

3. Mixed assessment of MHR performance

Two common criticisms of MHR are the patchy and out-of-date content in many MHR records; and uneven use among health providers (with specialists, allied health and private pathology being singled out for special mention). This is a source of disappointment and frustration for consumers and providers alike. This has not shaken MHR foundations but led people to ask more constructively how MHR can evolve, how confidence and trust in the system can be strengthened and – at a practical level – how upload and access to MHR content can be improved.

4. Linking MHR to other digital health initiatives

This theme comes up in many ways. One is that commentators point to recent examples of the sharp uptake and reliance on technology in healthcare delivery – such as telehealth, e-prescribing, and electronic messaging. Another is to point out that MHR has to move away from being a static / read only / digital filing cabinet. Linked to that is a call to re-platform MHR – for example, to apply artificial intelligence to reorganise how MHR content is presented and can be searched, to add extra functions such as message alerts for consumers and providers, and to connect with other health information services through smartphone apps and mobile device options.

5. Laying out an MHR roadmap

Submissions to this review strongly endorsed a call for the Agency to prepare a futures roadmap to explain the direction that MHR is expected to take in coming years. The roadmap could elaborate on the priority outcomes and principles set out in *Australia's National Digital Health Strategy*, which was prepared by the Agency. There is particular interest in engaging in practical and detailed discussion on meeting the 3 strategic objectives in the strategy – 'increased consumer participation', 'increased core clinical content' and 'extensive adoption by healthcare providers'.

6. Ensuring the MHR Act supports digital health innovation

The MHR system is anchored in the MHR Act, which is highly prescriptive of the structure and operation of the MHR system. Proposed changes to the MHR system may run up against the rigidity and complexity of the Act. It may, for example, inhibit digital innovation, as organisations that are authorised to access and use health information under the Act do not include software vendors or entities such as primary health networks that facilitate but do not provide health care. There is strong interest in exploring options for providing better personalised health support to individuals, through apps and mobile and wearable device options that allow MHR data to be integrated with other personal health information.

Drawing the themes together

Common themes ran through much of the commentary in the submissions and consultations. There was strong support for discussion to occur, in the context of an Agency roadmap or strategic plan, on specific MHR operational features that have (comparatively) been more or less successful. Three words/concepts capture the disappointment that was often expressed by healthcare provider groups:

- ***'Integration':*** Healthcare providers will commonly access multiple health information sources and would like better MHR workflow integration with other information systems, consistently with maintaining the privacy and security safeguards that are a vitally important feature of the MHR system.
- ***'Seamless':*** Workflow impediments were noted on matters such as software interoperability, logon requirements and screen display of MHR content.

'Perceptions': The benefits of MHR are, it is said, not well understood by healthcare providers and consumers. There is concern that the benefits can be overshadowed by a prevailing feeling that MHR has been disappointing.

The Agency's digital health program

Much of the commentary to this review on options for improving or re-platforming the MHR system align with projects already underway within the Agency. They include a refresh of the National Digital Health Strategy; the modernisation of the national digital health infrastructure that will explore the further use of external repositories and the use of atomic and more structured data; programs to improve specialist adoption of MHR in aged care; a joint project with the Australian Commission on Safety and Quality in Health Care to establish regular use of MHR by clinicians in hospital emergency departments; publication of a National Digital Health Workforce and Education Roadmap, a National Nursing and Midwifery Digital Health Capability Framework, and a Digital Health Capabilities Framework for Medicine; and user testing and research to improve consumer use of MHR, including through the development of mobile solutions for safe and secure access to MHR.

Recommendations

Chapter 3 of the report makes 4 recommendations:

- that government make a longer term funding commitment to the Agency as the System Operator for the MHR system and that it provide a direct appropriation to the Office of the Australian Information Commissioner (OAIC) for MHR oversight (to replace the current arrangement of a funding memorandum of understanding between the OAIC and the Agency)
- that the Department of Health conduct a review of the Practice Incentives Program eHealth Incentive (ePIP), as to the present practice of tying incentive payments to the upload of shared health summaries, and to examine other options for general practitioner incentive payments
- that the government initiate a review of practical incentives that could be adopted to support the objectives of the National Digital Health Strategy for increasing consumer participation in MHR, increasing core clinical content, and extending MHR adoption by healthcare providers
- that the Agency develop and publish a series of 'roadmap' or strategic planning documents as the basis for consultation with stakeholders on issues raised in this review regarding the future planning directions for MHR – such as consumer education programs, consumer access platforms other than myGov and through mobile devices, and for dealing with distinctive issues such as MHR and mental health records and obstacles to MHR participation by large employers such as the Australian Defence Force.

Reform of the MHR Act and supporting legislation

Chapters 4–12 of the report examine problematic aspects of the MHR Act and supporting legislation that were listed in the terms of reference and were noted during consultations for this review. The following summary does not cover all the recommendations made in these chapters for review or amendment of the MHR Act.

1. The System Operator functions, powers and responsibilities

Several aspects of the System Operator's functions are reviewed in Chapter 4 to examine if the Act adequately supports the System Operator's role. Several recommendations are made for revising functions that are narrowly framed and for extending the scope of the System Operator's safety net powers to safeguard the interests of vulnerable consumers.

2. Privacy settings in the MHR Act, data breach notification and OAIC oversight: explanation

Privacy is still an element of most discussions concerning MHR, although the prevailing mood seems to be that privacy has been well managed in MHR design, operation and oversight. There is equally an acceptance that strong privacy and security requirements are essential to retain community support for MHR and must be reflected in any new MHR design proposals.

Recommendations are made in Chapter 5 for harmonising the separate data breach notification scheme in the MHR Act with the later scheme in the *Privacy Act 1988* (Cth) and for addressing some gaps in the OAIC's privacy oversight powers.

3. Interaction of the HI Act and the MHR Act

Chapter 6 draws attention to the recommendations in an independent review in 2018 of the HI Act that align with recommendations in this report for ensuring that digital innovation initiatives have adequate legislative support. A recommendation is also made to review the exemptions that have been granted by the System Operator from the requirement to include an Individual Healthcare Provider Identifier in documents uploaded to the MHR system.

4. Healthcare recipient controls in MHR

Consumer control of individual records is a foundation principle of MHR and has not been doubted. Some questions have nevertheless been raised as to whether current requirements can be relaxed. These are examined in Chapter 7. Two that are discussed are the capacity of a healthcare recipient to hide a document in MHR so that it is unknown to a healthcare provider; and the obstacles that can be faced in an emergency hospital setting to identify and override a consumer access control.

5. Prohibition on using MHR-sourced information for insurance and employment purposes

New provisions were added to the MHR Act in 2018 making it an offence to use MHR patient information for the prohibited purpose of insurance and employment decision making. The provisions have been strongly criticised by the medical profession because of their reach, ambiguity, penalties, adverse impact on patient support and deterrent effect on MHR use. Chapter 8 supports the amendment of the MHR Act to allow a healthcare provider to prepare a report at the request of a patient when it would be in the best interests of the patient to act on that request.

6. Control of the MHR of minors

Changes to the MHR Act in 2018 introduced different rules for 3 age categories 0–13, 14–17, and 18 and over. There are gaps and anomalies in how MHR provisions now apply to those age categories. Recommendations are made in Chapter 9 for combining the 14–17 and 18 and over age categories; and resolving some gaps in the coverage of some of the System Operator's safety net powers.

7. Status of an MHR upon a person's death

The MHR Act has minimal rules relating to the MHR of a deceased person, as MHR is designed to support health care being provided to living people who can manage their own privacy settings. Chapter 10 discusses unanticipated complications to which the lack of guidance in the Act has given rise and makes recommendations for further consideration of legislative amendments to the MHR Act.

8. Facilitating use of MHR system data for public health research

It has long been anticipated that MHR system data would be used for public health research. Steps have been taken towards that objective, but they have not been fully implemented. Chapter 11 makes recommendations for taking the matter further – for example, through appointment of members to a Data Governance Board and the making of a Rule to provide a secure framework for supporting public health research.

9. Revising, updating and clarifying the MHR Act: explanation

Eight years of operation of the MHR Act have thrown up many gaps and anomalies in the MHR Act. Chapter 12 discusses these and makes recommendations for legislative change.

Acknowledgements

This review has benefited greatly from the input and assistance of many people.

Valuable informal interchange was held and thoughtful written commentary was received from a large number of people during the 2 consultation phases. Healthcare consumers, providers, regulators and policy planners willingly shared their knowledge, experience and suggestions.

Constructive support and assistance for the review was forthcoming at all levels in the Commonwealth Department of Health and the Agency.

Assistance to the review at key stages was ably provided by Tony Podpera, Kim Richter, Rachelle Stevens, Maddie Manning, Geoff Adams, Kirsten McNeill and Sam Peascod.

Special acknowledgement and thanks are owed to a small team within the Department of Health who worked closely with the review – Simon Cleverley, Amanda Kennedy and Tracy Cook. They provided excellent and able support at all stages and especially in coping with the added challenges for a review of this nature as Australia (and the department) responded to the COVID-19 pandemic. Simon, Amanda and Tracy's excellent rapport with people throughout Australia's health systems, and their own passionate commitment to e-health and digital innovation, added another dimension to the review.

Chapter 1. About this review

Why this review was conducted

The *My Health Records Act 2012* (Cth) (MHR Act) requires the Minister for Health to appoint an individual to review the operation of the Act and to report to the Minister within 3 years of a particular event.[1] The relevant event was the commencement on 2 December 2017 of a legislative rule[2] that made the opt-out model a feature of the My Health Record (MHR) system. In effect, this report is to be provided to the Minister by 1 December 2020. The Minister is then required to provide a copy of report to all Australian health ministers and table the report in both houses of the Australian Parliament within 15 sitting days of receiving it.[3]

The requirement to review the operation of the MHR Act has been a feature of the Act since it was enacted in 2012 to establish the Personally Controlled Electronic Health Records system (PCEHR). On 24 February 2020, The Hon Greg Hunt MP, Minister for Health, appointed Professor John McMillan AO to conduct an independent review of the operation of the Act. The review commenced in March 2020. Professor McMillan is an Emeritus Professor at the Australian National University and has relevant professional experience in administrative and constitutional law, as a legal practitioner and as a Commonwealth and state agency head. He has held appointments as Australian Information Commissioner, Commonwealth Ombudsman, NSW Ombudsman (Acting), Integrity Commissioner for the Australian Commission for Law Enforcement Integrity (Acting) and member of the Australian Copyright Tribunal.

The scope of this review

In establishing this review the Minister set out terms of reference that are at Appendix A to this report. The reviewer is to make recommendations for changes to the MHR Act and the rules and regulations.

A particular focus of the review, as outlined in the terms of reference, is whether the MHR legislation is adequately supporting 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 health care.

The review is to consider whether revision of the MHR legislation could improve:

- how healthcare recipients use the MHR system
- how healthcare providers and healthcare recipients interact with the MHR system and each other
- the use of MHR data for research and public health purposes, consistently with safeguarding privacy and security
- public trust and confidence in the MHR system, with an eye in particular to some of the balances that are struck in the MHR system design.

Other specific issues listed in the terms of reference relating to the MHR legislation and its operation are:

- compliance and enforcement activities
- complaint handling

---

[1] *My Health Records Act 2012* (Cth) (MHR Act) s 108.
[2] *My Health Records (National Application) Rules 2017* (Cth).
[3] MHR Act s 108(3).

- interaction of the legislation with the *Privacy Act 1988* (Cth)
- the role of the Office of the Australian Information Commissioner (OAIC) in overseeing privacy and data handling
- the rules regarding minors' information and how these interact with other Commonwealth, state and territory laws
- the interaction of the *Healthcare Identifiers Act 2010* (Cth) and the Healthcare Identifiers Service with the MHR system
- restrictions imposed by the MHR Act on eligibility to prepare a shared health summary that is uploaded to the MHR system and on being a nominated healthcare provider
- the authorisations of the System Operator for the MHR system
- the oversight role of the Australian health ministers.

Although the focus of the review is the MHR legislation, the reviewer could draw attention to legislative changes or operational improvements that could support the MHR legislation in achieving its objectives. The reviewer was not confined to drawing attention to improvements that are a matter for Commonwealth action only.

How this review was conducted

Consultation, both publicly and with key stakeholders, was a key activity in this review. Consultations were planned to commence in April 2020 but were deferred as a result of the COVID-19 pandemic. This was necessary as many key stakeholders had frontline responsibility for Australia's health response to the pandemic, and face-to-face meetings and public seminars around Australia were not possible. Two phases of consultation were subsequently undertaken. These included:

- ***Phase 1 (May–August 2020):*** Targeted bilateral meetings were held with nearly 50 individuals from consumer and professional organisations, state and territory government agencies, researchers, and 4 Commonwealth agencies with direct responsibilities in the MHR system (the Department of Health, the Australian Digital Health Agency, OAIC and Services Australia). This phase of the consultation process informed the development of a public consultation paper that was published in September 2020.
- ***Phase 2 (25 September – 21 October 2020):*** Publication of a consultation paper for the review opened a public consultation process in which members of the public, healthcare professionals and government and non-government bodies were invited to submit written submissions. A total of 41 submissions were received from consumers, practitioners, professional organisations and government agencies. Parties could request non-publication of either their submission or their identity. The public website established for the review publishes 37 submissions (12 anonymously) and lists 4 other parties that made submissions anonymously but did not want their submission published. Submissions principally came from interested healthcare recipients, healthcare provider organisations participating in the MHR system, and peak professional organisations or with government, public health, public policy or regulatory interests.

Other consultation activities conducted during the review included meetings with:

- the Interim National Data Commissioner and the Office of the National Data Commissioner to discuss the exposure draft of the Data Availability and Transparency Bill
- the Attorney-General's Department to discuss the review of the *Privacy Act 1988*.

The consultation in Phase 1 of the review identified 6 key themes that were a prominent feature of the consultation paper that commenced the Phase 2 round of public consultations. Those key themes and the submissions that were made in response are discussed in Chapter 3.

Chapter 2. Australia's My Health Record system

Scope and evolution of MHR

The MHR system is a secure national system for facilitating consumer-controlled access to key health information about individuals for healthcare purposes. The MHR system uses a federated model that draws health information from repositories that are independently managed, rather than storing all information in a central database.

MHR began in 2012 as an opt-in system, titled the Personally Controlled Electronic Health Records system (PCEHR). It transitioned to an opt-out participation model in July 2018 and was renamed 'My Health Record'. The system remains voluntary (opt-in) for healthcare providers and organisations.

The objects of the MHR system, which have remained unchanged, are stated in the MHR Act s 3:

> *The object of this Act is to enable the establishment and operation of a voluntary national public system for the provision of access to health information relating to recipients of healthcare, to:*
>
> *(a) help overcome the fragmentation of health information; and*
> *(b) improve the availability and quality of health information; and*
> *(c) reduce the occurrence of adverse medical events and the duplication of treatment; and*
> *(d) improve the coordination and quality of healthcare provided to healthcare recipients by different healthcare providers.*

MHR has evolved over more than a decade as a unique national digital health records scheme. As of October 2020:

- A total of 22.85 million eligible Australians had an individual MHR. Of those, over 19.9 million had health data entered in the record.
- A large majority of healthcare providers were registered in the system – 94% of general practitioners, 99% of pharmacies and 96% of public hospitals.
- Over 2.38 billion documents had been uploaded to MHR, including 2.1 billion Medicare documents, 175 million medicine documents uploaded by healthcare providers and 335,000 documents uploaded by healthcare recipients.
- MHR included nearly 68 million pathology reports, nearly 10 million diagnostic imaging reports and over 8 million discharge summaries.

MHR system features

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 any person who wishes to have one and who has also been assigned an Individual Healthcare Identifier (IHI) – a unique 16-digit number that identifies a healthcare recipient. An IHI is assigned by the Healthcare Identifiers 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 from a consumer's Medicare number and the IHI does not store health information.

An individual 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 healthcare recipient'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).

An 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 an Individual Healthcare Provider Identifier (HPI-I) or a Healthcare Provider Organisation Identifier (HPI-O).

The healthcare identifier enables the provider or organisation both to upload health information to a consumer's MHR and to access health information in the MHR. The default setting is that a participating healthcare provider or organisation can upload or access a healthcare recipient's personal health information for the purpose of providing health care to them.

The healthcare recipient can override those default settings and set advanced access controls that prevent a provider organisation from viewing or having access to their health information, either generally or subject to limitations the individual has specified. Another option is that the consumer can remove a document that has been uploaded to their MHR. A healthcare recipient may also advise a provider or organisation that a specified document is not to be uploaded. As at October 2020, almost 40,000 Australians have placed advanced access controls on their records.

Other specific features of the MHR system include special rules regarding the MHR of a minor, the appointment of a representative who may act on behalf of an MHR record holder, prohibitions on the use of MHR personal health information for insurance or employment purposes, and the proposed use of MHR information for research and public health purposes.

The MHR Act requires the Office of the Australian Information Commissioner (OAIC) to oversee and report annually 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.

The MHR system legislative framework

The MHR legislative framework consists of the MHR Act and supporting rules and regulations. These govern the implementation and operation of the MHR system.

The MHR Act establishes the role and functions of the System Operator and provides a registration framework for healthcare recipients and healthcare provider organisations to participate in the MHR system. It governs which entities can collect, use and disclose certain information in the system (such as health information contained in a healthcare recipient's MHR); and the penalties that can be imposed on improper collection, use and disclosure of this information.

The rules and regulations (subordinate legislation) made under the MHR Act are:

- My Health Records Regulation 2012
- *My Health Records Rule 2016* (MHR Rule 2016), which specifies operating requirements to be met by registered entities in the MHR system, including the foundation rules for consumer access controls
- *My Health Records (Assisted Registration) Rule 2015*, which specifies requirements for registered healthcare providers that assist individuals to register (through 'assisted registration')
- *My Health Records (National Application) Rules 2017*, which provide for the national implementation of the MHR system opt-out model under Schedule 1 of the MHR Act
- *My Health Records (Opt-Out Trials) Rule 2016*, which supported an early regional trial of the opt-out model

- *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*, which are made by the Australian Information Commissioner and set out the commissioner's general approach to exercising its privacy oversight enforcement and investigative powers under the MHR system.

Other important items of legislation that are part of the MHR framework are:

- *Healthcare Identifiers Act 2010* (Cth) (HI Act), which establishes the HI Service. The HI Service uniquely identifies individuals, healthcare provider organisations and individual healthcare providers
- Healthcare Identifiers Regulations 2020, which contain supplementary provisions regarding the operation of the HI Service
- *Privacy Act 1988* (Cth), which contains the Australian Privacy Principles (APPs) that regulate the collection, storage, use and disclosure of personal information, including health information; and confers regulatory compliance and enforcement powers on the Australian Information Commissioner
- *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016*, made by the Minister for Finance under the *Public Governance, Performance and Accountability Act 2013* (Cth) to establish the Agency.

Review of the MHR system

There have been a number of key reports that have informed the development of the MHR system, including independent reviews of key features of the PCEHR and MHR schemes. Major reports include the following:

- National E-Health and Information Principal Committee, *National E-Health Strategy* (Deloitte, 2008): This report was commissioned by the Australian Government and proposed a National E-Health Strategy, to include a framework for capturing, managing, sharing and protecting health information.
- Final Report of the National Health and Hospitals Reform Commission, *A healthier future for all Australians* (2009): This report proposed that a person-controlled electronic health record for each Australian should be part of a transformative e-health agenda for 'the smart use of data, information and communication'.
- Council of Australian Governments (COAG), 'National Partnership Agreement on E-Health' (2009): This COAG agreement included governance arrangements for a national healthcare identifier service to facilitate effective sharing of health information as part of a nationally consistent electronic health system.
- Department of Health, *Review of the Personally Controlled Electronic Health Record* (2014): This review by a 3-member panel made a large number of recommendations to change the PCEHR system, including a name change to MHR, a move to opt-out, new governance arrangements, improved system usability and expanded record content protocols.
- National E-Health Transition Authority, *Evolution of eHealth in Australia: achievements, lessons, and opportunities* (2016): The National E-Health Transition Authority – a collaborative enterprise of Australian governments – made this report on the foundations for e-health in Australia. The authority was abolished and replaced by the Agency in 2016.
- *A My Health Record for every Australian* (2017): This was a 2017–18 Budget announcement by the Australian Government, announcing an opt-out MHR scheme.
- COAG, 'Intergovernmental Agreement on National Digital Health' (January 2018).
- Australian Digital Health Agency, *Safe, seamless and secure: Australia's National Digital Health Strategy* (2018): The strategy outlines an agreed vision for digital health based on 7 pillars that include the MHR system.
- J Kelly, *Healthcare Identifiers Act and Service Review: final report* (Department of Health, November 2018): This was an independent review of the HI Act and HI Service, as required by the HI Act.

- Senate Community Affairs References Committee, *My Health Record system* (October 2018): The committee undertook a public review of the MHR system as part of the transition to an opt-out scheme. It received 118 public submissions.
- Department of Health, *Australia's Long Term National Health Plan* (August 2019): This report is a comprehensive outline of the Australian Government's plans for a better health system.
- Australian National Audit Office, *Implementation of the My Health Record system* (Report No 13, 2019–20): This performance audit looked at privacy and security safeguards in the MHR system opt-out model.

Chapter 3. Perspectives on the operation of My Health Record

This chapter summarises the main themes that arose in the 2 consultation phases of this review.

The themes are presented in 3 parts in this chapter. The first part lists 6 perspectives on the MHR system that were expressed during the first consultation phase. These perspectives formed the basis for the consultation paper that was published in September.

The perspectives were largely reinforced during the second consultation phase, which drew submissions from individual consumers, practitioners, professional organisations, academics and government agencies. The 6 perspectives are repeated in similar terms in this chapter, partly revised and updated in light of the written submissions that were received.

Many submissions also responded directly to a few broad questions about the MHR system that were asked in the consultation paper. Is it providing practical healthcare benefits to consumers and providers? Is MHR understood by consumers? Are there obstacles or disincentives to greater use of MHR? Is the future direction of MHR clear?

The second part of this chapter distils the responses to those questions in the submissions. The analysis of the responses leads into 4 recommendations that conclude the chapter. The recommendations mostly propose activities or topics for future public engagement in MHR review and planning. Many participants in the consultation phases of this review emphasised the importance of a broadly based and ongoing public dialogue about the benefits, challenges and future directions of the MHR system.

The third part of this chapter summarises some points made in the Australian Digital Health Agency (the Agency) submission to this review about its work program and future planning. That valuable work can be too easily overlooked in other spirited discussions about the operation of the MHR system.

Another introductory point to make is that the following summary of views expressed during the consultation phases does not evaluate or endorse those views. Later chapters of this report contain findings and discuss recommendations.

With a couple of exceptions, the individual submissions are not identified or referenced in this chapter. Rather, the aim is to synthesise a range of diverse views. Submissions are referenced in later chapters, and most are published on the website for this review.

Finally, the consultation commentary was wide-ranging and often extended beyond the terms of reference for this inquiry, which are focused on the provisions of the MHR Act. The operation of the MHR system is a far larger public policy topic. However, the commentary provides an important perspective when examining the MHR Act and can help to shape future lines of inquiry on the Act and its operation.

Six perspectives on MHR

1. Strong cross-sectional report for MHR

There is widespread support for MHR and a belief that, intrinsically, a national electronic health records system is essential. There is broad agreement that digital innovation improves health outcomes.

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

MHR can provide numerous benefits for healthcare recipients – knowing where their health information is stored and can be retrieved; being able to access their health information to manage complex health conditions and consult new health providers; avoiding duplicate testing; and becoming more health literate and engaged. Choice and mobility in health care have also become more important to healthcare recipients.

Several submissions from healthcare providers gave examples of practical benefits that MHR had provided: being able to access reliable and current health information about new patients, dealing with unexpected or emergency visits, and validating the occurrence of tests and prescriptions.

The submission from the Society of Hospital Pharmacists of Australia[4] conveyed the results of a survey of MHR use by its members. It was rated at 7.2 out of 10 as a tool to improve the safety and quality of health care. MHR is used by the majority (65.7%) of hospital pharmacists, with 75.1% of those who use it reporting that they use it multiple times in a day.

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
- an infrastructure that is aligned to developments in Australia's digital health program.

Many professional associations have published a statement in support of MHR on their websites.

2. MHR as a supplementary health record

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

MHR operates alongside and does not replace other health records 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 records system. For example, for a patient who regularly visits the same practitioner, there may be little need to access MHR for healthcare purposes or for the provider to do so. MHR will necessarily have greater utility in some situations than in 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.

An awareness of this context is integral to understanding the purpose of MHR and limitations on the currency and reliability of MHR content.

3. Mixed assessment of MHR performance

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

Two criticisms stand out. The first is that there is limited or uneven content in many MHR records. The 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 health care to them. These weaknesses can shake public and practitioner confidence in the utility of MHR and in that way be self-perpetuating.

---

[4] Submission No 26 (SHPA).

There are related criticisms of the content, use and presentation of health information within MHR. There is uneven MHR use across the health profession. Public hospitals, for example, have increased their upload and use of MHR health information when compared with areas of underuse such as 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.

Another doubt raised is that many consumers appear disinclined to access MHR. Contributing factors may be the need to link and access MHR through a myGov account, a lack of knowledge about the purpose and content of MHR, or awareness that the content 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/opt-out privacy debate cast a long shadow, but that may be clearing gradually over time. Recent events such as the COVID-19 pandemic have, anecdotally, 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 database in a federal system comprising 7 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
- the health profession's preference for using alternative record databases that may be simpler to access, particularly those operated by state and territory public health systems and by private diagnostic services.

4. Linking MHR to other digital health initiatives

MHR is one of 7 digital health priorities set down in *Australia's National Digital Health Strategy,* published by the Agency in July 2018 and endorsed by all Australian health ministers. Other strategic priorities include:

- secure digital channels for communication between healthcare providers and with patients
- standards to ensure interoperability between public and private healthcare services
- medicines safety, including e-prescribing
- 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 is said to have been 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 dropbox. In short, the creation of the record should not be seen as the end in itself. Although 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 health care. This can be fully met only 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 or for data uploaded to MHR to be coded. The benefit of so doing is that static MHR content could be curated or atomised and be presented and used differently and accessed more easily.

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 coordinate healthcare treatments for individuals.

Another inescapable digital question is whether, as an individual consumer choice, MHR should be electronically linked to other personal health information through mobile and wearable devices.

5. Laying out an MHR roadmap

Submissions to this review strongly endorsed the proposal for the Agency to prepare 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 3 strategic objectives – 'increase consumer participation', 'increase core clinical content' and 'achieve extensive adoption by healthcare providers'.[5] 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 records 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 records 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.

A roadmap – or series of specific-issue strategic planning options papers – would also better enable stakeholders to engage directly with the Agency and other interested parties and contribute to the development and evolution of MHR.

An analogous recommendation for development of a futures roadmap was made in the 2018 *Healthcare Identifiers Act and Service Review: final report* (discussed in Chapter 6). The report recommended that the Agency develop a strategy and roadmap for the Healthcare Identifiers (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.

6. Ensuring the MHR Act supports digital health innovation

There is a keen awareness that the MHR system is anchored in the MHR Act, which is highly prescriptive of the structure and operation of the MHR system. Any proposed change to the MHR system may run up against the rigidity and complexity of the Act.

---

[5] Australian Digital Health Agency, *Safe seamless and secure: evolving health and care to meet the needs of modern Australia. Australia's National Digital Health Strategy* (2018) p 23.

The Agency submission[6] points to features of the MHR Act that may run counter to digital innovation. One is that the Act lists the organisations that are authorised by the Act to have access to MHR information. This does not include software vendors or entities such as primary health networks that facilitate but do not provide health care. Their ability to participate in the MHR system is therefore limited.

The Agency submission notes that principles-based authorisations to collect, use and disclose information would align better with digital health innovation initiatives. The Australian Privacy Principles in the *Privacy Act 1988* (Cth) provide a model for principles-based regulation of information access, use, management and disclosure.

There has also been criticism of the MHR legislative design from the perspective of healthcare providers. It is said 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 patient health information.

An added disincentive for health providers is that the MHR Act imposes criminal and civil penalties for the unauthorised collection, use and disclosure of MHR patient 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 perceived as antagonistic to a patient's health interests.

On the other hand, several submissions emphasised the importance of maintaining an appropriate balance in the MHR Act between clinical utility and privacy and security. Striking that balance may be critical to ensuring public trust in the MHR system and realising the public benefits that it offers.

Drawing the themes together

A number of common themes ran through much of the commentary in the submissions and the consultations:

- There is strong interest across stakeholder groups in exploring options for strengthening and evolving the MHR system. There would be broad agreement with the 3 strategic objectives stated in the National Digital Health Strategy – 'increased consumer participation', 'increased core clinical content', and 'extensive adoption by healthcare providers'.
- There is equally strong recognition that practical incentives of varying kinds may be required for each of those objectives. This is taken up in Recommendations 2 and 3, proposing that the Department of Health review the allocation of incentives under the Practice Incentives Program eHealth Incentive (ePIP) and that government initiate a broader review of practical incentives to encourage participation in MHR. The submissions were equally open-minded about the range of financial and non-financial incentives that should be considered, including the option of tying eligibility criteria for specific government health benefit payments to those strategic objectives.
- While participants in this review support the broad and community-wide aims of the MHR system, their practical interest is often more confined to how the system could better assist particular groups or particular areas of health practice. The primary stakeholder interest is to participate in strategic planning conversations that focus on how MHR could be calibrated to provide specific or topical benefits. Similarly, sound business planning would take stock of groups or activities that gain special benefit from MHR and to reinforce that localised MHR dimension. A successful initiative could then be applied or tested in other areas where MHR has been less dynamic.

[6] Submission No 28 (Agency).

In a sense, stakeholders would like greater focus – publicly at least – on 'the value proposition' for MHR. This is taken up in Recommendation 4, proposing that the Agency publish a series of 'roadmap' or strategic planning documents as the basis for consultation with specific stakeholder groups.

- Healthcare provider groups repeatedly drew attention in consultations to workflow impediments in using and accessing MHR. Three words/concepts were commonly used:
  - ***'Integration':*** Healthcare providers access multiple health information sources (often concurrently) and can draw more value from MHR if there is workflow integration between those sources. While there is strong recognition of the legal and privacy constraints surrounding MHR, the ideal situation (particularly in a hospital setting) is that MHR information is displayed alongside other health information.
  - ***'Seamless':*** Workflow impediments that are frequently mentioned are the lack of software interoperability and clunky logon requirements (including for support staff); and that key and recent clinical information is not highlighted in MHR or presented in a consistent way.
  - ***'Perceptions':*** The benefits of MHR are not well understood by healthcare providers and consumers. The benefits are overshadowed by a prevailing feeling that MHR has been disappointing. There is a risk of this attitude becoming embedded.
- It was equally seen as important to repair or reform some features of the MHR Act that are viewed by practitioners as obstacles that impede stronger professional support for MHR. Some of these obstacles stem from the complex and rigid nature of the MHR Act framework. Some others stem from legislative changes in 2018 that have had unintended consequences. These issues are all taken up in subsequent chapters of this report.
- It is important to add that it would be self-defeating for government to regard these complaints as routine irritations with legislative requirements and to give them a lower priority. Failure to address them in a timely way will be perceived negatively and, conversely, a preparedness to address them promptly may be viewed as an encouraging government commitment to supporting and improving the MHR system.
- A related point is that there is earnest stakeholder interest in an avowed government commitment to improving the MHR system and developing it as part of a broader program of digital health innovation. Practical government support would be welcomed. This could come in the form of, for example, government sponsorship of legislative reform of the MHR Act, as well as government adoption of a longer term funding model for the MHR system – a matter taken up in Recommendation 1.

The Australian Digital Health Agency's digital health program

The Agency submission drew attention to a range of programs that are underway that are already dealing with many of the suggestions made in the submissions to this review:

- A refresh of the National Digital Health Strategy has been commenced. The strategy could embrace the connection to the MHR system of emerging digital technologies such as wearable devices, virtual care and genomics.
- A program is underway to modernise the national digital health infrastructure. This is occurring in consultation with stakeholders. The modernisation will explore the further use of external repositories and the use of atomic and more structured data.
- A 3-year program is underway to improve specialist adoption and use of the MHR system. This involves software design, educational packages and liaison with professional groups and colleges.
- A 2-year program is underway to increase aged care connection to the MHR system, involving software design, educational packages and registration drives.
- Liaison is occurring with private pathology and diagnostic imaging sectors to increase MHR uploads.

- A joint project is being conducted with the Australian Commission on Safety and Quality in Health Care to establish regular use of MHR by clinicians in hospital emergency departments.
- Processes are being refined for clinical software vendors to connect to the MHR system.
- A National Digital Health Workforce and Education Roadmap has recently been published.
- A National Nursing and Midwifery Digital Health Capability Framework has recently been published.
- A Digital Health Capabilities Framework for Medicine is being developed.
- User testing and research is being undertaken to improve consumer use of MHR, including the development of mobile solutions for safe and secure access to MHR.

Recommendations

Recommendation 1

The Australian Government review the current Budget funding arrangements for My Health Record (MHR) system activity and, in particular, review the desirability of:

- moving the current annual budgetary funding arrangement for the role of the Australian Digital Health Agency, as the System Operator for MHR, to a new arrangement of an annual appropriation tied to a forward estimate
- direct appropriation to the Office of the Australian Information Commissioner for its privacy oversight work in relation to MHR, to replace the current arrangement of an appropriation to the Australian Digital Health Agency that is transmitted to the Office of the Australian Information Commissioner under a memorandum of understanding between both agencies.

Recommendation 2

The Department of Health review the principles for incentive payments being made under the Practice Incentives Program eHealth Incentive (ePIP) to general practices that participate in My Health Record. The review should examine whether:

- the current practice of tying incentive payments to the upload of shared health summaries to My Health Record is achieving the objectives of MHR
- incentive payments should instead be made for other general practice activities that can support the security, integrity or effectiveness of MHR.

Recommendation 3

The Australian Government initiate a review of practical incentives that could be adopted to support 3 strategic objectives for MHR stated in the National Digital Health Strategy – 'increased consumer participation', 'increased core clinical content', and 'extensive adoption by healthcare providers'. The review should examine options for tying eligibility criteria for specific government health benefit payments to those strategic objectives.

Recommendation 4

The Australian Digital Health Agency develop and publish a series of 'roadmap' or strategic planning documents as the basis for consultation with stakeholders on the future planning directions for MHR. The roadmap documents should deal as specifically and discretely as possible with special interest topics raised by stakeholders, including as part of this review. Examples include:

- education programs that illustrate the benefits of MHR for consumers and that could stimulate active participation by consumers
- strategies for encouraging participation in MHR by groups or cohorts that are presently under-represented, such as specialists, allied and community health, and aged care

- consumer options for accessing MHR through platforms other than myGov, including through mobile devices
- adjustments that could be made to MHR operating principles in response to distinctive issues in areas such as mental health or hospital emergency clinics
- strategies for facilitating participation in MHR by large employers such as the Australian Defence Force.

Chapter 4. The System Operator's functions, powers and responsibilities

The nature and scope of the System Operator's role

The MHR system is operated by the System Operator. Since 1 July 2016, the System Operator has been the Australian Digital Health Agency (the Agency).[7] It was established the same year as a statutory agency by the *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016* (Cth) (Agency Rule).

The Agency's functions are set out separately in the Agency Rule[8] and include functions conferred on the Agency by other laws, such as the MHR Act.

The System Operator functions are set out in the MHR Act.[9] They include:

- establishing an index service for connecting different repositories of personal health information that can be accessed through the MHR system by registered healthcare recipients and participants
- operating a National Repositories Service for storing key health information records about registered healthcare recipients
- establishing access control mechanisms that enable registered healthcare recipients to control access to their MHR
- registering healthcare recipients and entities (such as healthcare provider organisations, repository operators and portal operators) in the MHR system
- establishing mechanisms for recording activity within the MHR system
- monitoring the operation of the MHR system through a reporting service, audit service, test environments and complaints handling
- ensuring the MHR system is administered so that problems relating to the administration of the system can be resolved
- advising the Minister in relation to the MHR system
- conducting public education about the MHR system
- for the purposes of public health research, preparing de-identified data and health information (with the consent of healthcare recipients)
- any other functions conferred by law on the System Operator
- doing anything incidental to or conducive to the performance of the above functions.

The Agency submission to this inquiry commented that the System Operator functions listed in the MHR Act 'lack a degree of clarity needed to provide confidence in the System Operator undertaking activities that improve and ensure the quality and effectiveness of the system'.[10] Examples were given of functions that are lacking or currently undertaken on a scaled-down basis to fit within the authorised powers. The Agency's experience is that it can be administratively complex and time-consuming to resolve questions about the scope of its System Operator functions.

---

[7] The Agency is prescribed as the System Operator by the My Health Records Regulation 2012 (Cth) reg 2.1.1.
[8] *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016* (Cth) (Agency Rule) r 9.
[9] MHR Act s 15.
[10] Submission No 28 (Agency) p 5.

Other submissions to this inquiry had little to say about the System Operator functions – and, importantly, none proposed that the functions be narrowed in any way. The Office of the Australian Information Commissioner (OAIC) recommended that the System Operator's function of registering healthcare provider organisations be strengthened.

The following discussion broadly endorses the principle that the functions of the System Operator should be clearly expressed in the authorising legislation. This is particularly important in light of the System Operator's substantial responsibility to control the collection, use and disclosure of sensitive personal health information of a high proportion of the Australian community.

A matter not fully explored in this inquiry is whether some functions that are not expressly anchored in the MHR Act could in fact be undertaken under the System Operator function to do anything 'incidental or conducive' to its enumerated functions. Incidental functions of that kind are customarily construed broadly to the extent that they authorise operational activities that do not transgress fundamental freedoms or principles.[11]

Similarly, the activities the Agency can undertake as System Operator can draw support from the list of Agency functions in the Agency Rule (subject to any contrary intention in the MHR Act). Those functions are set out in r 9 of the Agency Rule and include:

> *(c) to develop, implement, manage, operate and continuously innovate and improve specifications, standards, systems and services in relation to digital health, consistently with the national digital health work program;*
> *(d) to develop, implement and operate comprehensive and effective clinical governance, using a whole of system approach, to ensure clinical safety in the delivery of the national digital health work program; …*
> *(f) to develop and implement compliance approaches in relation to the adoption of agreed specifications and standards relating to digital health; …*
> *(i) to do anything incidental to or conducive to the performance of any of the above functions.*

The national digital health work program referred to in paras (c) and (d) in that list is prepared by the Board of the Agency[12] and includes responsibility for the MHR system.

Maintaining a reporting service to assess MHR system performance

Section 15(d) of the MHR Act confers the following function on the System Operator:

> *(d) to establish and maintain a reporting service that allows assessment of the performance of the system against performance indicators …*

The Agency explained in its submission that a method adopted to discharge that function is to create a de-identified or administrative dataset that can be provided to a primary health network or state health department and then used to assess the impact of the MHR system on healthcare delivery and to identify opportunities for improvement. For example, the dataset can be used to ascertain how effectively the MHR system supports COVID-19 related health care.

Creation of the de-identified dataset may nevertheless require the use of health information. To do that, the Agency relies on s 63(a) of the MHR Act, which authorises the System Operator to use health information from a recipient's MHR if the recipient 'would reasonably expect' their health information to be used for that purpose. That may involve conjecture about consumer expectations on each occasion that health information is used to create a dataset.

---

[11] Eg *Attorney-General v Great Eastern Railway Co* [1880] 5 App Cas 473, 478, 481; *Northern Land Council v Quall* [2020] HCA 33 [64]–[68].
[12] Agency Rule r 70.

At a legislative level, the issue the Agency has raised could be resolved by amending the MHR Act to give the System Operator a more generally expressed power to use health information from the MHR system for the purpose of performing a function or exercising a power under the Act.[13] It is recommended below that this option be given further consideration.

An alternative approach, at an administrative level, would be more strengthened reliance on the existing power in s 63(a) to use patient health information in a way that a person would 'reasonably expect' to occur. It is possible that this could be done at present by explaining directly in the System Operator Privacy Policy that health information may be used *in a de-identified form* for management or operational purposes. Currently, the System Operator Privacy Policy is expressed more narrowly:

> ***Collection, use and disclosures that are authorised under the My Health Record Act***
> *… The limited circumstances where your personal information is authorised to be disclosed include when it is … for the management or operation of the MHR system – if you would reasonably expect this to occur. For example, it may be to resolve any technical or other issues that may have an impact upon the accuracy, security or privacy of information in your MHR.*[14]

Whether the clarification of the System Operator's function is addressed at a legislative or an administrative level, the Agency's submission correctly notes that creation of a de-identified dataset is consistent with the OAIC's general privacy guidance. The OAIC guideline on de-identification advises that personal information that has been de-identified no longer falls within the definition of 'personal information' in s 6 of the *Privacy Act 1988* (Cth), which refers to information 'about an … individual who is reasonably identifiable'. Consequently, the OAIC observes, 'de-identification can generally be considered incidental to the primary purpose of collection'.[15]

Operating a test environment for the MHR system

Section 15(ia) of the MHR Act confers the following function on the System Operator:

> *(ia) to establish and operate a test environment for the My Health Record system, and other electronic systems that interact directly with the My Health Record system, in accordance with the requirements (if any) in the My Health Records Rules …*[16]

This function does not extend to using the live MHR environment for testing purposes.

The Agency explained in its submission that it would be valuable to have the authority to do testing in the live environment, as issues arise that do not occur or cannot be replicated in the test environment. Examples include using a test patient or test Individual Healthcare Identifier (IHI) or testing records to assess if they conform to technical specifications and data quality requirements. The Agency advises that this testing could be undertaken using only test data and not personal or health information.

The Agency's proposal could be implemented by extending the scope of s 15(ia) or by conferring a separate explicit function of conducting testing in the MHR system. It is recommended below that this option be given further consideration.

---

[13] This proposal is adapted from s 63(b) of the MHR Act, which provides in similar terms that a participant in the MHR system may use health information 'in response to a request by the System Operator for the purpose of performing a function or exercising a power of the System Operator'.
[14] Australian Digital Health Agency, My Health Record, 'Privacy Policy' https://www.myhealthrecord.gov.au/about/privacy-policy.
[15] Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (March 2018) p 8.
[16] There is no relevant requirement in the *My Health Records Rule 2016* (MHR Rule 2016).

Other testing and clinical safety analysis

The Agency submission described 2 other testing and analytical functions that are not directly described in s 15 of the MHR Act:

- testing of MHR data to assess if it conforms to technical specifications and data quality requirements. Testing of this kind is regarded as important to the clinical safety of the MHR system, the value of the system to healthcare recipients and providers, and the value of MHR data for research and public health purposes. Currently, this testing is undertaken only on a case-by-case basis when the legal authority is clear.
- clinical safety analysis of MHR data and also of the MHR system. At present the Agency relies on other functions to ensure clinical safety in the MHR system. The other functions are the System Operator's implicit responsibility under the MHR Act to ensure that the MHR system is operating in a clinically safe manner; and the Agency's function under r 9(d) of the Agency Rule to ensure, through effective clinical governance, clinical safety in the national digital health work program.

It is important that the System Operator has authority to maintain the integrity of the MHR system by checking technical specifications and data quality and undertaking clinical safety analysis. The only issue is whether an explicit or direct function is needed.

An alternative view is that those activities are already authorised – for example, by s 15(a) (supported by the incidental power in s 15(o)), which confers authority to establish a system that links health information in different repositories so that it can be accessed by registered healthcare recipients and MHR system participants.

It is nevertheless recommended below that the option of legislative amendment be given further consideration.

Notifying events to healthcare recipients and providers

The System Operator plays a limited role in notifying events to healthcare recipients – for example, sending an email or SMS notification that a healthcare provider organisation has uploaded a new shared health summary to the person's MHR.

There is support (within both the Agency and the healthcare community) for the System Operator to play a more active notification role. For example, based on the information within a person's MHR, the System Operator could send a routine health check or follow-up reminder to a healthcare recipient or a notice alerting a healthcare provider to an event affecting a patient.

Active notifications of that kind could extend the practical benefit of the MHR system for healthcare recipients and providers. Conferring such a function expressly on the System Operator would provide a firmer basis for developing such a role. A recommendation to that effect is made below.

Imposing registration or other charges

The Agency submission proposes that consideration be given to authorising the System Operator to impose a charge for specified activities such as deciding an application by a portal or repository operator to be registered.[17] The Agency comments that cost recovery could be appropriate, as the assessment process can be resource intensive.

[17] MHR Act Pt 3 Div 3.

The Australian Government policy is that a charge can be imposed where government provides a service or regulation.[18] However, clear statutory authority is required to levy money.[19] Presently, the MHR Act authorises neither the imposition of a charge nor the making of a regulation to impose a charge.

It is recommended below that consideration be given to conferring this charging power on the System Operator.

Authorised and nominated representatives

The MHR Act provides for the appointment of authorised and nominated representatives to control or assist in managing a person's MHR.

Several issues concerning the adequacy of the MHR Act provisions relating to representatives as discussed below in Chapter 9 in relation to managing the MHR of a minor. Three recommendations are made in that chapter:

- ***Recommendation 20:*** The default setting in the MHR Act is that the MHR of a child aged 13 or younger is controlled by their authorised representative – namely, a person who satisfies the System Operator that they have parental responsibility for the child.[20] This recommendation would modify that default setting by enabling a child aged 13 or younger to apply to the System Operator to take control of their own MHR.
- ***Recommendation 22:*** This recommendation would remove the separate age category 14–17 and apply to a person of that age the MHR Act provisions that presently apply to a person aged 18 or above. Consequently, a person aged 14 or over could agree to a nominated representative; and the System Operator could approve an appropriate person to be an authorised representative for a record holder who lacked the capacity to make decisions on their own behalf.[21]

  As explained in Chapter 9, an authorised representative substitutes for the record holder, who no longer has access to or control of their record; whereas a nominated representative exercises power concurrently with the record holder but subject to any restrictions the record holder has imposed.
- ***Recommendation 23:*** This recommendation would require the System Operator's approval for the appointment of a minor as the authorised or nominated representative of another person.

Several other issues relating to the role of representatives and the powers of the System Operator to protect a healthcare recipient against harm should also be addressed.

Persons who are unsuited to be representatives

The MHR Act does not currently contain a comprehensive and coherent framework to prevent the recognition of an unsuitable representative. A few provisions partially achieve that objective and could be extended or supplemented.

The System Operator can decline to recognise a person as an authorised representative of a child aged 13 or younger if satisfied that the life, health or safety of the child or any other person 'would be put at risk' by the representative.[22] Two aspects of that power require comment.

---

[18] Department of Finance, *Australian Government cost recovery guidelines* (RMG 304, 3rd ed, 2014).
[19] Ibid; and *Attorney-General v Wilts United Dairies Ltd* (1921) 37 TLR 884.
[20] MHR Act s 6(1).
[21] MHR Act s 6(4).
[22] MHR Act s 6(1A)(b).

The first aspect is that the System Operator would require a strong evidentiary basis to be affirmatively satisfied that a child or other person's safety 'would' be at risk. By contrast, the MHR Rule 2016 r 15 imposes a similar but lesser test for suspension of an authorised representative's access to a healthcare recipient's MHR: the System Operator can suspend access if satisfied that suspension 'is *likely* to [reduce] a serious risk to an individual's life, health or safety'.

The second aspect (discussed in Chapter 9) is that it is unclear if this power also applies to children aged 14–17 or only to children aged 0–13. There is no similar power in the MHR Act applying to a representative for an adult.

An appropriate option would be to extend this safety net power to apply in respect of all record holders. That is, the System Operator could decline to recognise an authorised or nominated representative for a person of any age if doing so is likely to pose a risk to the life, health or safety of a person. Recommendation 6 below is to that effect.

Another relevant provision in the MHR Act states that the duty of a representative is to give effect to a healthcare recipient's will and preferences or otherwise to act in their best interests.[23] There is no direct mechanism in the MHR Act to respond to a breach of that obligation. In particular, the System Operator lacks any general power to initiate action to remove access by a representative to a person's MHR if there is reason to believe that the representative is unable or unwilling to act in a way that promotes the personal and social wellbeing of the healthcare recipient.

This issue could be addressed in either of 2 ways. The first option would be to confer a general removal power of the kind just noted. This direct option may overcome the current complexity in the MHR Act and MHR Rule 2016 as to the System Operator's powers in respect of representatives.

The second option would be to make a representative's obligation to act in accordance with a healthcare recipient's will and preferences an element of that eligibility framework to be a representative. This would tie in to existing power conferred on the System Operator to cancel a representative's access to a healthcare recipient's MHR if no longer satisfied that the person is eligible to be a representative.[24] (An example of where that power is currently used is where a healthcare recipient has rescinded the agreement under which the person was a representative.)

Recommendation 6 below is that the Department of Health further consider those 2 options.

The Agency, in raising this issue in its submission, comments that it is not proposing that the System Operator would have an allied responsibility to monitor a representative's compliance with their obligations.[25]

Evidence to support a safety net decision

The Agency submission proposes that consideration be given to how the System Operator might be satisfied that a person poses a risk to another's health or safety. Liaison with other bodies – such as the Family Court of Australia, police, schools or refuges – may be needed to obtain relevant information. (This issue would be equally relevant to any power conferred on the System Operator to cancel MHR access of a representative who was not meeting their obligation to give effect to a recipient's will and preferences.)

There is no apparent constraint in the MHR Act on the System Operator gathering information that may be relevant to the exercise of a safety net power. It is presumptively open to an administrator to collect information from any source and to take account of it in making a decision (as reflected in the familiar statutory instruction to administrative tribunals that the tribunal is 'not bound by the rules of evidence but may inform itself in such manner as it thinks appropriate'[26]).

---

[23] MHR Act s 7A.
[24] MHR Rule 2016 r 13(1)(b).
[25] Submission No 28 (Agency) p 13.
[26] Eg *Administrative Appeals Tribunal Act 1975* (Cth) s 33(1)(c).

Legal constraints can subsequently apply after information is collected. For example, personal information must be managed in accordance with the Privacy Act; and administrative law principles (such as procedural fairness) can affect the reliance that can be placed on particular items of information.

The larger issue is whether government and non-government entities are legally free to provide information to the System Operator. It is common that secrecy provisions and privacy laws constrain information sharing between entities. On the other hand, as the Agency submission notes, New South Wales law facilitates information sharing between entities that have responsibilities relating to the safety, welfare or wellbeing of children.[27]

Privacy laws often contain a similar exception, allowing disclosure for the secondary purpose of lessening or preventing a serious threat to a person's life, health or safety.[28] Generally, too, there is no constraint on a court directing that a court order that be notified to another body if it raises personal safety issues.

Another option that is sometimes adopted between entities (when permitted by legislation) is to enter into a joint memorandum of understanding to facilitate information sharing and protection.

This matter could best be taken forward by the Department of Health undertaking a study of Commonwealth, state and territory legislation and administrative protocols that may bear upon information sharing of the kind envisaged by the Agency. Recommendation 7 below is to that effect.

Deletion of an MHR by an authorised representative

The System Operator is required to cancel a person's registration in the MHR system if requested to do so either by the person[29] or by their representative.[30] Following a change to the MHR Act in 2018,[31] the System Operator is also required to destroy all health information in a person's MHR upon cancellation of their registration.[32]

A difficulty can arise if a person has more than one authorised representative. The System Operator is required to act on the instruction of any one representative. Prior to the 2018 changes the System Operator would notify any other authorised representatives that an MHR registration had been cancelled. A representative who disagreed with that action could re-register the person and restore their MHR.

That is no longer feasible, as the record of health information will have been destroyed. To mitigate the risk of a disputed cancellation and record destruction, the System Operator follows an administrative protocol of writing to all authorised representatives prior to implementing an instruction to cancel a person's registration. If the representatives are in disagreement, the System Operator will not take further action on the basis that contradictory instructions have been received.

---

[27] *Children and Young Persons (Care and Protection) Act 1998* (NSW) Ch 16A.
[28] Eg *Privacy Act 1988* (Cth) s 16A(1), item 1 ('permitted general situation … in relation to the … disclosure of personal information').
[29] MHR Act s 51(1).
[30] MHR Act ss 6(7), 7(2). Under those provisions, the instruction to cancel a person's MHR can be given by either an authorised or a nominated representative. The My Health Record website incorrectly states that a nominated representative cannot cancel a healthcare recipient's MHR: Australian Digital Health Agency, My Health Record, 'Nominated Representatives' https://www.myhealthrecord.gov.au/for-you-your-family/howtos/nominated-representatives. In practice, that is often a stated condition in the written agreement to make a person a nominated representative. For that reason the issue is discussed in this report as one that principally relates to cancellation action initiated by an authorised representative.
[31] *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) Sch 1 cl 6.
[32] MHR Act s 17(3).

As the Agency submission suggests, a clearer procedure would be to amend the MHR Act to provide that the System Operator must be satisfied that all representatives are in agreement before acting on the instructions of any one representative to cancel a person's MHR registration and destroy health information in their record. Recommendation 6 below endorses that suggestion.

Misuse of information obtained while a representative

Another unique problem raised by the Agency in consultation is that a person who was a nominated representative of a former partner may have obtained MHR health information about the partner and later seek to use that information to the partner's detriment in Family Court proceedings.

It would be hard to frame a statutory provision to deal specifically with a problem of that kind. The MHR Act already provides some protection, and perhaps adequate protection, against misuse of information. As noted above, the duty of a nominated representative is to give effect to the healthcare recipient's will and preference in relation to their MHR or, if that is not known, to act in a manner that promotes the recipient's personal and social wellbeing.[33]

That could be construed as a continuing and enforceable legal obligation owed to the healthcare recipient by a current or former representative. Consequently, the healthcare recipient could object to a person who was formerly a representative using any information they had obtained in that capacity. The objection could be raised in any contested Family Court proceedings or the recipient could apply to a court for an injunction to restrain any breach of the obligation.

Temporary protection measures

Another issue is whether the System Operator should have power to 'lock' a person's MHR while a threat of harm to that person is investigated.

The MHR Rule 2016 presently requires the System Operator to suspend access by an authorised or nominated representative to a healthcare recipient's MHR in 2 situations – while investigating a claim that an authorised representative is not eligible to be a representative;[34] and while investigating if a representative poses a risk of harm to an individual.[35] In light of those powers, it is not clear that a broader power to suspend access or lock an MHR is required.

Resolving a dispute between representatives

The System Operator has no direct function or power to resolve a dispute between representatives. The lack of any such function is more likely to be an issue when there is a dispute between the authorised representatives of a child.

Recommendation 6 proposes that the System Operator should have a general power to initiate action to remove access by a representative to a person's MHR if there is reason to believe that the representative is unable or unwilling to act in a way that promotes the personal and social wellbeing of the healthcare recipient. Recommendation 6 also proposes that the System Operator must be satisfied that all representatives are in agreement before acting on the instructions of any one representative to cancel a person's MHR registration.

Beyond those powers, it would be problematic to require the System Operator to play a more general or active role in resolving disputes between representatives. If faced with contradictory instructions given by representatives, the System Operator can decide not to act until the disagreement is resolved by the parties – for example, through normal family or community dispute resolution procedures.

---

[33] MHR Act s 7A.
[34] MHR Rule 2016 r 14.
[35] MHR Rule 2016 r 15.

Removing information from the MHR system

The System Operator has several powers under the MHR Act and the MHR Rule 2016 to destroy or remove records in the MHR system. The Agency submission queries whether those powers are adequate and properly aligned.

The main powers are as follows:

- If requested by a healthcare recipient, the System Operator is required to cancel the recipient's registration in the MHR system.[36] In so doing, the System Operator is to destroy any health information in the recipient's MHR, leaving only their name, their healthcare identifier and the date of cancellation.[37]
- A healthcare recipient may 'effectively remove' a record from their MHR under the default access controls but also restore that record.[38] 'Effective removal' means that (unless restored) the record is inaccessible through the MHR system to the healthcare recipient, their representatives and healthcare provider organisations.[39]
- The System Operator may 'effectively remove' a record in the MHR system, or direct a participant (such as a repository or portal operator) to do so, for the following reasons:
  - the record contains a defamatory statement
  - the record is likely to affect the security, integrity or operations of the MHR system
  - the record that was uploaded by a registered healthcare organisation was prepared by a person who was not authorised to prepare a record for MHR purposes.[40]

  The System Operator is to notify the healthcare recipient that a record has been removed. A participant may upload a replacement record that addresses the concern that led to its effective removal.[41]
- The System Operator also has functions relating to records management:
  - to maintain a register that includes such administrative information about registered healthcare participants as is necessary for the purposes of the operation of the MHR system[42]
  - to ensure that the MHR system is administered in a way that resolves problems relating to its administration[43]
  - to do anything incidental or conducive to those or other functions.[44]

The Agency submission raises several queries:

- Can the System Operator remove a record from a healthcare recipient's record for an unspecified purpose – for example, because the record has been uploaded to the wrong MHR?
- Can the System Operator remove a record that poses a risk to clinical or personal safety?
- If the System Operator removes a record for one of those reasons, should the healthcare recipient be notified, and can the record be destroyed or only 'effectively removed'?

---

[36] MHR Act s 51(1).
[37] MHR Act s 17(3)
[38] MHR Rule 2016 r 5(e).
[39] MHR Rule 2016 r 4, definition of 'effectively remove', and rr 7(2)(c), 8(2(c).
[40] MHR Rule 2016 r 21.
[41] MHR Rule 2016 r 21(3)(b).
[42] MHR Act ss 15(e), 56, 57.
[43] MHR Act s 15(k).
[44] MHR Act s 15(o).

The first point to make in response to those questions is that effect must be given both to the specific removal powers listed above (that are relatively clear in scope) and to the more general System Operator functions of regular and efficient administration of the MHR system[45] (discussed earlier). It is noteworthy that the rule authorising the System Operator to remove records for specific reasons (defamation, security, integrity, unauthorised content) declares that this power does not 'by implication [affect] the System Operator's functions or powers to manage the MHR system'.[46]

Consequently, the System Operator would have power to remove a document for administrative reasons, such as correcting an uploading error. This could be done without notifying the healthcare recipient and by effectively destroying the record as entered in the recipient's MHR. Removal in those circumstances does not involve any substantive disturbance of the recipient's MHR. (Though not required, it would be open to the System Operator to advise a healthcare recipient of this action.)

On the other hand, removing a record for reasons of clinical or personal safety does involve a substantive disturbance or rearrangement of the record and should be done on a clear statutory footing. This view is reinforced by the provisions of the MHR Act and the MHR Rule 2016 that prescribe specific circumstances in which MHRs can be altered.

Overall, it would be better if the MHR Act or MHR Rule 2016 was amended to spell out in a consolidated and comprehensive way the powers of the System Operator to manage and control the upload, removal and destruction of records in the MHR system.[47] This would remove the need for the System Operator to rely on the general MHR system management functions. A recommendation to this effect is made below.

Ensuring regulatory compliance in healthcare provider organisation registration

A function of the System Operator is to register healthcare provider organisations as participants in the MHR system.[48] Once registered, an organisation can collect, use and disclose MHR patient health information for the purpose of providing health care to a registered healthcare recipient.[49]

The OAIC submission to this inquiry[50] was critical of a lack of rigour in the registration process. This criticism was based on a series of privacy assessments the OAIC initiated in 2019 of healthcare provider organisations that had applied to be registered as participants in the MHR system. The OAIC's view was that numerous organisations did not comply with the statutory requirements of the MHR Act and MHR Rule 2016 at the time of registration and during subsequent use of the MHR system following registration. The OAIC submission proposed that this problem be addressed by a legislative amendment to the MHR Act to impose a stronger regulatory compliance obligation on the System Operator.

The statutory context for the OAIC's view will be explained:

- The MHR Act sets out the requirements to be registered as a participant, including the procedure to be followed and the conditions to be met at the time of registration and subsequently.

---

[45] Eg *K&S Lake City Freighters Pty Ltd v Gordon & Gotch Ltd* (1985) 157 CLR 309, 315, on interpreting statutory words in context.
[46] MHR Rule 2016 r 21(4).
[47] An analogous control is that a healthcare provider organisation has no obligation to upload any specific record to the MHR system and could, for example, decide not to upload a record on clinical or personal safety grounds.
[48] MHR Act s 15(f), Pt 3 Div 2.
[49] MHR Act s 61.
[50] Submission No 36 (OAIC).

- The System Operator has an obligation to register a healthcare provider organisation that meets 4 prerequisites:
  - the organisation has a healthcare identifier
  - it complies with the requirements of the MHR Rule 2016
  - it agrees to be bound by any conditions imposed by the System Operator
  - the System Operator has not assessed the organisation to be a threat to the security or integrity of the MHR system.[51]
- The MHR Act imposes standard conditions on registered organisations regarding the preparation of records that are uploaded to the MHR system, the uploading procedure and the obligation of a registered organisation not to discriminate against people who do not have an MHR or who have an MHR but have set access controls.[52]
- The MHR Rule 2016 sets out a range of *general* and *security* requirements that must be met by a healthcare organisation to be registered as a participant.[53] Importantly, the MHR Rule 2016 states that a healthcare organisation must comply with these requirements 'to be eligible, and remain eligible, for registration'.[54]
- The MHR Act provides that the System Operator may cancel or suspend the registration of an entity that no longer meets the registration requirements, has contravened the MHR Act or a condition of registration or poses a threat to the security and integrity of the MHR system.[55]
- Among the *general* registration requirements in the MHR Rule 2016 are that a registered organisation must act through authorised officers, those officers must exercise due care and skill in uploading and downloading documents, the System Operator must be notified of material errors, and software system interoperability must be maintained.
- The most important of the *security* registration requirements in the MHR Rule 2016 (and the one singled out in the OAIC submission) is the obligation of a registered organisation to have a written policy that deals with access to the MHR system, training, physical and information security measures and identifying security risks.[56] The policy must be communicated to all employees of the organisation and, upon request, to the System Operator.

The OAIC submission noted that none of the organisations it had assessed had a security policy at the time their registration was approved.

The legislative amendment the OAIC proposes (to ss 44 and 51(3) of the MHR Act) is twofold: to require a healthcare provider organisation, when applying for registration, to provide evidence that it meets the requirements of the MHR Rule 2016; and to require the System Operator to confirm that evidence and to take action if the organisation is noncompliant either at the time of registration or subsequently.

There is merit in the OAIC proposal, particularly in a setting where registration entitles an organisation to access sensitive MHR patient health information. A statutory duty on the System Operator to ensure compliance by others with registration requirements would be a proportionate mechanism.

On the other hand, the MHR Act currently contains the powers necessary to achieve the desired objective:

- A condition of registration is that an organisation meets and continues to meet eligibility requirements, such as the obligation to have a security policy.

---

[51] MHR Act ss 42–44.
[52] MHR Act ss 45–46.
[53] MHR Rule 2016 rr 25–32A, 41–45.
[54] MHR Rule 2016 rr 25, 41.
[55] MHR Act s 51(3).
[56] MHR Rule 2016 r 42.

- The System Operator is required to devise the registration application form,[57] which could include an obligation to provide all necessary evidence.
- A function of the System Operator is 'to manage and monitor, on an ongoing basis, the system of registration'.[58]
- The System Operator may also cancel or suspend the registration of an organisation that, at any time, fails to comply with the eligibility requirements for registration.[59]

The problem the OAIC has raised may have more to do with the manner in which those powers are being administered than with those powers being cast in a discretionary rather than mandatory form. The OAIC submission notes that the function of registering organisations under s 44 of the MHR Act has been delegated by the Agency (as System Operator) to the Chief Executive Medicare, and the function is exercisable by Services Australia.[60] It may be that the administration of the registration process is a matter that should first be explored between the Agency and Services Australia.

Furthermore, it is always open to the Australian Information Commissioner to draw attention to problems of this kind in the annual report on the commissioner's activities relating to the MHR system.[61]

On the basis of those considerations, this report does not recommend an amendment to the MHR Act as proposed by the OAIC. However, the OAIC has raised an important issue regarding the operation of the MHR system. If the issue is not adequately addressed, the need may arise to consider the option of legislative amendment along the lines proposed.

Recommendations

The following recommendations are made to give effect to the findings in this chapter:

- ***Recommendation 5:*** This recommendation is tied to the discussion in this chapter of the System Operator's functions listed in s 15 of the MHR Act. The discussion noted that some functions are narrowly framed and do not provide explicit support for System Operator activities that would be beneficial to the MHR system.
- ***Recommendation 6:*** This recommendation is tied to the discussion of the System Operator's powers in this chapter and proposes that some powers be clarified or extended. This includes safety net powers that the System Operator could use to safeguard the interests of vulnerable healthcare recipients who are registered in the MHR system.
- ***Recommendation 7:*** Doubt has been expressed as to whether Commonwealth, state and territory laws may impede the System Operator from obtaining information that could support an exercise of the System Operator's safety net powers to safeguard the interests of vulnerable healthcare recipients. This recommendation proposes that the Department of Health explore this matter in discussion with the states and territories.

Recommendation 5

The Department of Health consider the desirability of amending the MHR Act to provide more explicitly that the functions of the System Operator listed in s 15 of the Act include:

- using health information from the MHR system for the purpose of performing a function or exercising a power under the Act (and, in particular, to perform the function of establishing and maintaining a reporting service in s 15(d))

[57] MHR Act s 42(2)(a), and definition of 'approved form' in s 5.
[58] MHR Act s 15(f).
[59] MHR Act s 51(3).
[60] MHR Act s 98.
[61] MHR Act s 106.

- establishing and conducting testing in both a test environment and the MHR system (or live environment)
- testing MHR system data to assess if it conforms to specifications and standards for the MHR system
- undertaking analysis of clinical governance and clinical safety in MHR system data and in the MHR system
- notifying registered healthcare recipients and registered healthcare provider organisations of any matters arising from or connected to the operation of the MHR system.

Recommendation 6

The Department of Health consider the desirability of amending the MHR Act to:

- authorise the System Operator to impose a charge for specified activities
- extend the terms of s 6(1A)(b) to the circumstances of any healthcare recipient – that is, to authorise the System Operator not to recognise a person as an authorised or nominated representative of a healthcare recipient if doing so is likely to put at risk the life, health or safety of the healthcare recipient or another person
- authorise the System Operator to initiate action to remove a representative's access to a person's MHR if the System Operator has reason to believe that the representative is unable or unwilling to act in a way that promotes the personal and social wellbeing of the healthcare recipient; or, in the alternative, to make a representative's obligation under s 7A of the MHR Act to act in accordance with a healthcare recipient's will and preferences an eligibility requirement for a person to have access to the healthcare recipient's MHR
- provide that the System Operator must be satisfied that all representatives of a healthcare recipient are in agreement before the System Operator is required to act on the instructions of any one representative to cancel a person's MHR registration and destroy health information in their record
- consolidate and revise the provisions of the Act that authorise the System Operator to manage and control the upload, removal and destruction of records in the MHR system.

Recommendation 7

The Department of Health review (and prepare a report on) Commonwealth, state and territory laws and administrative protocols that regulate the capacity of government entities to provide information to the System Operator that may be relevant to the responsibilities of the System Operator under the MHR Act to take action to protect the life, health or safety of a healthcare recipient.

Chapter 5. Privacy protection under the My Health Records Act

Security and privacy safeguards in the MHR system

The essential premise of the MHR system is that it is a safe and secure system for facilitating electronic access to personal health information. Security and privacy safeguards have been at the forefront of all planning and public discussion.

The importance attached to MHR security and privacy safeguards is captured in the following 2 comments – the first is from the 2018 Senate Community Affairs References Committee report *My Health Record system*; and the second is from the submission to this current review by the Office of the Australian Information Commissioner (OAIC):

> *The MHR system is a significant healthcare reform with the potential to improve the quality of healthcare and health outcomes for many Australians. To achieve this, the system needs a high degree of support from both the public and medical practitioners [who] need to have a high degree of confidence in the integrity of the system.*[62]
>
> *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. … 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.*[63]

Many system features discussed in other chapters of this report are designed with privacy and security objectives in mind:

- The MHR system uses a federated model that draws health information from repositories that are independently managed, rather than storing all information in a central database.
- A consumer can choose whether to have an MHR and can cancel their registration at any time, leading to the destruction of all health information in their MHR.
- Healthcare provider organisations must be registered to access the MHR system.
- A consumer can control the health information that is uploaded to their MHR, as well as access to their record, by setting a Record Access Code, Limited Document Access Code or healthcare provider access list.
- A consumer can invite a person to be a nominated representative to help manage their MHR.
- A consumer can require email or SMS notification when their MHR is accessed by a healthcare provider or representative.
- A consumer must consent to their personally identifiable health information being used in public health research.
- An electronic access history log is kept of all access to a person's record to upload, view or change documents.
- The OAIC maintains privacy oversight of the MHR system and can investigate privacy breaches.
- The System Operator has regulatory powers to suspend or cancel access to the MHR system by a person or organisation in order to safeguard individual safety or the security or integrity of the system.

---

[62] Senate Community Affairs References Committee, Parliament of Australia, *My Health Record system* (October 2018) para 5.1.
[63] Submission No 36 (OAIC).

- There is a prohibition against MHR health information being used for insurance or employment purposes.
- Criminal and civil penalties apply to the unauthorised collection, use or disclosure of MHR patient information.

The importance that Australians attach to privacy protection has been recorded in the periodic surveys on Australian community attitudes to information privacy that the OAIC conducts. The 2020 survey results found that 70% of respondents consider that protection of personal information is a major concern in their life. Among the biggest risks that people believe they face are data security and data breaches (61% of respondents) and the operation of digital services (58%). The organisations that were considered most trustworthy in handling personal information were health service providers (70% trustworthy / 11% untrustworthy) and federal government agencies (51%/25%). Activities that respondents singled out as a potential misuse of their personal information included defective management of personal information (84%) and use of personal information for a purpose different to that for which it was collected (84%).

The *Privacy Act 1988* (Cth) reflects the importance that people attach to health information privacy by classifying 'health information about an individual' as 'sensitive information'.[64] So classified, health information generally has a higher level of privacy protection, particularly as to collection, use, disclosure and direct marketing.[65]

Privacy and security were prominent issues in the consultations and submissions for this review. Several contrasting themes were aired:

- A number of submissions (particularly from healthcare consumers) emphasised the importance of strong privacy and security safeguards in the MHR system.[66] Some submissions queried whether adequate privacy protection was possible and pointed to the proportion of Australians (10%) who had chosen to opt out of the MHR system.
- A few submissions (particularly from professional organisations) felt that privacy and security risks had been well handled in both the design and the operation of the MHR system.[67] This theme is taken up in the next section of this chapter, which describes the reported views and findings of the Australian Digital Health Agency (the Agency), the OAIC and the Australian National Audit Office (ANAO).
- There was general acknowledgement that privacy impact is likely to be a relevant factor in evaluating any proposed change to the MHR Act or related legislation. This theme is taken up in other chapters in this report. For example, privacy considerations are dealt with in Chapter 7, which discusses the circumstances in which access controls set by a healthcare recipient can be overridden; and in Chapter 11, which discusses the conditions applying to the use of MHR patient information for public health research.
- The privacy framework in the MHR Act, while generally complimented in this review, was singled out for adverse comment on a few specific features. Topics discussed below that have attracted criticism are the data breach notification requirements in the MHR Act and gaps in the OAIC's privacy oversight functions and powers.

Another preliminary matter to note is that a general review of the Privacy Act commenced in October 2020, with the publication of an issues paper by the Attorney-General's Department.[68] The impetus for the review is the need to tailor privacy protections to digital services and transactions.

---

[64] *Privacy Act 1988* (Cth) s 6(1).
[65] See Australian Privacy Principles 3.3, 6.2(a)(i), 7(3). See also *Privacy Act 1988* (Cth) s 16B relating to 'permitted health situation'.
[66] Eg submission Nos 2 (Anon), 3 (Anon), 4 (Anon), 5 (Anon), 21 (Fell), 22 (PPA), 24 (Fernando), 27 (PSA), 31 (Arnold).
[67] Eg submission Nos 8 (Anon), 23 (AIHW), 29 (MIGA), 37 (Pharm Guild), 40 (AMA), 41 (RACGP).
[68] Attorney-General's Department, *Privacy Act review: issues paper* (October 2020).

The MHR Act is not within the scope of the Privacy Act review. However, the issues paper notes that the Privacy Act interacts with privacy protection frameworks in other Commonwealth regulatory schemes, such as the MHR system. The paper invites submissions on the continuation of separate privacy protection frameworks and whether greater harmonisation of those different frameworks is desirable.[69] Many of the key concepts and issues that will be examined in the Privacy Act review also have an MHR relevance – such as the definition of 'personal information', consumer consent requirements, the criteria for data breach notification, and creation of a right of action for privacy breaches.

Evaluation of MHR security and privacy safeguards

The annual reports of the Agency and the OAIC, together with a recent review of privacy and security risks by the ANAO, are a good benchmark for evaluating the operation and effectiveness of the security and privacy safeguards in the MHR system. The composite picture from those reports is that security and privacy have been well managed.

Agency annual reports

The MHR Act requires the System Operator to prepare an annual report that includes statistics on complaints received in relation to the MHR system, occurrences that compromise the integrity or security of the system, and other regulatory enforcement action by the System Operator.[70]

The Agency's annual report for 2018–19 included the following information:[71]

- There were no purposeful or malicious attacks during the year that compromised the integrity or security of the MHR system.
- Under the data breach notification requirements in the MHR Act, 76 matters were notified to the OAIC by entities (38 matters), the System Operator (4) and Services Australia as a Registered Repository Operator (34). Most of these breaches were attributable to administrative error (such as intertwined records), 3 involved unauthorised access to a person's record, and 7 involved suspected Medicare fraud that was logged in information uploaded to MHR.
- The Agency received 304 complaints and over 10,000 enquiries. The majority of these related to the transition in the reporting year to an opt-out system and a healthcare recipient's ability to delete a record.
- The System Operator did not accept any enforceable undertakings during the year or initiate proceedings in relation to enforceable undertakings or injunctions.

The Agency's annual report for 2019–20 included the following information:[72]

- Two matters were reported under the data breach notification requirements – one by the System Operator (a possible compromise to external IT infrastructure) and one by a state/territory authority (a potential unauthorised access to MHR). Both matters were investigated and resolved without compromise to the system.
- The Agency received 134 complaints in relation to MHR.
- The System Operator did not accept any enforceable undertakings during the year or initiate proceedings in relation to enforceable undertakings or injunctions.

---

[69] Ibid p 86.
[70] MHR Act s 107.
[71] Australian Digital Health Agency, *Annual report 2018–19* (2019) p 62.
[72] Australian Digital Health Agency, *Annual Report 2019–20* (2020), section on 'MHR system registration, usage, security and complaints'.

OAIC annual reports

In the OAIC's words, since 2012 it has been 'the independent regulator of the privacy aspects of the MHR system'.[73]

The MHR Act provides that a contravention of the Act in relation to a person's MHR patient health information is to be treated as an interference with privacy that can be investigated by the OAIC under the Privacy Act.[74] Consequently, the OAIC can exercise the functions and powers conferred upon it by the Privacy Act – such as complaint handling, own-motion investigations, compliance assessments, and enforcement powers that include determinations, enforceable undertakings, injunctions and civil penalties. Those functions are discharged in accordance with the *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016*.

The OAIC's MHR privacy oversight work is funded through a memorandum of understanding with the Agency – with an expenditure of $2.07 million in 2019–20. Recommendation 1 in Chapter 3 of this report supports the alternative of a direct budgetary appropriation to the OAIC for this work.

The Australian Information Commissioner is required by the MHR Act to prepare an annual report on OAIC activities during the year relating to the MHR system, including statistics on complaints, investigations and regulatory enforcement action. (The following summary does not include the statistics on data breach notification, which are given above in the Agency's annual reports.)

The OAIC annual report for 2018–19[75] advised that the OAIC:

- received 57 complaints and 145 enquiries (many related to the transition to opt-out and the deletion of records)
- conducted 4 privacy assessments (1 carried over from the previous year). The assessments examined compliance with Australian Privacy Principle (APP) standards by the Agency, private hospitals (2), pharmacies (14) and pathology and diagnostic imaging services (8)
- made 2 submissions to the Senate Community Affairs References Committee and Community Affairs Legislation Committee in relation to MHR inquiries the committees were undertaking
- provided policy advice to the Agency and stakeholders (15 instances related to MHR system), published a range of written and video guidance materials (many relating to the opt-out transition) and participated in public events
- liaised with the Department of Health and the Australian Institute of Health and Welfare on the secondary research use of MHR system data
- generally monitored developments in digital health and the MHR system.

The OAIC annual report for 2019–20[76] included similar information about the advice, liaison, monitoring and public education work undertaken during the year. The specific statistics for the year were that the OAIC:

- received 10 complaints
- conducted 6 commissioner-initiated investigations
- commenced 1 new privacy assessment and continued or closed 5 others. The new assessment was of mobile health applications that access MHR.

---

[73] Submission No 36 (OAIC).
[74] MHR Act s 73.
[75] Office of the Australian Information Commissioner, *Annual report of the Australian Information Commissioner's activities in relation to digital health 2018–19* (2019).
[76] Ibid.

ANAO inquiry

The ANAO completed a performance audit in November 2019 of the implementation of the MHR system under the opt-out model.[77]

The ANAO's 2 main findings in relation to security and privacy were:

- Risks relating to privacy and the IT system core infrastructure were largely well managed and were appropriately informed by privacy risk assessments and cybersecurity measures.
- Management of shared cybersecurity risks could be improved with respect to risks shared with third-party software vendors and healthcare provider organisations.

The ANAO made 5 recommendations that were accepted by the Agency and the Department of Health:

- the Agency update its risk management framework after conducting an end-to-end privacy risk assessment of MHR
- the Agency and the department, in consultation with the OAIC, review the procedures for monitoring use of the emergency access function in the MHR Act and notifying contraventions to the OAIC under the data breach notification requirements
- the Agency develop an assurance framework for connecting third-party software to MHR
- the Agency develop and report on a strategy to monitor compliance with legislative requirements relating to security by registered healthcare provider organisations and contracted service providers
- the agency develop a program evaluation plan for MHR.

The Agency published a plan in February 2020 that outlined how the recommendations would be implemented.[78] This work is expected to be completed late in 2020.

Data breach notification under the MHR Act

The MHR Act was the first national law to include a data breach notification scheme (in 2012). It operates alongside the comprehensive national scheme in Part IIIC of the Privacy Act that commenced later in 2018. The Privacy Act scheme does not apply to data breaches that are required to be notified under the MHR scheme.[79]

Some entities are subject to both notification schemes: examples include most health service providers,[80] private hospitals, medical clinics, pharmacies, Australian Government agencies, and contractors that fall under the MHR Act. On the other hand, some entities are subject only to the MHR notification scheme, such as state and territory health authorities.[81]

---

[77] Australian National Audit Office, *Implementation of the My Health Record system* (Report No 13, 2019–20).
[78] Australian Digital Health Agency, *ANAO Health Record Performance Audit Implementation Plan* (February 2020).
[79] *Privacy Act 1988* (Cth) s 26WD.
[80] The Australian Privacy Principles and the data breach notification scheme apply to an 'APP entity' (ss 13, 26WE). The term 'entity' is defined in s 6(1) to include an 'agency' (that is, Australian Government agency) and 'organisation' (which includes an individual, body corporate, and partnership: s 6C). There is an exemption for small business operators with an annual turnover of less than $3 million, but that exemption does not apply to a body that 'provides a health service to another individual and holds any health information except in an employee record' (s 6D(4)(b)).
[81] The Privacy Act definition of 'entity/organisation' excludes 'a State or Territory authority' (s 6C(1)).

There is general acceptance of the need for a separate MHR scheme. The main issue that has been raised is whether the MHR scheme should be reframed so that it is more similar to and harmonised with the Privacy Act scheme. A particular concern is that the notification obligations under the MHR scheme apply more broadly and are less clear as to what must be reported.

Both schemes will be briefly described.

Privacy Act data breach notification scheme

An entity that is subject to the Privacy Act scheme (known as an 'APP entity') is required to give notice of an 'eligible data breach' that has the following elements:

- the APP entity holds personal information about one or more individuals
- there has been a loss or unauthorised access to or disclosure of that personal information
- the breach could result in serious harm to an individual to whom the information relates.[82]

The APP entity is to notify the breach to the OAIC and to each individual who is at risk, providing information on steps that can be taken in response to the data breach.[83] If it is not practicable to notify each individual, reasonable steps must be taken to publicise the breach on the entity's website and in other appropriate ways.

The OAIC can investigate whether the APP entity has met its notification obligations and whether the entity is in breach of APP 11, which requires that reasonable steps be taken to secure personal information.

Two key features of the Privacy Act scheme should be noted:

- it only applies to data breaches that could result in serious harm to individuals
- a breach is to be notified to individuals who may be affected (if practicable).

Those 2 features were explained by the Minister in the second reading speech as 'the rationale for mandatory data breach notification', so that individuals who are likely to be at risk of serious harm can take action to protect themselves (for example, by changing an online password or cancelling a credit card).[84] More generally, the mandatory notification scheme reinforces the requirements of the APPs for entities to manage information securely and be transparent about information-handling practices.

MHR Act data breach notification scheme

The data breach notification scheme in the MHR Act applies to the Agency, registered healthcare provider organisations, registered portal and repository operators, and contracted service providers (described as 'entities').[85] An entity is required to give notice of a data breach, in which it is directly involved, of either of 2 kinds:

- a person may have contravened the MHR Act by the unauthorised collection, use or disclosure of MHR patient health information
- there has been an event or circumstance (regardless of whether it is a contravention of the MHR Act) that may compromise the security or integrity of the MHR system.

An entity is to notify the breach to both the System Operator and the Australian Information Commissioner – with the exception of a state or territory authority that is to notify only the System Operator. A civil penalty applies if this notification obligation is not complied with.[86]

---

[82] *Privacy Act 1988* (Cth) s 26WE.
[83] *Privacy Act 1988* (Cth) ss 26WL, 26WK.
[84] Commonwealth, *Parliamentary Debates*, House of Representatives, 19 October 2016, 2430 (Minister for Justice, Michael Keenan).
[85] MHR Act s 75(1)(a).
[86] MHR Act s 75(2).

The System Operator's obligation is to notify the Australian Information Commissioner of breaches that either directly involve it or of which it becomes aware.[87]

The nature of the obligation to notify a breach to individual healthcare recipients is not straightforward:[88]

- An individual is to be notified of a contravention, event or circumstance that '*may have occurred* or arisen … if there is a reasonable likelihood that … the effects ... might be serious'.
- An individual is to be notified if a contravention, event or circumstance *has occurred* or arisen that has 'affected' them (though double notification is not required[89]).
- If a 'significant number of healthcare recipients' were affected by a breach that has already occurred or arisen, the general public is to be notified as well.
- The obligation to notify affected individuals rests on the System Operator.
- The obligation of other entities, upon becoming aware of a notifiable breach, is to 'ask the System Operator' to notify individuals, and the System Operator must comply.[90]

In addition to those notification obligations, an entity is also obliged to take reasonably practicable steps to contain a potential or actual data breach and to undertake a risk analysis of the elements of the breach.[91]

Criticisms of the MHR Act data breach notification scheme

Several submissions made the general point that it is confusing and burdensome for entities to comply with 2 data breach notification schemes that are differently framed.[92] The preference expressed in the submissions is for the MHR scheme to be altered so as to harmonise with the Privacy Act scheme.

Specific criticisms can also be levelled at the MHR scheme:

- The range of notifiable data breaches is indeterminate – for example, when is an entity 'directly involved' in a breach and when does an event potentially compromise the 'security or integrity' of the MHR system?
- Notwithstanding that uncertainty, the range of notifiable breaches appears to be quite extensive, embracing contraventions of the MHR Act that may be more technical than serious and also events that pose a risk to MHR security and integrity even though no contravention of the Act has occurred.
- It is questionable whether there should be an obligation to notify a data breach to the OAIC (and potentially affected individuals) when the breach can easily be rectified without posing any risk to an individual. Examples that appear to fall within the notification requirements are an incorrect Medicare data entry that was promptly rectified; and an unauthorised but unsuccessful attempted data entry on an administrative support system.
- The obligation on entities to notify a data breach to the System Operator is difficult to discern because of the way the obligation is defined in the MHR Act[93] and the indeterminate elements that comprise the obligation.

---

[87] MHR Act s 75(3).
[88] MHR Act s 75(5), (6).
[89] MHR Act s 75(7).
[90] MHR Act s 75(8).
[91] MHR Act ss 75(5)(a), (b); 75(6)(a), (b).
[92] Submission Nos 19 (Defence), 27 (PSA), 28 (Agency), 29 (MIGA), 31 (Arnold), 35 (Avant), 36 (OAIC), 37 (Pharm Guild), 40 (AMA), 41 (RACGP).
[93] See MHR Act ss 75(5)(c) and 75(6)(c).

- It is questionable whether the responsibility to notify individuals of a data breach should be assigned exclusively to the System Operator and whether voluntary notification by an entity is permitted.[94]
- The extensive reach of the MHR scheme could result in an over-reporting of data breaches, which could be misinterpreted publicly as an indication of inherent security and privacy risks in the MHR system.[95]

Reform of the MHR Act data breach notification scheme

Based on those criticisms, there is a strong case for revising the data breach notification scheme in the MHR Act. The Privacy Act scheme provides a good model for doing this. It has clearer requirements and suitably focuses on notifying individuals of data breaches that pose a serious risk to the security of their personal information.

By comparison, the MHR scheme seems to conflate 3 different objectives:

- placing an obligation on entities to have procedures in place to maintain the security of patient health information
- requiring entities to keep the System Operator informed of events and circumstances in the MHR system that pose security, integrity or privacy risks
- requiring entities (or the System Operator) to notify the OAIC and individuals of data breaches that pose a threat to the security of personal information, so that individuals can take precautionary action if necessary.

Each of those objectives is independently important but could be separately presented in the MHR Act – as proposed in Recommendation 8.

It is appropriate that the MHR Act separately contains data breach notification requirements that apply to MHR data. The MHR system contains a large and growing volume of sensitive personal health information. As noted in the OAIC submission,[96] the MHR system has the unique feature of being a searchable network of connected registered repositories storing sensitive personal information.

MHR data breach notification requirements, while separate, should be aligned to the Privacy Act requirements. Harmonisation of the 2 schemes in that way would be coherent and respond to an understandable criticism that healthcare providers have made of the current MHR Act requirements.

OAIC privacy oversight functions and powers

The OAIC submission noted some gaps in the OAIC oversight functions and powers and recommended that these be resolved by amendment of the MHR Act.

OAIC oversight of state and territory government actions

As noted earlier in the discussion of data breach notification, the Australian Information Commissioner has privacy oversight of the actions of an extensive range of entities such as Australian Government agencies, health service providers, private hospitals, medical clinics and pharmacies. Consequently, the OAIC can apply a privacy lens to most activities occurring under the MHR Act.

---

[94] This point was made in submission No 35 (Avant), which explained that it and the System Operator held a different view on this point.
[95] This point was made in the submissions from the Agency (No 28) and MIGA (No 29).
[96] Submission No 36 (OAIC).

An important exception is that state and territory government authorities are not generally subject to the Privacy Act[97] – or, in turn, to the Australian Information Commissioner's privacy oversight under the MHR Act. This is in accordance with Australian federal arrangements, whereby each state or territory is largely responsible for supervision and accountability of agencies that discharge government functions. All but 2 states and territories (South Australia and Western Australia) have privacy or health information laws that apply to government agencies.

State and territory authorities that participate in the MHR system are nevertheless required to comply with the requirements of the MHR Act and subordinate laws. For example, state/territory authorities must be registered under the MHR Act to access the MHR system, and they are required to notify data breaches to the System Operator. The OAIC, however, cannot examine whether the actions of a state/territory authority contravene the MHR Act and constitute an interference with the privacy of a healthcare recipient.[98]

The consequence, for instance, is that the OAIC cannot examine MHR system privacy compliance in a state public hospital or health facility. Similarly, if a facility is jointly run by a private sector body and a state authority, the OAIC can examine privacy compliance by the private sector body but not the state authority. There could be a potential blind spot, for example, if it is unclear whether an action was that of a state or private sector staff member, if the interaction between those staff members was fluid and not precisely recorded, or if a staff member was unclear as to the privacy rules that apply to their actions.

A model for extending the Australian Information Commissioner's privacy oversight to state/territory government actions is the privacy oversight framework applying to COVID app data that was enacted in early 2020.[99] COVID app data collected by a Commonwealth body can be shared with state/territory health authorities for contact tracing purposes.

With the agreement of all Australian governments, the Privacy Act was amended to provide, first, that state/territory health authorities are subject to the purpose-designed privacy safeguards that apply to COVID app data and for the protection of COVIDSafe users[100] and, secondly, that the Australian Information Commissioner can examine contraventions of the Privacy Act safeguards by state/territory authorities and conduct assessments of their compliance actions.[101] As to investigation of complaints, the Privacy Act provides that the Australian Information Commissioner is to transfer to a state/territory privacy authority any matter that they could more conveniently deal with.[102]

In principle, a similar framework could be enacted as part of the MHR Act to extend OAIC privacy oversight to state/territory authorities. Another mechanism already in the Privacy Act is that a state or territory may request the Commonwealth to make a regulation that extends the Privacy Act to the activities of a state or territory authority.[103]

These options were raised with state and territory health agencies during the consultations for this review. Their informal response was that existing arrangements have worked satisfactorily since 2012. There are privacy authorities in most Australian jurisdictions that maintain active oversight of information handling by state/territory health agencies. It may create more rather than less confusion to carve out MHR privacy compliance from the state/territory oversight regime.

On the other hand, it is desirable that there is an integrated and coherent privacy oversight framework applying to the handling of personal health information in the MHR system. The importance of a single and effective privacy oversight framework may increase over time as the volume of health information and transactions in the MHR system expands.

---

[97] *Privacy Act 1988* (Cth) s 6C(1).
[98] MHR Act s 73(1), (3).
[99] *Privacy Act 1988* (Cth) Pt VIIIA.
[100] *Privacy Act 1988* (Cth) s 94X.
[101] *Privacy Act 1988* (Cth) ss 94R, 94T.
[102] *Privacy Act 1988* (Cth) s 94V.
[103] *Privacy Act 1988* (Cth) s 6C(4).

For the moment, an appropriate recommendation to make on this issue is that the Department of Health should continue to discuss options with state and territory health agencies for extending the Australian Information Commissioner's privacy oversight jurisdiction to all actions under the MHR Act.

OAIC oversight of the registration process

OAIC oversight of the privacy aspects of the MHR system does not extend to actions taken by the System Operator under Part 3 of the MHR Act in registering a healthcare provider organisation.

The System Operator can decline to register an organisation if satisfied that doing so may compromise the security or integrity of the MHR system, having regard to the requirements of the MHR Rule 2016.[104] The MHR Rule 2016 contains extensive requirements that an organisation applying for registration must meet in order to demonstrate its preparedness and capacity to comply with the requirements of the MHR Act and MHR Rule 2016.

OAIC oversight under the MHR Act extends to acts and practices that contravene the Act in relation to MHR patient health information and to compliance with Parts 4 and 5 of the Act.[105] Registration by the System Operator of a healthcare provider organisation occurs under Part 3 of the Act, and the act of registration itself does not have a connection with MHR patient health information.

The OAIC submission comments: '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'.[106] Recommendation 10 proposes that the OAIC's jurisdiction under the MHR Act be extended to include the oversight of the privacy aspects of the registration process.

Sharing information with the System Operator

The MHR Act provides that the Australian Information Commissioner can disclose to the System Operator information relating to an OAIC privacy investigation under the MHR Act if the commissioner is 'satisfied that to do so will enable the System Operator to monitor or improve the operation or security of the MHR system'.[107]

The scope of that authority to disclose is tied to an OAIC investigation. Information relating to privacy and security risks that becomes known to the OAIC as a result of its general oversight and monitoring activity is not expressly covered by the disclosure authority in the MHR Act (although disclosure of at least some OAIC insights would be incidental to the discharge of its privacy oversight functions).

Nevertheless, as the OAIC submission noted, recent amendments to the Privacy Act relating to COVID app data confer more extensive authority on the OAIC to share information with state and territory privacy authorities.[108] Disclosure can be done for the purpose either of the OAIC discharging its functions in relation to the handling of public contact information or of a state/territory privacy authority discharging its authorised functions. Before disclosing, the Australian Information Commissioner must be satisfied that a state/territory authority has satisfactory arrangements in place to protect any information provided by the OAIC.

The OAIC recommends that the MHR Act be amended to authorise in similar terms the disclosure of information by the commissioner to the Agency and Services Australia. This proposal is endorsed in Recommendation 11.

---

[104] MHR Act s 41(2).
[105] MHR Act s 73(1).
[106] Submission No 36 (OAIC).
[107] MHR Act s 73A.
[108] *Privacy Act 1988* (Cth) s 94W.

Other privacy issues

A few other points were raised in submissions that are briefly noted here but are not the subject of recommendations:

- The OAIC submission observed that there are inherent privacy risks in some new proposals for extending or re-platforming the MHR system. Examples include the application of artificial intelligence software, the interaction of the MHR system with other health record systems and the expansion of clinical uses of the MHR system.

  It is important, the OAIC noted, that any such proposals are outlined publicly in a way that enables proper assessment of privacy risks. An Agency strategic plan or 'futures roadmap' would be an ideal way of doing that. The OAIC submission further noted that the Agency may be required to undertake a privacy impact assessment of any new proposal by the *Privacy (Australian Government Agencies – Governance) APP Code 2017.*
- There was mention in some submissions of the new Consumer Data Right (CDR) introduced in 2020.[109] To bolster consumer choice, the CDR enables a person to direct an organisation to share their data via a secure online system with a competitor organisation accredited by the Australian Competition and Consumer Commission. This must be done in accordance with 13 Privacy Safeguards that are outlined in the legislation (based on the APPs). The CDR will apply first to the banking sector, followed by the energy and telecommunications sectors.

  The OAIC has a role in monitoring whether an accredited recipient complies with privacy safeguards and security requirements. There is also a new individual right of action for damages against an organisation that breaches the CDR privacy safeguards.[110]

  The CDR framework could possibly be adapted as a tailored privacy scheme, including private rights of action, applying to MHR patient information that is shared with third parties such as software developers. The development of direct rights of action to enforce privacy standards, including the award of civil damages for privacy breaches, is being examined as part of the Privacy Act review noted at the beginning of this chapter.
- The OAIC submission suggested that wider consideration be given to introducing an 'accreditation' system based on the CDR scheme. For example, the System Operator could be given a function of accrediting MHR system participants (such as healthcare provider organisations) as having adequate procedures in place to meet the security and privacy safeguards in the MHR Act and MHR Rule 2016.
- The Australian Privacy Foundation submission[111] called for stronger privacy protection and pointed to the limited scope of operation of s 71 of the MHR Act. It observed that patient health information that is obtained from the MHR system is not protected if it is subsequently stored and used on another system. An exception is that the prohibited purposes provisions may continue to apply to MHR patient health information after it has been downloaded from the MHR system. The Privacy Act and similar laws may also apply to health information that is held on other systems.

A submission from a privacy researcher[112] called for the MHR Act to be amended to require the System Operator to send a notice annually to record holders advising that they can cancel their registration (in effect, a half-way measure between an opt-in and opt-out scheme).

---

[109] *Competition and Consumer Act 2010* (Cth) Pt IVD.
[110] *Competition and Consumer Act 2010* (Cth) s 56EY.
[111] Submission No 30 (APF).
[112] Submission No 17 (Krieg).

Recommendations

Recommendations 8–11 address the following issues raised in the preceding discussion:

- ***Recommendation 8:*** The MHR Act contains data breach notification requirements that operate separately to those enacted in 2018 in the Privacy Act. The MHR Act appropriately contains separate requirements. However, the present requirements are complex and indeterminate and go further than may be required to meet notification objectives. There is strong support for harmonising the MHR Act requirements with those in the Privacy Act.
- ***Recommendation 9:*** The Australian Information Commissioner's privacy oversight functions under the MHR Act do not extend to the actions of state and territory health agencies. By contrast, the commissioner can examine contraventions by state and territory authorities of the Privacy Act safeguards applying to COVID app data. It would be desirable to have a single, coherent and integrated privacy oversight framework applying to the handling of personal health information in the MHR system. A necessary step in achieving that objective is for the Department of Health to consult on the options for doing so with its state and territory health counterparts.
- ***Recommendation 10:*** The OAIC's privacy oversight functions under the MHR Act do not extend to actions taken by the System Operator under Part 3 of the Act in registering a healthcare provider organisation. It is recommended that the OAIC's functions be extended to address this regulatory gap.
- ***Recommendation 11:*** The authority of the Australian Information Commissioner under the MHR Act to disclose information to the System Operator is tied to information relating to an investigation conducted by the commissioner under the Act. It is recommended that the commissioner have authority, more broadly, to disclose information relating to the regulatory oversight functions of the commissioner.

Recommendation 8

The MHR Act s 75 be amended to introduce data breach notification requirements that are, to the extent practicable, similar to those in Part IIIC of the *Privacy Act 1988*.

Recommendation 9

The Department of Health consult with state and territory health agencies as to the options for applying the Australian Information Commissioner's functions and powers under the MHR Act to the actions of state and territory authorities.

Recommendation 10

The MHR Act s 73 be amended to include compliance by the System Operator with a provision of Part 3 of the Act as a matter that can be investigated by the Australian Information Commissioner under s 73 of the Act.

Recommendation 11

The MHR Act s 73A be amended to confer a more general authority on the Australian Information Commissioner to disclose information or documents to the System Operator, the Department of Health and Services Australia for the purpose of the commissioner exercising powers or performing functions or duties under the Act.

Chapter 6. Interaction of the Healthcare Identifiers Act and the My Health Records Act

The healthcare identifier system

Healthcare identifiers (HIs) have been described as 'a key building block for the MHR system'.[113] A larger role has also been envisaged in the description of HIs as 'a foundational service for the broader digital health ecosystem in Australia'.[114]

The purpose of the Healthcare Identifiers Service (HI Service) is described in the *Healthcare Identifiers Act 2010* (Cth) (HI Act):

> *The purpose of this Act is to provide a way of ensuring that an entity that provides, or an individual who receives, healthcare is correctly matched to health information when healthcare is provided.*[115]

In short, a HI can be used in communicating and managing health information about healthcare consumers. Correctly matching health information to the consumer at the point of care supports the policy objectives of the MHR system. The aim is to ensure that health care provided to consumers is coordinated, continuous, well informed, safe, effective and consumer engaged.

Those aims have added importance in light of current trends of consumers being more likely to access multiple healthcare services and providers – geographically, throughout their lifetime, and in relation to individual health episodes and conditions.

A HI is a unique 16-digit number that identifies a healthcare recipient, a healthcare provider or a healthcare provider organisation. The HI Service is managed by Services Australia as the Healthcare Identifiers Service Operator under the HI Act.[116]

Identifiers are assigned by the HI Service and are of 3 kinds:[117]

- ***Healthcare recipient identifier:*** An Individual Healthcare Identifier (IHI) is assigned automatically to a person by the HI Service upon Medicare enrolment or registration with the Department of Veterans' Affairs. The number of IHIs assigned in the 10-year period from 1 July 2010 (when the HI Service commenced) to 30 June 2020 was 29,324,605, including 520,972 in 2019–20.[118]
- ***Healthcare provider identifier:*** An Individual Healthcare Provider Identifier (HPI-I) is assigned to an individual provider (such as a clinician, nurse, pharmacist or dentist) upon application to the Australian Health Practitioner Regulation Agency (AHPRA). AHPRA administers a National Registration and Accreditation Scheme for the health profession, in partnership with 15 National Boards. A healthcare provider who is not registered with one of the boards may apply directly to the HI Service for an HPI-I. The total number of HPI-Is assigned between 2010 and 2020 was 936,311, including 46,420 in 2019–20.[119]

---

[113] Services Australia, *Healthcare Identifiers Service annual report 2019–20* (2020) p 5.
[114] Ibid p 3.
[115] *Healthcare Identifiers Act 2010* (Cth) (HI Act) s 3(1).
[116] The HI Act s 6 provides that the 'service operator' is the Chief Executive Medicare. Funding for the HI Service is provided to the Australian Digital Health Agency, which has a service agreement with Services Australia to deliver the HI Service.
[117] HI Act s 9.
[118] Services Australia, *Healthcare Identifiers Service annual report 2019–20* (2020).
[119] Ibid.

- ***Healthcare provider organisation identifier:*** A Healthcare Provider Organisation Identifier (HPI-O) is assigned by the HI Service upon application by an organisation (such as a hospital, general practice or pharmacy). The HI Act[120] also incorporates an added distinction between 'seed HPI-Os' and 'network HPI-Os', to adapt to health organisation structures in which separate business areas or franchises are linked to an overarching healthcare organisation. The total number of HPI-Os assigned between 2010 and 2020 was 18,914, including 1,988 in 2019–20.[121]

The identifiers record minimal identifying details. An IHI records a person's name, date of birth and gender; and the HPI records similar identifying and address details as well as field of practice or services provided. Health information is not recorded in a HI or by the HI Service.

The identifiers can only be used for health care and related management purposes. However, a person is not required to obtain or use a HI to obtain health care or claim a Medicare benefit. Penalties apply to the unauthorised use or disclosure of HI information; and for a breach of record-keeping obligations imposed by HI Act and regulations under the Act.[122]

Interaction of the HI Service and MHR system

A HI both enables and is essential for registration and participation in the MHR system.

At a functional level, HIs also underpin the key procedures and safeguards in the MHR system. For example, a healthcare provider organisation that is accessing a healthcare recipient's MHR to view or upload a record will use both the consumer's IHI and a provider HPI-I or HPI-O. The logon and transaction details are recorded electronically, providing an audit log that is an essential source for monitoring the security and integrity of the MHR system.

Equally, HIs can be a reference point to support additional (and future) uses of MHR health data in analysing the quality, effectiveness, safety and cost efficiency of healthcare services.

The close connection between the HI Act and the MHR Act is clear from numerous cross-references in each Act to the other Act.

Examples from the HI Act include:

- The Service Operator for the HI Service can collect, use and disclose an IHI for the purposes of the MHR system.[123]
- The System Operator for the MHR system can use an IHI as the identifier for the purposes of the MHR system.[124]
- A healthcare provider can use an IHI for the purpose of communicating or managing information as part of providing health care to a healthcare recipient.[125]

Examples from the MHR Act include:

- Records of certain kinds can only be uploaded to the MHR system if prepared by a person who has professional recognition of a particular kind under the HI Act.[126]
- To be eligible to be registered in the MHR system, an individual must have been assigned an IHI.[127]

---

[120] HI Act s 9A.
[121] Services Australia, *Healthcare Identifiers Service annual report 2019–20* (2020).
[122] HI Act ss 25E, 26; Healthcare Identifiers Regulations 2020 (Cth) reg 12.
[123] HI Act s 15.
[124] HI Act s 17, item 2.
[125] HI Act s 14, item 5(a).
[126] MHR Act s 45.
[127] MHR Act s 40(a), Sch 1, cl 4(a).

- To be eligible to be registered as a participant in the MHR system, an organisation must have been assigned an HPI-O.[128]
- A person cannot be an authorised representative of a healthcare recipient unless the person has an IHI.[129]
- A nominated representative of a healthcare recipient cannot set access controls in relation to the recipient's MHR unless the representative has an IHI.[130]

Important textual similarities between the HI Act and the MHR Act should be borne in mind in any change (or recommendation for change) to either Act. Two specific examples are that there is a similar prohibited purposes stipulation in both Acts;[131] and the HI Service and the MHR system are both subject to privacy oversight by the Australian Information Commissioner.[132]

Review of the HI Act

An independent review of the HI Act and the HI Service was undertaken in 2018, as required by the HI Act (HI Review).[133] There has not yet been a government response to the report of the HI Review, the *Healthcare Identifiers Act and Service Review: final report*.[134]

The MHR Act was excluded from the scope of the HI Review, although the interaction of both Acts was a prominent theme. The HI Review report commented that the effectiveness of the HI Service is measured by the extent to which it supports services such as MHR and secure message delivery.[135]

The broad findings of the HI Review that are relevant to the MHR Act and system were as follows:

- The HI Service is achieving its core objective of delivering a unique identification service for healthcare recipients and providers. The HI Act provides appropriate support for that HI Service objective. Technical and service delivery objectives are being met.
- MHR has been the primary driver for the use of the HI Service by healthcare organisations. The HI Act provides adequate support to the MHR system at present.
- Healthcare provider identifiers (HPI-Is and HPI-Os) are not adopted consistently across all provider types. There has been low take-up of those identifiers by specialists and in community and allied health. This shows up in low participation by those provider groups in the MHR system. To the extent that healthcare providers choose to use HIs other than the HPIs for specific purposes, this can detract from the objective of the HI Service of being a single source of validated HIs for all healthcare providers.
- The 2018 HI Review recommended that a few changes to the HI Act could be considered to better support current MHR activity as well as to enable future MHR developments:
    - Express authority could be conferred on the HI Service Operator to collect information directly from an individual for the purposes of assigning an IHI; and the prohibited purposes stipulations in the HI Act and the MHR Act should be aligned following the 2018 amendments to the MHR Act.

---

[128] MHR Act s 43(a).
[129] MHR Act s 6(6).
[130] MHR Act s 7(3).
[131] See HI Act s 14(2).
[132] HI Act ss 29, 30.
[133] HI Act s 35.
[134] J Kelly, *Healthcare Identifiers Act and Service Review: final report* (Department of Health, November 2018).
[135] Ibid para 1.3.

- Some HI Act features do not gel with other health system practices – for example, an IHI is retired 90 days after fact of death data is received by the Service Operator; and annual renewal of an HPI-I is required by a healthcare provider who is not registered with one of the AHPRA boards.
- More generally, IHIs are strictly regulated by the HI Act in line with an earlier expectation that they would include health information. The regulatory requirements can be an impediment to broader use of IHIs, including by states and territories. IHIs do not include health information and a more flexible regulatory model could now be considered for the HI Act.

- The 2018 HI Review thought that, at that time, HIs were not being fully leveraged in a way that would achieve the full range of benefits contemplated by the HI Act. For example:
  - The HI Review said there could be increased use of HIs to develop existing digital activities such as secure messaging between healthcare providers, e-prescribing through the transfer of prescription information between prescribers and community pharmacies, and e-referrals through the transmission of health information between healthcare providers.

    (That trend has in fact commenced since the HI Review reported. For example, as part of the Commonwealth Government's COVID-19 response, HIs have been used in e-prescribing, e-referrals, e-requests and e-results in pathology and diagnostic imaging.)
  - The HI Review observed that HIs were not being used as the primary identifier in the broader public health system in Australia. An example is that some states and territories have been developing a local and standalone system of patient health identifiers. Contributory factors to why Commonwealth HIs are not being used more expansively included technical/system incompatibility issues, legal constraints in the HI Act on more flexible use of HIs, and lack of strategic initiative at the Commonwealth level.
  - The HI Review found there was no strategic questioning about whether future patient use of HIs would be supported – such as individual consumer use of an IHI to integrate health information stored on different digital platforms with a personal item such as a wearable device or a mobile phone app.
  - The HI Review noted that other potential secondary uses of IHIs that could be considered include tracking hospital readmissions, evaluating the effectiveness of health treatment outcomes and inter-agency case management.
- The HI Review recommended that planning for new and updated national public digital health and information initiatives should consider in the policy development phase how the HI Service could support the program. The HI Review envisaged that this could expand the use that is made of HIs, consistently with the terms of the HI Act, and ensure that Australia's healthcare system is making steps towards national interoperability on key fronts.
- To address those and other findings in its report, the HI Review recommended that the Australian Digital Health Agency (the Agency) develop a HI Service strategy and roadmap. The HI Review thought this to be necessary, as there is minimal active planning at present on how the HI Service could be used to progress other digital health programs. The strategy planning could also consider whether the business architecture of the HI Service is fit for other purposes.

Commentary on interaction between the HI and MHR Acts and systems

The preceding discussion has pointed to changes that could be made to the MHR Act and the HI Act to address integration and alignment issues between both Acts and systems. A few submissions to this review also addressed this theme.

The changes that could be considered are of 2 types:

- specific amendment of existing provisions of either Act
- restructure of either Act to facilitate expansion of the HI Service or MHR system in line with national digital health strategies.

Amendment of the HI Act is not strictly within the scope of this review of the MHR Act. Some proposed changes will nevertheless be noted, as the rationale for the proposal is to improve MHR processes.

Proposed changes to current provisions of the MHR Act or the HI Act

- ***HI Review proposals:*** The HI Review made 2 specific proposals for amendment of the HI Act that are relevant to the MHR system.

  The first recommendation was that s 12 of the HI Act be amended to enable the Service Operator to collect information directly from an individual for the purposes of assigning an IHI.[136] This recommendation was based on the understanding that direct collection was necessary, but not currently possible, if the person to be assigned an IHI was not eligible for Medicare enrolment. This matter has been considered internally within government, and the current view is that direct collection is possible under s 12 as currently worded. Accordingly, no recommendation on this issue is made in this report.

  The second recommendation was that s 14(2) of the HI Act be reviewed to ensure it is aligned with the provisions of the MHR Act relating to prohibited purposes.

  As discussed in Chapter 8 of this report, the MHR Act provisions on prohibited purposes were inserted into that Act in 2018, modelled on s 14(2) of the HI Act. This report recommends that the provisions inserted in 2018 be revised – see Recommendation 18. Section 14(2) of the HI Act could be amended to harmonise with any such change to the MHR Act: see Recommendation 12.

- ***Seed and Network HPI-Os:*** A healthcare provider organisation, in registering with the HI Service, can choose to adopt a single Seed HPI-O structure (commonly used for a small medical practice) or a combined Seed and Network HPI-O structure (more suited to a hospital with multiple departments).[137] An organisation that is on a healthcare recipient's access list is further required to set access flags that will determine which associated healthcare organisations are added to the healthcare recipient's access list.[138]

  Those arrangements are designed to provide helpful granularity in the HPI-O structure, in the access history and in privacy controls. However, that intention can be undermined if a large organisation adopts a single (Seed) HPI-O structure or if separate organisations that have grouped together for IT efficiency are covered by a single HPI-O. The audit log will record access to a person's MHR at the HPI-O level, making it difficult to identify the organisation within the group that accessed the record. This runs counter to consumer expectations of transparency in the access history.

  This problem could be addressed at either a legislative level (for example, redefining the use of HPI-O structures) or an administrative compliance level (encouraging organisations to adopt HPI-O structures that align with MHR and digital health system principles).

---

[136] Ibid, recommendation 6a, p 54.
[137] HI Act s 9A.
[138] MHR Rule 2016 rr 9, 10.

Recommendation 13 proposes that the Department of Health consider these options, in consultation with the Agency (as MHR System Operator) and Services Australia (as HI Service Operator).

- ***Exemption from including HPI-I in uploaded clinical documents:*** The Agency can grant an exemption from the requirement that an HPI-I be included in a clinical document that is uploaded to MHR.[139] The exemption can be of practical benefit for a healthcare provider organisation by relieving it of the task of collecting and using HPI-Is in uploaded documents. On the other hand, the exemptions run counter to transparency in the MHR system.

  Recommendation 14 proposes that the Department of Health review the pattern of exemptions, in consultation with the Agency, to decide if criteria for granting exemptions should be more strictly applied.

- ***Uploading HI-authored records:*** The submission from MIGA[140] drew attention to a provision of the MHR Act that is linked to the HI Act in a way that makes compliance difficult.

  Section 45 of the MHR Act provides that a condition of registration for a healthcare provider organisation is that it will not upload to a repository a record of a specified kind unless the record: (a) has been prepared by an individual healthcare provider to whom a HI has been assigned under the HI Act; and (b) the provider's professional association membership is not conditional, suspended, cancelled or lapsed.[141]

  The MIGA submission makes the point that it is unreasonable to expect that a healthcare provider will know if those requirements are met when the record was prepared externally – for example, a report prepared by a specialist that is being uploaded by a general practitioner.

  Recommendation 15 endorses the MIGA suggestion that s 45 of the MHR Act be amended to provide that it is a condition of registration that a healthcare provider does not knowingly upload a record that fails to meet those requirements.

Restructuring the HI Service in line with digital health strategies

The Agency submission[142] echoed some of the findings of the HI Review report in expressing the following views:

- Further steps are needed to encourage and improve adoption of HIs by public and private healthcare provider organisations around Australia.
- Consideration should be given to easing the restrictions that the HI Act applies to HIs, given that they do not include health information. Reliance could instead be placed on the *Privacy Act 1988* (Cth) to ensure that HI personal information is properly managed. Notably, Australian Privacy Principle 9 deals with the adoption, use and disclosure of government-related identifiers. This change could improve adoption of HIs.
- The recommendations of the HI Review, particularly those relating to broader adoption and integration of HIs, are of critical importance in assessing whether the objects of the MHR system are enabled by the MHR Act.
- The present structure of the HI Act is that entities specified in the Act are authorised to collect, use and disclose information acquired under the Act.[143] This is prescriptive and does not support other types of information flows that may be proposed or designed in a digital health system. An alternative approach is to adopt principles-based authorisations (the Agency's view on this matter is also noted in Chapter 12).

---

[139] Submission No 41 (RACGP) commented on this issue.
[140] Submission No 29 (MIGA).
[141] See MHR Act s 45(b)(ii). The records to which this condition applies are specified in the MHR Rule 2016 r 19 (specifically, any record other than a shared health summary or advance care planning information).
[142] Submission No 28 (Agency) p 9.
[143] HI Act Pt 3.

The proposals for amendment of the HI Act are more appropriately dealt with in the context of government consideration of the HI Review report. However, many of the issues raised in the HI Review report and alluded to by the Agency overlap with those noted in Chapter 3 of this report as appropriate topics for an Agency roadmap or strategic plan to cover future planning directions for MHR. This process would dovetail with the recommendation in the HI Review report for the Agency to prepare a HI Service strategy and roadmap.[144]

Recommendations

Recommendation 12

The Department of Health consider the desirability of amending the *Healthcare Identifiers Act 2010* (Cth) s 14(2) to take account of any changes that may be made to the provisions of the MHR Act relating to prohibited purposes, in response to Recommendation 18 in this report.

Recommendation 13

The Department of Health consult with the Australian Digital Health Agency (as System Operator for the MHR system) and Services Australia (as Service Operator for the Healthcare Identifiers Service) regarding the use of Healthcare Provider Organisation Identifier structures by healthcare provider organisations in a way that runs counter to the objective of transparency in revealing access events in the MHR system. The purpose of the consultation should be to resolve the question of whether there is a problem that should be addressed either by administrative compliance action by the System Operator and the Service Operator or by amendment of the MHR Act or *My Health Records Rule 2016*.

Recommendation 14

The Department of Health, in consultation with the Australian Digital Health Agency, review the pattern of decisions by the System Operator granting exemptions from the requirement to include an Individual Healthcare Provider Identifier in a clinical document that is uploaded to the MHR system. The purpose of the consultation should be to decide if the criteria for granting an exemption should be more strictly applied.

Recommendation 15

The MHR Act s 45 be amended to provide that it is a condition of registration for a healthcare provider organisation that it will not *knowingly* upload to a repository a record that was prepared by an individual healthcare provider who did not meet the requirements specified in s 45.

[144] J Kelly, *Healthcare Identifiers Act and Service Review: final report* (Department of Health, November 2018) recommendation 1, p 51.

Chapter 7. Healthcare recipient controls in My Health Record

Explanation of the MHR system consumer controls

Consumer control is a foundation principle of the MHR system, as reflected in a few key elements:

- ***The title:*** MHR, which builds on the earlier title of Personally Controlled Electronic Health Record.
- ***Voluntary participation in MHR:*** Following the end of the opt-out period on 31 January 2019, a healthcare recipient must apply to be registered in MHR;[145] a healthcare recipient can decide at any time to cancel or suspend their registration in MHR.[146]
- ***Control of health information included in MHR:*** A healthcare recipient may advise a registered healthcare provider organisation that it is not to upload to MHR any health information records specified by the recipient.[147] The default position that otherwise applies is that an organisation can upload the recipient's health information. A healthcare recipient can remove a record that has been uploaded.[148]
- ***Control over who has access to health information:*** A healthcare recipient can set access controls that prevent registered healthcare provider organisations from viewing or having access to the recipient's health information, either generally or subject to limitations.[149] This includes concealing a health record so that its inclusion in the recipient's MHR is not known to others.[150] The default position that otherwise applies is that an organisation, in accordance with the MHR Rule 2016, can access, use and disclose the recipient's health information for the purpose of providing health care to the recipient.[151]
- ***Penalties for contravening a recipient's directions:*** The MHR Act contains criminal and civil penalties for the unauthorised collection, use and disclosure of health information in a healthcare recipient's MHR.[152]

The principle of consumer control differentiates MHR from other health record systems that are structured on a principle of practitioner or organisational control. In those systems the consumer may have no independent right of entry to the system, no control over what personal health information is uploaded to the system, and no access to personal information in the system other than through privacy legislation. That is the operating model, for example, of public sector health record systems established by state and territory governments and instrumentalities.

There appears to be general acceptance, both in the health sector and in the broader community, that consumer control should remain the foundation principle of the MHR system. That principle was and continues to be firmly emphasised to people who are deciding whether to join or remain in MHR.[153]

---

[145] MHR Act Sch 1 cl 6; see also s 39.
[146] MHR Act s 51(1).
[147] MHR Act Sch 1 cl 9; see also s 41(3). A healthcare recipient may similarly advise the System Operator that Medicare health information relating to the recipient is not to be uploaded to MHR: Sch 1 cl 13.
[148] MHR Act s 15(b)(ii); MHR Rule 2016 r 5(e).
[149] MHR Act s 15(b), (c); MHR Rule 2016 r 6(1), (2).
[150] MHR Act s 15(b)(i); MHR Rule 2016 r 5(e).
[151] MHR Act s 61(1); MHR Rule 2016 r 5(a).
[152] MHR Act s 59.
[153] Eg see the landing page of www.myhealthrecord.gov.au – 'Access to Your Record is in Your Control. Find Out How'.

Consumer control also aligns with a central privacy tenet that people should have the right to control when and how their personal information is shared with others. In the health sphere in particular there will be many reasons why individuals do not want sensitive information about their health diagnoses, tests, reports and queries to be known to others.

Those considerations mean that individuals should retain control over whether personal health information can be uploaded to MHR and over third-party access to information that has been uploaded. Statutory exceptions to a person's control over their own health record should be eminently justifiable and carefully framed.

Questions have nevertheless been raised about whether some adjustments could be made so that there is less rigidity in the way the MHR system functions. It is suggested that this would have practical benefit for healthcare recipients and make healthcare providers more inclined to use MHR. Three suggestions are considered below:

- revising the 'hidden/removed documents' feature of MHR
- revising the criteria for emergency record access and the reporting and auditing obligations that attach to it
- allowing general MHR system access by hospital emergency departments.

Hidden/removed documents in MHR

A function of the System Operator under the MHR Act is to establish and maintain access controls that enable a healthcare recipient to control access to their MHR.[154] This function is reiterated in the MHR Rule 2016, which provides that the System Operator must establish 'Default access controls' and 'Advanced access controls'.[155]

Three examples of default access controls listed in the MHR Rule 2016 are:

- All registered healthcare provider organisations that are on an access list of organisations involved in the care of a healthcare recipient are permitted to access that person's MHR.
- A healthcare recipient may remove records from their MHR.
- A healthcare recipient may authorise the System Operator to restore a record that has been removed.[156]

Two examples of advanced access controls listed in the MHR Rule 2016 are:

- A healthcare recipient may control access to their MHR by preventing a registered healthcare organisation from accessing the recipient's MHR, or documents in the MHR, unless the organisation is on a recipient's access list or has been given a record or document access code.
- A healthcare recipient may be alerted electronically when their MHR is accessed by a third party.[157]

A low number of healthcare recipients have imposed advanced access controls – fewer than 40,000, or 0.2%, of the 22 million record holders.[158] Just under 90% of those record holders imposed a Record Access Code control and the remainder a Limited Document Access Code control.

---

[154] MHR Act ss 15(b), (c), 109(6).
[155] MHR Rule 2016 rr 5, 6.
[156] MHR Rule 2016 r 5(a), (b), (e).
[157] MHR Rule 2016 r 6(1).
[158] Australian Digital Health Agency, My Health Record, 'My Health Record Statistics' (October 2020) https://www.myhealthrecord.gov.au/statistics (statistics for September 2020).

The MHR website explains the advanced access controls set by the System Operator as follows:[159]

> ***Document access settings***
> *There are four document settings you can apply to your documents:*
> - ***General Access:*** *Allows healthcare providers and your representatives to view a document.*
> - ***Restricted:*** *Only your healthcare providers and your representatives with 'Restricted Access' can view the document.*
> - ***Hidden:*** *You, your healthcare providers and your representatives cannot view this document in your MHR. To view this document, you or your representatives need to reinstate the document.*
> - ***Removed:*** *You, your healthcare providers and your representatives cannot view this document in your record including in a medical emergency.*[160]

Those access levels are consistent with the MHR Act and the MHR Rule 2016, although there is a confusing inconsistency between the descriptions used on the MHR website and in the legislation. The MHR Rule 2016 uses the terms 'restricted' and 'removed' but not the term 'hidden'. The MHR Rule 2016 also anticipates that a record that has 'been effectively removed' can be restored.[161] There is uneven advice on 2 adjacent pages of the website as to the effect of document removal: one page advises that removing a document means 'only you and the person who added it to your MHR can see it' and the other page advises that removing a document means 'it cannot be viewed by anybody, even in an emergency'.[162]

Putting those discrepancies to one side, an issue on which there are differing views is the ability of a healthcare recipient to hide or conceal a document in the MHR system. The document will not be known to healthcare professionals, even through use of the emergency access function.[163] An adjustment was made to that practice[164] following a review of the MHR system in 2013[165] so that the author of a document that has been uploaded to a person's MHR can see that the document has been removed from view.

Several criticisms are made of hidden/concealed documents. The first is that the practice is unnecessary, as healthcare recipients already have the option to restrict access to specified documents or document categories. [166] Access by a third party will then be possible only if they are on the recipient's access list or have been given the recipient's record or document code.

---

[159] Australian Digital Health Agency, My Health Record, 'Move, Restrict or Hide Information' https://www.myhealthrecord.gov.au/help/remove-restrict-hide.
[160] The website page accessed through a person's MHR account on myGov explains, as to a document that has been removed, that 'You or your representatives cannot reinstate the document'.
[161] MH Rule 2016 r 5(e).
[162] Australian Digital Health Agency, My Health Record, 'Control Access to your Record' https://www.myhealthrecord.gov.au/for-you-your-family/howtos/control-access-your-record; Australian Digital Health Agency, My Health Record, 'Control Access to Documents' https://www.myhealthrecord.gov.au/for-you-your-family/howtos/control-document-access.
[163] MHR Rule 2016 r 7(2)(c).
[164] As advised in submission No 28 (Agency) p 7.
[165] *Review of the Personally Controlled Electronic Health Record* (2013), Recommendation 27.
[166] Criticisms were raised in consultations for this inquiry and in some submissions – eg submission Nos 19 (Defence), 29 (MIGA), 35 (Avant), 37 (Pharm Guild).

A second criticism is that a healthcare provider will not know if a document has been concealed and must assume that possibility in accessing a patient's MHR. This may undermine practitioner confidence in the reliability of MHR and encourage scepticism. This runs counter to the objectives of the MHR system, which envisage it playing a dependable and dynamic role in health care. A patient may not fully understand what information will be relevant to a healthcare consultation. As one submission commented, 'There is an important distinction for the health profession between assuming that a MHR will be by its nature incomplete, and knowing that a patient has chosen to make certain aspects of their clinical history incomplete'.[167]

A third criticism is that the hidden category could be modified by marking in a person's MHR that a document has been concealed, without identifying its contents. A practitioner would then be on notice that the visible record is not complete, and they could have a conversation with the patient of a kind that health professionals are well versed in having.

A variation of that criticism is that specified kinds of information should be marked if hidden. The Advance Care Planning Australia (ACPA) submission[168] to this review argued that advance care planning information should not be hidden – if it is, it should at least be marked. An individual's healthcare team would then be on notice that the individual had taken the important step either of personally uploading this information or (as required by the MHR Rule 2016) of instructing a healthcare provider organisation to upload it.[169] This would make it more likely that the information could be used as intended.

Another example given was that information about opioids/narcotics is important medical/pharmaceutical information that should at least be flagged if hidden.[170]

The contrasting view is that the hidden category of documents should be retained as an MHR feature without alteration. The feature is well established and is integral to the central MHR principle of consumer control. The ability to remove documents from view underpins community confidence that the MHR system safeguards personal privacy and encourages participants to play an active role in their own health management. A benefit to consumers is that they have a secure, permanent and accessible place to keep personal health information which they control.

An allied comment is that MHR can only ever be regarded as a supplementary resource for healthcare providers. A patient's MHR may not be a complete health record, not least because other healthcare providers may not have uploaded relevant health information. A standard feature of healthcare practice is that patient interactions must be approached afresh and with a questioning and open mind to elicit relevant information.

The response to the suggestion that hidden documents be marked is that when a healthcare recipient is in a healthcare consultation they could be in the invidious position of having to discuss their choice to conceal health information from healthcare providers. This may discourage a healthcare recipient from consenting to health information being uploaded and influence them to choose another option to store or access private health information in the future.

---

[167] Submission No 29 (MIGA).
[168] Submission No 16 (ACPA).
[169] MHR Rule 2016 r 32A.
[170] Eg submission Nos 19 (Defence), 37 (Pharm Guild).

On balance, this report does not recommend any change to the current document access settings. While it is understandable that the 'hidden' access setting is a source of concern to health providers who are encouraged to rely on MHR as a valuable and reliable source of patient health information, the retention of the current arrangement has been broadly endorsed – including in submissions to this inquiry by the Australian Digital Health Agency (the Agency), the Office of the Australian Information Commissioner (OAIC), Pharmaceutical Society of Australia, Australian Medical Association (AMA), Royal Australian College of General Practitioners (RACGP) and Telstra Health.[171]

It is significant that only a small number of MHR record holders have set an access control (0.2 per cent), and the number of hidden/removed documents may be much smaller. A few submissions noted that this low figure points to the need for better education and understanding among healthcare recipients and professionals about competing use objectives – that consumer control is a fundamental feature of the MHR system, yet healthcare recipients should be encouraged to make their MHR a complete health record.

The Agency submission commented that its own user testing indicates that the access controls are difficult to understand and use.[172] The Agency will explore opportunities to improve that feature.

Emergency record access to MHR health information

If a healthcare recipient has not imposed any access controls, the default position of 'general access' applies and a registered healthcare provider organisation can access and use health information in a person's MHR for the purpose of providing health care to them.[173] If an access control is in place, the standard access condition is that the healthcare provider organisation must be on the recipient's access list or have been given the recipient's Record Access Code or Limited Document Access Code.

There is an important override exception, described in the MHR Act as 'serious threat' and popularly known as 'emergency record access' or the 'breakglass' feature.[174] A participant in the MHR system (such as a registered healthcare provider organisation) may collect, use and disclose health information in a healthcare recipient's MHR (except healthcare recipient only notes[175] and documents that have been removed[176]) if the participant reasonably believes that MHR access is necessary to lessen or prevent a serious threat to:

- an individual's life, health or safety[177]
- public health or safety.[178]

Three conditions apply if that exceptional override power is used to access a person's MHR to prevent a threat to an individual's life, health or safety:[179]

- The participant must be reasonably satisfied that it is unreasonable or impracticable to obtain the healthcare recipient's consent to the collection, use or disclosure.

---

[171] Submission Nos 28 (Agency), 36 (OAIC), 27 (PSA), 40 (AMA), 41 (RACGP), 25 (Telstra Health). The AMA noted that it was open to discussion on options for marking that an MHR contains hidden or removed documents.
[172] Submission No 28 (Agency) p 8.
[173] MHR Act s 61(1); MHR Rule 2016 r 5(a).
[174] Eg Australian Commission on Safety and Quality in Health Care, *Emergency department clinicians' guide to My Health Record* (November 2019) p 9.
[175] MHR Act s 64(3).
[176] MHR Rule 2016 r 7(1)(c).
[177] MHR Act s 64(1); MHR Rule 2016 r 7.
[178] MHR Act s 64(2); MHR Rule 2016 r 8.
[179] MHR Act s 64(1).

- The participant must advise the System Operator of the basis for being reasonably satisfied that emergency access was necessary and consent could not be obtained.
- The collection, use or disclosure must occur within 5 days of that advice being given to the System Operator.

The emergency record access power was discussed in an Australian National Audit Office (ANAO) report in 2019 that examined the control and monitoring of privacy risks in the MHR system.[180] The report made the following findings:

- Use of the emergency record access power had risen from 80 instances in July 2018 to 205 instances in March 2019.
- In only 8.2% of emergency access instances over the period of the audit was an advanced access control in place.
- The System Operator had procedures in place to monitor use of the power by requesting a written explanation from a healthcare provider organisation for each use of the power and then analysing the provider response.
- The System Operator had not received a response from an organisation in a number of instances and could not therefore be satisfied if an interference with privacy had occurred.
- Some provider responses indicated a potential contravention of the MHR Act, although no data breach notification had been made under s 75 of the MHR Act to the OAIC by either the System Operator or the provider organisation.[181]

The ANAO report recommended that the Agency and the Department of Health, in consultation with the OAIC, review the adequacy of the procedures in place for monitoring use of the emergency record access power and notifying contraventions of the MHR Act to the OAIC.[182] The recommendation was accepted by the Agency and the department. In February 2020 the Agency published an Implementation Plan for the ANAO recommendations. This included development of a regulatory compliance framework to ensure proper understanding and monitoring of the statutory requirements attaching to the emergency record access power.[183]

This review was shown an advanced draft of a proposed new emergency access compliance guideline being developed by the Agency. Subject to internal approvals, the guideline may be published late 2020 or early 2021. There is a brief mention below of the role that such a guideline could play.

It was apparent during the consultations for this review that there is a level of frustration among healthcare providers regarding the process to be followed in using the emergency record access power. The concerns mostly relate to the use of the power in hospital emergency departments and to lessen threats to an individual's life or health, rather than to protect public health or safety.

A clinician will first have to ascertain if there is an advanced access control in place or if, instead, default general access can be used to view all available MHR patient health information. The MHR website advises that a provider will be prompted by their clinical software if a Record Access Code or Limited Document Access Code is required.[184] The patient can be asked to provide the code – but they may not remember it or may lack cognition or judgement at the time.

---

[180] Australian National Audit Office (ANAO), *Implementation of the My Health Record system* (Report No 13, 2019–20) paras 3.42–47.
[181] The MHR Act s 75(1)(b)(i) requires notification when a person 'has, or may have, contravened this Act in a manner involving an unauthorised collection, use or disclosure of health information in a healthcare recipient's MHR'.
[182] ANAO, above n 180, Recommendation 2.
[183] Australian Digital Health Agency, *Implementation plan – ANAO performance audit of the MHR* (February 2020).
[184] Australian Digital Health Agency, My Health Record, 'Emergency Access' www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/emergency-access.

The clinician is not likely to know whether any restricted documents in fact exist within the record or if there is relevant health information that can be accessed with the code.

The figures in the ANAO report bear out that uncertainty. In over 90% of cases there was no advanced access control in place to warrant the use of the emergency record access power. Use of the power would not have yielded additional health information. This suggests that the power was used either in a setting of uncertainty or on the mistaken assumption that it was a power to be used by emergency department staff.

Difficulties of that kind may be resolved if the Agency were to develop a compliance guideline in response to the ANAO report. The guideline may facilitate a better understanding of when the emergency record access power can be used and the obligation on healthcare provider organisations to monitor use of the power and report to the System Operator.

A larger issue, falling beyond the scope of a compliance guideline, is whether the current legislative settings in the MHR for emergency access are appropriate.

The view on one side, put in the OAIC submission,[185] is that the current emergency access provisions are an important MHR system feature that appropriately balances privacy and clinical needs. They enable access to potentially life-saving information but, equally, recognise that individual consumer consent should ordinarily be obtained before personal access controls are overridden.

The opposing view is that the present settings are not aligned to the realities of emergency medical decision making, which can be hurried and pressured, but are shaped by the professional ethical obligations of the healthcare provider. An unnecessary or inadvertent use of emergency access can constitute an unauthorised collection or use of MHR health information that triggers the data breach notification procedure in the MHR Act and exposes a healthcare provider to a penalty under the Act. The auditing process applying to any use of the power may also engage a healthcare provider in an extended process of explanation and justification. Those considerations may discourage a clinician from using the emergency record access power in circumstances where it would be beneficial to do so.

Following are the main options for legislative change that have been raised with this review:

- ***Lower the threshold for emergency access:*** There are 5 elements of the emergency record access power that together set a high threshold for using it: a provider must be (1) 'reasonably satisfied' that it is (2) 'necessary' to access a person's MHR to (3) 'lessen or prevent' a (4) 'serious threat' to an individual's (5) 'life, health or safety'.

  The second of those elements presents an obvious difficulty. How can a provider be reasonably satisfied that it is 'necessary' to access a person's MHR when the contents of the record are not known? Similarly, it may be more in the realm of speculation than reasonable satisfaction that accessing a person's MHR will 'lessen or prevent' a serious threat that currently exists to their health.[186]

  It is questionable whether those threshold requirements are stricter than required by the underlying MHR principle of consumer control. An alternative approach would be a lower access threshold but tighter control on the use that can be made of any health information in a person's record.

  For example, the access requirement could be reframed to allow access if a healthcare provider is reasonably satisfied that by gaining access they will be better able to deal with a threat to a person's life, health or safety. The provider would be required to report to the System Operator on the steps subsequently taken to ensure that health information from the record was not used or accessed by others beyond that immediate use.

---

[185] Submission No 36 (OAIC) p 6.
[186] Eg submission No 37 (Pharm Guild).

Another suggested variation, in the ACPA submission,[187] is that a clinician should be authorised to override a healthcare recipient's access controls to obtain advance care planning information that is not otherwise available. This would benefit the person by ensuring that their advance care preferences and values are respected.

- ***Simplify the reporting/auditing requirements:*** A healthcare provider organisation is presently required to notify the System Operator on each occasion that the emergency record access power is used.[188]

  There is scope within that requirement to adjust the level of detail and rigour required in a report to the System Operator. The statutory objective of ensuring that use of the power is recorded, monitored and assessed against the statutory requirements can be met without imposing onerous reporting obligations on healthcare provider organisations. The compliance guideline being developed by the Agency will deal with this issue.

  An alternative is to amend the MHR Act to impose a modified reporting requirement. A customary approach is to require that a report to the regulator is provided on a monthly or sampling basis.

- ***Alter the access control code display:*** The Agency submission advises that, regardless of whether a patient has applied an advanced access code, the clinical software for MHR entry displays emergency access functionality and the Record Access Code and Limited Document Access Code field. This is done to comply with the MHR Rule 2016.[189]

  This display is a frequent cause of inadvertent use of emergency access by clinicians.[190]

  Removing this requirement from the MHR Rule 2016 when an individual has not in fact applied a code would be likely to cause a substantial reduction in noncompliant use of emergency access. In turn this would cause a commensurate reduction in notifications of emergency access and compliance investigations by the System Operator.

- ***Decouple emergency access from data breach notification:*** The data breach notification requirement in the MHR Act is discussed in Chapter 5 of this report.

  An entity (such as a registered healthcare provider organisation) is required to notify a breach to the System Operator and the OAIC if the entity becomes aware that an unauthorised collection, use or disclosure of health information from a person's MHR has or may have occurred.[191] In effect, as the ANAO report found, a separate data breach notification may have been required on each occasion that a health provider had not properly notified the System Operator that it had used the emergency record access power.

  It is questionable whether there is an additional compliance and privacy protection benefit from notifying noncompliant use of the emergency record access power under the data breach notification requirements. Use of the emergency access function is recorded in the access history of a person's MHR and reported to the System Operator. Since a central purpose of data breach notification is to notify individuals who may be affected, that purpose is already satisfied by other MHR system requirements.

A final point to make is that any reconsideration of the emergency record access power should occur in a broader policy setting that has regard to competing views on the need for and purpose of such a power.

At one end of the spectrum is the view that emergency record access is inconsistent with the underlying principle of consumer control. On this view it should be an option for a consumer to set a privacy access control that cannot be overridden in any circumstance.

---

[187] Submission No 16 (ACPA).
[188] MHR Act s 64(1)(b).
[189] MHR Rule 2016 rr 7, 8.
[190] The same point was made in submission Nos 29 (MIGA), 35 (Avant).
[191] MHR Act s 75(1)(b)(i).

The competing view, at the other end of the spectrum, is that emergency access is an accepted feature of the MHR system. An important MHR objective is to develop a comprehensive personal health information database that can be accessed to provide better quality health care to individuals.

MHR access by hospital emergency departments

A related issue is whether the MHR Act should include a supplementary power that enables hospital emergency departments to access an in-patient's MHR regardless of any advanced access control the patient has imposed.

The argument made in support of such a power is that the emergency setting is a reality, little may be known about the health circumstances of patients arriving unexpectedly, there can be strong pressure on hospital emergency staff to respond quickly, and accessing MHR patient health information may lessen the risk of an incorrect diagnosis or treatment.

There are opposing considerations. The first is the difficulty of framing the criteria for the exercise of such a power. From one hospital to the next it may be difficult to identify what constitutes the 'emergency department'. Also, it is not clear that all individuals seeking emergency department treatment in fact face a health emergency or cannot make an informed choice about their MHR being accessed by the hospital. The wider the scope of any such power the stronger the privacy objection is likely to be.

An option for framing a power of this nature would be to authorise the System Operator to approve an application from an individual hospital for general consent to access patient MHRs in accordance with conditions and reporting obligations set by the System Operator.

No recommendation to that effect is made in this report. However, the matter may warrant further discussion and clarification alongside Recommendation 16.

Recommendations

It is premature to recommend specific changes to the MHR Act while the Agency is developing a new regulatory compliance framework in response to the ANAO recommendation. The Agency's work may lead to a better understanding of the statutory compliance requirements and to a reorganised use of the powers. Accordingly, Recommendation 16 proposes that the Department of Health consider the desirability of legislative reform in the light of the regulatory compliance review that the Agency is currently undertaking.

On the other hand, Recommendation 17 proposes an alteration of the MHR Rule 2016 that could be implemented ahead of the Agency's current review work.

Recommendation 16

The Department of Health consider whether amendment of s 64 of the MHR Act is desirable:

- to specify less demanding criteria for emergency record access
- to remove the requirement that every use of the power be notified individually to the System Operator
- to provide that s 75 of the Act (data breach notification) does not apply to an action taken under s 64.

The review of s 64 by the Department of Health should be undertaken after completion of any action currently being taken by the department and the Australian Digital Health Agency, in consultation with the Office of the Australian Information Commissioner, in response to Recommendation 2 of the report of the Australian National Audit Office, *Implementation of the My Health Record system* (2019).

Recommendation 17

The *My Health Records Rule 2016*, rr 7 and 8, be amended to require that the Record Access Code and Limited Document Access Code are displayed in clinical software only where a healthcare recipient has applied an advanced access code.

Chapter 8. Prohibition on using My Health Record sourced information for insurance and employment purposes

Background to the prohibition introduced in 2018

A central principle of the MHR system is that patient information in a person's MHR is made available to others only for the purposes of providing health care to that person.[192]

A concern raised in 2018 was that the introduction of an MHR opt-out model would lead to more health information being collected about more people, which in turn would arouse external interest in accessing patient health records.[193] Of particular concern was that government, law enforcement agencies, insurers and employers would seek to access this expanded repository of personal health information.

To allay privacy concerns, amendments were made to the MHR Act in 2018 to preclude access of that kind except in limited circumstances.

The changes to restrict access by government and law enforcement agencies appear to have been welcomed and not to have attracted criticism. A new provision was added to the MHR Act providing that health information in a person's MHR must not be disclosed to a government agency except in accordance with the order of a designated judicial officer. The judicial officer cannot issue an order unless satisfied that the agency has coercive information-gathering powers, the agency reasonably requires the information for an authorised agency function, there is no other effective means for the agency to obtain the information, and disclosure to the agency would not unreasonably interfere with the privacy of the healthcare recipient.[194]

On the other hand, there has been criticism of the 2018 changes to the MHR Act that restrict use of MHR patient information in insurance and employment decisions. There are 3 lines of criticism:

- ***Healthcare provider support to patients:*** The 2018 legislative changes are criticised as being unnecessarily broad and imprecise, constraining practitioners in providing effective healthcare assistance to patients and deterring practitioner support for MHR through severe penalties for any breach.
- ***Employment:*** The impact of the legislative changes on some areas of employment (such as the Department of Defence (Defence)) raises special issues that may warrant adjusting the uniform application of the MHR Act provisions.
- ***Insurance:*** The legislative changes create complications for insurers when it becomes known only midway through an insurance transaction that a client or healthcare provider has supplied MHR-sourced health information.

The principal line of criticism relates to the impact of the 2018 changes on healthcare providers. That perspective is adopted in the following analysis of the MHR Act provisions. The special issues relating to employment and insurance are taken up at the end of this section.

---

[192] MHR Act s 4.
[193] Eg Senate Community Affairs References Committee, *My Health Record system* (October 2018) paras 2.71–2.87; Senate Community Affairs Legislation Committee, *My Health Records Amendment (Strengthening Privacy) Bill 2018* (October 2018) Ch 2.
[194] MHR Act ss 69A, 69B. An existing provision in the MHR Act provided for disclosure to the Auditor-General for Australia, Commonwealth Ombudsman and Australian Information Commissioner: MHR Act s 65.

The MHR Act provisions on use/disclosure for a prohibited purpose

It is helpful to begin by explaining the MHR Act provisions on use and disclosure of MHR patient health information that applied prior to the 2018 changes and that continue to apply except as modified in 2018.

The MHR Act makes it an offence for any person to collect health information about a person from their MHR or to use or disclose any such information obtained from the MHR system, except as authorised by the MHR Act.[195]

The authorisation that is principally relevant to registered healthcare provider organisations is that they may collect, use and disclose MHR patient information for the purpose of providing health care to the person and in accordance with access controls either set by the person or applying as default access controls under the MHR Rule 2016.[196]

MHR patient health information that is obtained in accordance with that authorisation is not thereafter subject to the prohibitions in the MHR Act if the same information could be obtained other than by using the MHR system.[197] Similarly, the prohibitions in the Act do not apply to patient health information that is in fact obtained by other means.[198]

The 2018 changes modified that framework by providing that MHR patient information could not be used for a 'prohibited purpose' – namely, to:

- underwrite a contract of insurance for the healthcare recipient
- decide whether to enter a contract of insurance with the healthcare recipient
- decide whether a contract of insurance covers the healthcare recipient in relation to a particular event
- make an employment decision relating to the healthcare recipient.[199]

Use of MHR patient information for one of those prohibited purposes is a criminal offence[200] and can attract a civil penalty imposed by a court in civil proceedings.[201] The current maximum penalties for individuals are, for a criminal offence, 5 years' imprisonment or a fine of $66,600; or a civil penalty of $333,000.[202]

The criminal and civil penalty provisions are expressed to apply broadly: they apply to any person and to the following actions:

- using MHR patient information for a prohibited purpose 'if the person obtained the information by using or gaining access to the MHR system'[203]
- requesting or requiring MHR patient information for the prohibited purpose[204]
- using health information for a prohibited purpose that 'is or was included in a healthcare recipient's MHR'.[205]

---

[195] MHR Act s 59.
[196] MHR Act s 61; MHR Rule 2016, rules 5, 6.
[197] MHR Act s 71(2), (4).
[198] MHR Act s 71(1).
[199] MHR Act ss 70A, 70B.
[200] MHR Act s 71A.
[201] MHR Act ss 59A, 71B.
[202] The maximum penalty amount for a body corporate is 5 times higher: *Crimes Act 1914* (Cth) s 4B(3).
[203] MHR Act s 59A(1) (civil penalty).
[204] MHR Act s 70A(6).
[205] MHR Act s 71A(1) (criminal offence), 71B(1) (civil penalty).

An insurer or employer would commit an offence by requesting a client/employee's MHR record from that client/employee or by using MHR health information provided by a client/employee.

A health practitioner could commit an offence by using MHR patient information in a report to an insurer or employer, regardless of whether that information was obtained directly from the MHR system for that purpose, had earlier been downloaded onto the practitioner's local clinical information system[206] or was supplied directly by the patient.

To commit a criminal offence the health practitioner must know the MHR patient information is being used for a prohibited purpose or be reckless as to that fact.[207] There is no similar limitation in the civil penalty provision, which applies if health information that is or was included in a healthcare recipient's MHR is used for a prohibited purpose.[208]

An element of the 2018 framework that was not changed is that a report by a healthcare provider to an insurer or employer may use health information that was obtained from a source other than the MHR system – for example, from the patient or an alternative health records system.[209] Health information obtained from that other source can be used even if there is duplicate information in the MHR system.

Commentary – general observations

The MHR Act provisions on use and disclosure for a prohibited purpose are not easy to navigate. Three examples will be noted.

First, the 2018 amendments were added alongside the existing provisions on use and disclosure. A consequence is that there are 2 sets of similarly worded and partially overlapping provisions – one set applies generally to use and disclosure of MHR patient information and the other set applies to use and disclosure for a prohibited purpose. Similarly, there are separate (though similarly worded) criminal offence and civil penalty sections in each set of provisions.[210]

Secondly, some key phrases in the legislation may be difficult to apply in practice. As noted above, one category of prohibited purpose is using MHR health information to make an employment decision relating to the healthcare recipient – or, as defined in the legislation, for 'the purpose of … an employer employing, or continuing or ceasing to employ, the healthcare recipient'.[211]

Does that encompass a health or capacity assessment of a person that is prepared by a medical practitioner to assist the person and a current or prospective employer to adapt their abilities to the requirements of a particular role? The assessment could come within the prohibited purposes provisions, for example, if it highlighted the patient's unsuitability for the role and led to a loss of employment. It may therefore be uncertain whether MHR patient information can be used at the time that a healthcare provider is preparing a report for a patient to be given to their employer.

A third example of a difficult constructional issue is a section stating that:

> *[A criminal or civil penalty] does not apply if the information was not collected from, and is not derived from a disclosure that was made by, a person who obtained the information by using or gaining access to the MHR system. For this purpose, it does not matter whether or not any collection or disclosure of the information was authorised under this Act or any other law.*[212]

---

[206] It is noted below (in the text accompanying footnote 212) that ss 71A(2) and 71B(2) are open to a construction that an offence is not committed if MHR health information was obtained from a system rather than a person.
[207] MHR Act s 71A(1)(b).
[208] MHR Act s 71B(1).
[209] MHR Act s 71(1), (3).
[210] Eg compare MHR Act ss 59A and 71B.
[211] MHR Act s 70A(1)(a)(iv).
[212] MHR Act ss 71A(2), 71B(2).

A possible reading of that section is that a penalty may not apply if a healthcare provider obtains MHR patient information from a local clinical information system rather than from or with the assistance of a 'person'. However, that result would appear to run counter to the objective of the prohibited purposes provisions, which is broadly to prevent the use of health information that 'is or was included in a healthcare recipient's MHR'.

Commentary – impact on healthcare providers

Those constructional difficulties lead into the larger issue of whether the prohibited purposes provisions, as presently framed, can have an unreasonable impact on healthcare providers and the healthcare service they provide to patients.

As noted, the provisions can apply not only to the use of health information that was downloaded or requested for a prohibited purpose but also to information that 'is or was included in a healthcare recipient's MHR'. [213] Consequently (and putting to one side the third constructional difficulty explained above[214]), the prohibition can extend to information that was provided by a patient or downloaded by the healthcare provider on an earlier occasion for a different healthcare purpose.

A provider must therefore be alert to the possible source of information that is being used in a report to an insurer/employer. The risk may be greater if the provider has not partitioned or separately tagged MHR patient health information that was separately provided to or downloaded by the provider. Tagging may not in fact be practicable. The view of the Australian Digital Health Agency (the Agency) is that it is not practicable for the Agency to effectively tag information that is downloaded and that a significant investment of resources may be required for a healthcare provider organisation to track the source of health information they hold.[215]

There can be numerous flow-on consequences for a healthcare provider. One is that MHR patient information may be used unwittingly in a report prepared for an insurer/employer. The stiff criminal and civil penalties in the MHR Act may nevertheless apply to the wrongful use of the MHR patient health information.

The safest course for a healthcare provider who has been asked by a patient to assist in preparing a report for an insurer/employer may be to seek a fresh copy of any test/report that is on the clinical file – for example, to ask a pathology provider directly to provide a copy of a pathology report that is on file after having earlier been uploaded to the patient's MHR. Another option is to arrange for a new medical test or diagnosis to be undertaken (and not to upload the report to the patient's MHR). Both options run counter to the objectives of the MHR system, which are to reduce duplication of treatment and fragmentation of health information and to improve coordination among healthcare providers.[216]

Another flow-on consequence is that the healthcare provider may be inhibited in providing an effective healthcare service to a patient. It is not uncommon that a patient will seek the assistance of a provider to prepare a report for an insurer or employer that outlines the patient's medical history – for example, to provide a general health assessment, an accident injury report, a list of pre-existing illnesses, a disability or terminal illness statement, a return to work plan or a certificate of capacity to work.

---

[213] MHR Act ss 71A(1)(d), 71B(1).
[214] See text accompanying footnote 212.
[215] Submission No 28 (Agency) p 8.
[216] MHR Act s 3.

The patient's MHR may be the most reliable or complete record of their medical history, particularly if the patient has consulted numerous healthcare providers over time or in relation to particular medical conditions. The patient may be disadvantaged in relation to the insurer/employer if their full medical record or history cannot be consulted and they cannot provide adequate evidence of, for example, their ability to return to work or their eligibility for an insurance or compensation benefit or special rate. The provider has a professional obligation to act on the best and most reliable health information available.

Another point made in the Agency submission is that these consequences stemming from the 2018 legislative changes run counter to an underpinning principle of the MHR system. The intention was that MHR would not require creation of a separate health information management framework. Health information would continue to be managed in accordance with the requirements of the *Privacy Act 1988* (Cth) on matters such as use and disclosure of personal information and acting in accordance with a record holder's consent or expectations.

Several submissions to the inquiry from professional associations, industry bodies and state authorities acknowledged their support for a prohibited purposes stipulation but in a revised form. Common suggestions were that the prohibition should allow use of MHR health information at the request and consent of a patient, and that unintentional breaches by a healthcare provider should not be penalised.[217]

Recommendations – healthcare providers

In summary, 3 considerations support a revision of the prohibited purposes provisions as they apply to healthcare providers:

- By imposing criminal and civil penalties on the use of health information that 'is or was included' in a person's MHR, the prohibition can be a practical deterrent to a healthcare provider accessing or using a patient's MHR, at least for the purpose of preparing a report that may be acted on by an insurer/employer. The risk to the healthcare provider is amplified by the fact that the prohibition can apply to MHR-sourced health information provided by the patient or earlier downloaded onto a local clinical information system but not earmarked as MHR information.
- To avoid contravening the prohibition, a healthcare provider who is preparing a report to an insurer/employer requested by a patient may need to obtain a second copy of an existing MHR record or arrange for new and duplicate medical tests or diagnoses. This can be inefficient and run counter to the objectives of the MHR system.
- The prohibition has been raised repeatedly as a concern by bodies representing healthcare providers. To what extent the prohibition is a routine practical worry in a clinical setting is speculative and hard to assess empirically. Nevertheless, professional trust and confidence in the MHR system is a vital component of its success. There can be value in removing any actual or perceived obstacle to that support if the removal can be done without any downside.

On the other hand, there is a strong justification for retaining a prohibited purposes stipulation in at least a modified form:

- The transition to the opt-out system in 2018 has made MHR an expanded and richer source of health information about a high proportion of Australians. The prohibited purposes provisions reinforce a central MHR principle that personal health information in the system is to be used to provide health care to individuals.

[217] Submission Nos 29 (MIGA), 34 (Victoria), 35 (Avant), 37 (Pharm Guild), 40 (AMA), 41 (RACGP). Other submissions also supported the need for a prohibition in some form – eg submission Nos 11 (Anon), 30 (APF), 31 (Arnold).

- In the absence of the prohibition, there is a risk that pressure will be placed on individuals (including indirectly through healthcare providers) to make their MHR health information available to an insurer/employer on doubtful grounds. Among the risks are that employers/insurers may use MHR-sourced information in risk profiling,[218] MHR-sourced information provided to an employer/insurer may include unrelated sensitive health information, the information may not be as securely protected as in MHR, and people may be hesitant to upload health information to their MHR.
- The prohibition indirectly discourages medical clinics from adopting a routine or unregulated practice of providing MHR patient information to insurers and employers. Even though disclosure would occur at the request of a patient, the patient may not disclose that pressure was imposed by an insurer/employer to provide MHR information or the elements of 'knowledgeable consent' may be lacking.

A balance could be struck between those competing considerations by excluding 2 areas of conduct from the current prohibited purposes provisions and penalties:

- conduct of a healthcare provider in using MHR patient health information at the request of a patient (or representative) to prepare a report to an insurer/employer if the provider is reasonably satisfied that it is in the patient's interest to do so and that the patient has not been pressured by an insurer/employer to make the request
- conduct of an insurer/employer in using MHR patient health information contained in a report prepared by a healthcare provider that is accompanied by a statement confirming the matters outlined in the previous bullet point.[219]

A prohibited purposes stipulation as modified in that manner would have the following benefits:

- It would enable a healthcare recipient to use their MHR in the same way they can use other personal health information, which includes providing that information to an insurer/employer. A person would have the option of declining consent to their MHR health information being provided to others.
- A healthcare provider who chose to use MHR patient health information at the request of the patient would be obliged to ascertain that the patient's request was independently made and in their best interests.
- An insurer/employer could use MHR health information only if it was provided through a healthcare provider. The prohibited purposes stipulation would otherwise prevent the insurer/employer from requesting that a person provide MHR health information and from using information that was provided directly by a person.

Commentary – distinctive employment settings

The submission from Defence[220] explained that the Joint Health Command, which delivers medical and healthcare services to Australian Defence Force (ADF) personnel, does not interact with MHR because of the prohibited purposes provisions. Consequently, documents such as shared health summaries, event summaries and medicinal dispensing histories are not uploaded to MHR. That information will not therefore be available from MHR to a current or former ADF member or to their private healthcare provider.

---

[218] A constraint in the *Private Health Insurance Act 2007* (Cth) s 55-5 is that a private health insurer must not discriminate against a person on the basis of their health condition.
[219] Submission No 28 (Agency) p 9 briefly canvassed other options for reforming the prohibition, including removing its application to information previously uploaded to MHR, redefining the uses that an employer/insurer can make of MHR information, and broader regulation of employment/insurance use of MHR health information.
[220] Submission No 19 (Defence).

The Defence submission noted also that the prohibition can prevent Defence from accessing MHR health information when assessing a person's fitness to commence military service or to continue service as a Defence Reserves member. Those decisions, Defence notes, 'come with considerable risk to the health of the individual and potentially others'. Use of MHR health information may also relieve an applicant or serving member from having to go through additional assessments and investigations.

Defence proposes that a special exemption be made from the prohibited purposes provisions for Defence-related health care.

The Defence submission raises an important point that warrants closer consideration. It is possible that similar issues arise in other distinctive employment settings. An example is that a healthcare practitioner who is engaged by an employer to provide onsite health services in a remote mining town may be inhibited by the prohibition in either accessing or uploading health information to the employee's MHR. This may also weaken any 3-way conversation that occurs between the employer, the healthcare provider and the employee.

Recommendation 18 (which would allow a healthcare provider or employer to use MHR patient information at the request and consent of the healthcare recipient) would go some way toward addressing the issue that Defence has raised. However, there is a larger issue of whether the MHR Act needs to take special account of distinctive employment settings. The most suitable way of addressing such an issue may be through a rule or regulation made under the MHR Act that would operate as an exception to the prohibited purposes provisions. That would require amendment of the MHR Act.

The issue of distinctive employment settings should be examined further to gauge the dimension of the issue and the options for dealing with it. Recommendation 4 (earlier in this report) proposed that the issue could be examined as part of the roadmap or strategic plan developed by the Agency. An alternative is for the Department of Health to consider the issue, as set out in Recommendation 19 below.

Commentary – insurance transactions

The submission from MLC Life Insurance[221] (MLC) drew attention to some practical issues that the prohibited purposes provisions cause for insurers.

MLC advised that it never requests MHR information from a customer or provider and understands that it cannot be used if it is provided. However, MLC may later become aware that MHR-sourced information was provided. If so, the insurance transaction (such as an application or claim) will have to be stopped and the customer asked to provide relevant health information from another source. MLC comments that this comes at a financial and time cost to the insurer and the customer.

A related problem is that, if a non-disclosure issue arises in relation to a customer's application or claim, the insurer will not be able to rely on MHR health information that a customer had earlier provided even though the insurer did not know the source of that information at the time it was provided. MLC comments that this prevents it from relying on its rights in law for non-disclosure.

The implementation of Recommendation 18 would largely resolve the issue that MLC has raised (depending on the precise terms of any legislative amendment provision). Specifically, that recommendation would allow an insurer to rely on MHR health information included in a report from a healthcare provider if the provider confirmed the information was being given at the request of the patient and with due regard to the patient's best interests.

[221] Submission No 38 (MLC Ltd). See also submission No 12 (Anon).

The recommendation would not alter the present MHR Act setting that an insurer cannot rely on MHR health information given directly by a customer. A practice of that kind, without any intervening moderation by a healthcare provider, would pose a risk of undermining the objective of the prohibited purposes stipulation.

Recommendations

Recommendation 18

The provisions of the MHR Act relating to prohibited purposes be amended to exclude their application to:

- use by a healthcare provider of health information included in a registered healthcare recipient's MHR if the use:
  - is in a report to an insurer or employer relating to the healthcare recipient
  - the report was prepared by the healthcare provider at the request of the recipient (or their representative)
  - the healthcare provider is reasonably satisfied that the use of the health information is in the recipient's best interests and the recipient was not subject to any pressure by the insurer or employer to allow the use of the information
- use by an insurer or employer of health information included in a registered healthcare recipient's MHR if:
  - the information is included in a report prepared by a healthcare provider
  - the healthcare provider has confirmed in writing that he or she is satisfied that use of the health information is in the recipient's best interests and the recipient was not subject to any pressure by the insurer or employer to allow the use of the information.

Recommendation 19

The Department of Health consider the desirability of amending the MHR Act to exempt some employment categories from the scope of the prohibited purposes provisions, such as employment in the Australian Defence Force or Defence Reserves.

Chapter 9. Control of the My Health Record of minors

Explanation of the MHR Act provisions relating to minors

A person aged between 0 and 17 (a minor or child)[222] will commonly have their own MHR:

- This ordinarily occurs as part of Medicare registration for a child who was born in Australia or migrated to Australia.
- A child who does not have an MHR can be registered for an MHR under the MHR Act.[223] The registration application may be lodged by a child aged between 14 and 17 or by the authorised representative of a child aged between 0 and 13.[224] (A child may not have an MHR, for example, because a parent or guardian took opt-out action for the child in the transition period leading up to the opt-out scheme commencing on 1 February 2019.)
- A person's MHR registration can be cancelled.[225] This can be initiated by a child aged between 14 and 17 or by the authorised representative of a child aged between 0 and 13.

Prior to amendments to the MHR Act[226] commencing in December 2018, a single set of rules applied to all minors. Those rules still apply (with a couple of small changes) to minors aged 0–13, but different rules now apply to minors aged 14–17.

Minors aged 0–13

The MHR of a child aged 13 or younger is controlled by their 'authorised representative' – which is any person who satisfies the System Operator (the Australian Digital Health Agency (the Agency)) that they have 'parental responsibility' for the child.[227] More than one person can be an authorised representative.

A person has parental responsibility for a child in one of following 3 situations:

- The person is the child's parent and no order has been made under the *Family Law Act 1975* (Cth) altering their parental responsibility.
- A parenting order has been made under that Act – for example, an order that the child is to live with the person or spend time with the person.
- The person has guardianship or custody of the child under an Australian law.[228]

A person *cannot* be an authorised representative of a child in the following 2 situations:

- A court order requires the person to be supervised when spending time with the child.

The System Operator is satisfied that the life, health or safety of the child or any other person would be at risk if the person was an authorised representative of the child.[229]

---

[222] For a general discussion of the issue of children's privacy see J Gligorijevic, 'Children's Privacy: The Role of Parental Control and Consent' (2019) 19 *Human Rights Law Review* 201–29.
[223] MHR Act Sch 1 cl 6.
[224] This is not expressly stated in the MHR Act but arises by implication – eg from s 6.
[225] MHR Act s 51.
[226] *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth).
[227] MHR Act s 6(1). The *My Health Records (Assisted Registration) Rule 2015* (Cth) r 8 requires a healthcare provider organisation to exercise reasonable care if making a declaration to support a healthcare recipient's assertion of parental responsibility for a child.
[228] MHR Act s 5, definition of 'parental responsibility'.
[229] MHR Act s 6(1A).

If no person meets the 'parental responsibility' test to be an authorised representative of a child, the System Operator may appoint a person who is authorised under Australian law to act on behalf of the child or who is otherwise an 'appropriate person' to be the authorised representative of the child.[230]

A child aged 13 or younger does not have any separate control over their MHR or any separate right to view their record. Those rights are exercisable by the authorised representative.[231]

Prior to the 2018 amendments, when a single set of rules applied to all minors, a child of any age could take control of their MHR by satisfying the System Operator that he or she wanted to manage their own record and was capable of doing so (for example, by providing a statement from a healthcare provider attesting to their maturity).[232] This provision was repealed in December 2018, when different rules were introduced for minors aged 14–17.

Minors aged 14–17

A child aged between 14 and 17 has control over their own MHR. For example, the child can set privacy access controls that regulate which healthcare provider organisations can view either the record or specific documents; or the child can cancel their MHR registration (which results in destruction of their record).

A parent or guardian can access the child's record only if they are an authorised representative or a nominated representative:

By written notice to the System Operator, the child may nominate one or more persons (such as a parent or guardian) to be their authorised representative.[233] Each authorised representative substitutes for the child, who will no longer have access to or control of their own MHR.[234] The authorised representative's access is cancelled when the child turns 18, or before that if the child has cancelled it.[235]

- The child may enter into an agreement with one or more persons (such as a parent, guardian or partner) to be a nominated representative and notify that agreement to the System Operator.[236] Each nominated representative exercises concurrent powers with the child unless the agreement states otherwise.[237] For example, the agreement may state that the representative has 'view only' access to the child's MHR or to particular documents or that the representative cannot cancel the child's MHR registration.

Prior to 2018, a person with parental responsibility for a child aged between 14 and 17 controlled the child's MHR unless the child satisfied the System Operator of their wish and capability to manage their own record.[238]

Authorised and nominated representatives

A representative's duty is to make reasonable efforts to ascertain and give effect to the record holder's will and preferences[239] or, if these cannot be ascertained, to act in a manner that promotes the personal and social wellbeing of the record holder. This obligation applies to both authorised and nominated representatives and whether the record holder is a child or an adult.

---

[230] MHR Act s 6(2).
[231] MHR Act s 6(7).
[232] MHR Act s 6(3) prior to amendment by the *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth).
[233] MHR Act s 6(3).
[234] MHR Act s 6(7).
[235] MHR Rule 2016 r 11(1)(b).
[236] MHR Act s 7(1).
[237] MHR Act s 7(2), (4).
[238] MHR Act s 6(3) prior to amendment by the *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth).
[239] MHR Act s 7A.

Commentary on the MHR Act provisions relating to minors

Several aspects of the suitability of the current rules relating to the MHRs of minors have been questioned. The following analysis should be read in conjunction with the discussion in Chapter 4 of the powers of the System Operator to control a representative's access to a person's MHR and the information that may be required to exercise those powers. The issues noted in that discussion more commonly arise for representatives for minors than for other record holders.

Minors aged 0–13

There has been no change to the principal rule that a parent or guardian who satisfies the System Operator that they have parental responsibility for a child aged between 0 and 13 will be an authorised representative of that child. There is a sound policy basis for that rule, and it has not been suggested that it should be changed.

Two issues have been raised as to the suitability of the current rules.

The first issue relates to the provision, repealed in 2018, that enabled a child to take control of their own MHR by establishing to the System Operator's satisfaction that they had the maturity to control their own MHR. The Agency submission gave 2 examples of why it is important to have that procedure in the Act. The first is that a child aged 13 or younger may face a risk to their safety from a parent or guardian who is an authorised representative and who could locate the child through address information in the child's MHR. The second is that a child of that age may be a parent or carer for another person but would be unable to manage the MHR of that person because the child is not recognised by the MHR Act as having capacity to manage their own MHR.

Recommendation 20 below is that the former rule should be restored as part of a general revision of the rules relating to minors. The former rule was aligned to the objectives of the MHR system of enabling individuals to manage their own MHRs and to minimise risks to the health and safety of record holders.

The second issue has to do with the rules defining who can be an authorised representative of a child aged between 0 and 13. A concern raised by a few state government agencies[240] is that a parent who is not suited to being an authorised representative may nevertheless be eligible under the provisions of the MHR Act. The following examples have been given:

- A parent may have unsupervised access to a child even though a state court order has removed parental responsibility by placing the child in state care.
- A court order may require a parent to be supervised when spending time with a child, but the court order may not have come to the notice of the System Operator, in part because orders of that nature can change repeatedly and quickly.
- A state child protection database may not record whether a birth parent has supervised or unsupervised access.

There has been no elaboration on those issues in submissions to this inquiry. The concerns are partly addressed in 2 recommendations in Chapter 4: Recommendation 6, that a person should be ineligible to be an authorised representative if the System Operator is satisfied that the life, health or safety of a child 'is likely to be put at risk' rather than 'would be put at risk' (as currently required by s 6(1A)(b) of the MHR Act); and Recommendation 7, that the Department of Health examine whether state and territory laws and administrative protocols impede information sharing with the System Operator.

The issue of concern earlier raised by the states may extend beyond the boundary of those 2 recommendations. Accordingly, Recommendation 21 is that the Department of Health should consult with state and territory government agencies as to any remaining concerns they hold about the effectiveness of the safety net powers in the MHR Act.

---

[240] In correspondence with the Department of Health prior to the commencement of this inquiry.

Minors aged 14–17

There appears to be broad acceptance, including in submissions to this inquiry,[241] of the rule introduced in 2018 that a child aged between 14 and 17 has control of their MHR unless they appoint an authorised representative to control the record.

The child's record many contain health information that he or she does not wish others, including parents, to view. For example, the record may reveal that the child has individually sought confidential advice from a health practitioner or specialist adolescent clinic on a matter that involves sexual or mental health or drug use. Similarly, the child's record may contain the results of a pathology or diagnostic test that reveals a possible health condition of a sensitive or private nature.

Another reason for separate control is that a child's parents may be separated or in conflict. A possible hazard is that one or other parent could use information from the child's MHR to agitate a dispute with the other parent. Equally, the child may be apprehensive about allowing parents who are in disagreement to have equal access to the child's health record.

A few submissions to this inquiry nevertheless made the point that, beyond the scope of the MHR Act, a child aged 14 or above is not necessarily regarded as having independent capacity in medical decision making.[242] There was mention in some submissions of the competency standard in *Gillick v West Norfolk Health Authority* – 'the parental right to determine whether or not their minor child below the age of sixteen will have medical treatment terminates if and when the child achieves sufficient understanding and intelligence to enable him or her to understand fully what is proposed'.[243]

Resetting the age categories

While there is general acceptance that a child aged between 14 and 17 should have control of their MHR, the introduction of this separate age category to achieve that result is open to question. The alternative is to combine the 14–17 age category with the adult category.

Prior to 2018 the MHR Act defined 2 age categories – 0–17 (minor) and 18 and above (adult). There are now 3 age categories – 0–13, 14–17 and 18 and above.

The age category 14–17 was not part of the 2018 amending Bill sponsored by the government;[244] it was a crossbench proposal that was made during parliamentary debate on that Bill. There was already a similar administrative practice in place whereby the System Operator would write to a child who turned 14 advising that they could apply to take control of their own MHR and for the access of an authorised representative (usually a parent or guardian) to be removed. This aligned with the practice also adopted by Services Australia of allowing children aged 14–17 direct access to their Medical Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) information (and removing access for their parents/guardians).

The 2018 change introduced anomalies that can be to the disadvantage of children aged 14–17. These anomalies would largely be resolved by combining the 14–17 and 18 and above age categories as proposed in Recommendation 22.

---

[241] Eg submission Nos 19 (Defence), 29 (MIGA), 31 (Arnold), 34 (Victoria), 36 (OAIC), 37 (Pharm Guild), 40 (AMA).
[242] Eg submission Nos 35 (Avant), 40 (AMA), 41 (RACGP).
[243] *Gillick v West Norfolk Area Health Authority* [1986] AC 112 (Lord Scarman), approved in *Secretary of the Department of Health & Community Services v JWB* (1922) 175 CLR 218 (*Marion's Case*).
[244] *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) (Act No 154 of 2018).

First, there is no procedure in the MHR Act to recognise an authorised representative of a child aged between 14 and 17 who lacks the capacity to make decisions on their own behalf. The MHR Act presently has a procedure of that kind for adults who lack capacity – specifically, the System Operator may recognise a person authorised under Australian law to be a substitute decision maker or, if there is no such person, to recognise 'an appropriate person'.[245]

The Agency submission advises that it has implemented an interim process of a similar kind of recognising a person who has explicit legal authority to act on behalf of a child aged between 14 and 17.[246] However, that option is not open if there is no court order or other clear legal authority.

Secondly, a child aged between 14 and 17 can consent to having either an authorised representative or a nominated representative. As noted above, an authorised representative substitutes for the child, whereas a nominated representative exercises the powers agreed to by the child (for example, concurrent power or view-only access). It is possible that a child may not fully understand that difference and the implications (although the Agency submission notes that this is explained to a child seeking to appoint a representative, with a recommendation that the nominated representative mechanism be used).

The different structure applying to adults is that an adult may agree to a nominated representative; and the authorised representative procedure is only available if an adult lacks the capacity to make decisions on their own behalf.[247]

Thirdly, the System Operator can decline to recognise a person as an authorised representative of a child aged 13 or younger if doing so would pose a risk to the life, health or safety of the child or any other person.[248]

It is unclear whether that safety net power also applies to children aged 14–17. The System Operator's power is expressed in the MHR Act to apply to 'a healthcare recipient aged under 18',[249] whereas the subsection heading for the relevant powers refers to 'Healthcare recipients aged under 14'.[250]

It is appropriate that this safety net power should apply to children aged 14–17. A child in that age range could face unreasonable pressure to agree to an unsuitable parent/guardian as an authorised representative. In fact, Recommendation 6 in Chapter 4 is that this safety net power should apply to record holders of any age – a matter that becomes more important if the 14–17 and 18 and above age categories are combined as proposed in Recommendation 22.

Fourthly, the 2018 amendments have highlighted another issue on which there is no clear guidance in the MHR Act: whether a minor can be appointed as an authorised or nominated representative.

Prior to the 2018 amendments the rule applying to all children aged 0–17 was that an authorised representative would be a person with 'parental responsibility' for the child.[251] That rule still applies to children aged 0–13. By contrast, a child aged between 14 and 17 may now nominate any person to be their authorised representative by a written notice to the System Operator and may similarly agree to any person being their nominated representative.

It may be appropriate that a child aged between 14 and 17 can agree to nominate a person of similar age (for example, the 2 people may be in a marriage-like or dependant relationship). It may similarly be appropriate that an adult can nominate a minor as their representative (for example, the adult may face difficulty in making decisions because of illness or other circumstance and would like to nominate a mature child to make decisions on their behalf).

---

[245] MHR Act s 6(4).
[246] Submission No 28 (Agency) p 11.
[247] MHR Act s 6(4).
[248] MHR Act s 6(1A)(b).
[249] MHR Act s 6(1A).
[250] MHR Act s 6.
[251] MHR Act s 6(1) prior to amending Act No 154 of 2018.

On the other hand, an alternative scenario can be imagined in which a child or adult agrees to nominate a minor who is not suited to managing their MHR. The MHR Act could address this issue directly by providing that the System Operator must be satisfied that a minor nominated as an authorised or nominated representative is an appropriate person to perform that role. That is proposed in Recommendation 23.

Age settings in other laws and schemes

Medicare

Medicare documents are the largest component of documents uploaded to MHR.[252] Consequently, a large volume of medical and pharmaceutical benefits and other claims history information is accessible through both Medicare and MHR.

Medicare and MHR have different child age settings: a child is eligible to obtain a separate Medicare card at age 15 yet has control of their own MHR from age 14. A child can also remain listed on a parent's Medicare card after obtaining their own card.

Medicare information access principles have been implemented that lessen any bearing of those different age settings:

- A child aged 14 or above can access their Medicare claims information directly through both Medicare and MHR (if the information has been uploaded).
- Medicare requires the signed consent of a child aged 14 or above before releasing their claims information to a parent.[253]
- Medicare claims information ceases to flow to a child's MHR once they turn 14. The information flow recommences when the child takes control of their MHR or turns 18. (Upon turning 14 the child must take active steps within myGov to take control of their record.)
- Claims information relating to a child aged between 0 and 13 can be obtained by a person with parental responsibility for the child either through MHR or from Medicare if the child is listed on the person's Medicare card.

There is asymmetry between MHR and Medicare access principles at 3 points.

First, if a child aged between 14 and 17 appoints an authorised representative, only that representative and not the child has access to the child's MHR. By contrast, the child's consent is required for a representative (such as a parent) to access the same information directly from Medicare.

This irregularity would be resolved if the 14–17 age category was combined with the adult category. The authorised representative mechanism would then be restricted to the situation in which a healthcare recipient aged 14 or above lacked the capacity to manage their own MHR.

Secondly, if a child (of any age) is listed on more than one parent's Medicare card, claims information in the Medicare database is partitioned between their cards. A parent can access claims information only if it is connected to their card.

By contrast, Medicare claims information that is uploaded to the MHR system is not partitioned and will be available to any person with access to an MHR. This creates an obvious risk – and potential danger to one or more individuals – that a parent may access Medicare claims information relating to their child that the other parent does not wish them to see.[254]

---

[252] The Chief Executive Medicare has a discretion, as a registered repository operator, to upload health information to MHR: MHR Act s 38(2) Sch 1 cls 11–13.
[253] See Medicare form, 'Request for Medicare claims information (MS031)'.
[254] See submission No 28 (Agency) p 13. The adverse impact of this practice was explained by a parent of a child in submission No 3 (Anon).

Thirdly, if the upload of Medicare data to MHR for a child aged 14 or above is not actively restored by the child or a representative, the value of the MHR to the child is correspondingly reduced.

The first of those 3 points can be resolved through amendment of the MHR Act – specifically, by combining the 14–17 and adult age categories as proposed in Recommendation 22.

The second and third points could probably be resolved at an administrative level by the Department of Health, Medicare and the System Operator. Changes would be required to a few MHR system features: the Medicare information that is uploaded to MHR; the partitioning of health information in a child's MHR; and advice given by the System Operator to parties as to the optional access control settings available to them in MHR. Recommendation 24 proposes that the department initiate discussion with Medicare and the Agency on those points.

Other Commonwealth health information repositories

Two other Commonwealth health information repositories that are linked to MHR and contain age settings can be briefly noted.

The Australian Immunisation Register is a national register that records all vaccines given in Australia, including private flu and travel vaccinations; and vaccinations given through programs such as the National Immunisation Program and school programs. Similar to MHR, the Australian Immunisation Register functions on an opt-out basis and a person aged 14 or above can block disclosure of identifying personal information on the register (for example, to vaccination providers) and can decline to receive vaccination notices.[255]

The Australian Immunisation Register contains vaccination information for nearly 15 million people. A person aged 14 or above can access their vaccination information on the register (via myGov) through either MHR or Medicare online. A parent/guardian can access information for a child aged between 0 and 13 but requires the consent of a child aged 14 or older to access their personal information on the register.

The Australian Organ Donor Register[256] is a voluntary register that enables individuals to register their decision on organ and tissue donation following their death. A person must be aged 18 or above to enter a donation decision on the register, but they can register their intent to be an organ and tissue donor from the age of 16.

The Australian Organ Donor Register contains organ and tissue donation decisions for 1.6 million people. A person can access their entry on the register through MHR or Medicare online.

Interaction of MHR and state and territory rules

Some states and territories upload medical history information into MHR, including medical history information relating to minors. The laws of each state and territory (such as right to information and health privacy laws) regulate access to information that is in the possession of a state. Those laws do not apply to information that has been uploaded to MHR.

It is therefore possible, for example, that a parent cannot access health information relating to a child under state or territory law but can access it through MHR.

Recommendations

Recommendations 20–24 address the following issues raised in the preceding discussion. They should be read in conjunction with Recommendation 6 in Chapter 4 relating to authorised and nominated representatives:

---

[255] *Australian Immunisation Register Act 2015* (Cth) s 11.

[256] Established by the Organ and Tissue Authority under the *Australian Organ and Tissue Donation and Transplantation Authority Act 2008* (Cth).

- ***Recommendation 20:*** The 2018 amendments to the MHR Act repealed a provision that enabled a child aged between 0 and 13 to establish to the satisfaction of the System Operator that he or she had the maturity to control their own MHR. That repeal may have been an inadvertent consequence of other legislative changes. It is recommended that the provision be restored.
- ***Recommendation 21:*** Some state government agencies have expressed concern to the Department of Health that safety net powers in the MHR Act may not be wholly effective to ensure that the life, health or safety of a child is not put at risk by a person who is the child's authorised representative. This recommendation proposes that the Department of Health consult states and territories further on this issue, particularly in the light of other recommendations in this report that may address the concern the states had earlier raised.
- ***Recommendation 22:*** There is no compelling policy rationale for the MHR Act to have separate age categories for 14–17 and 18 and above. The same fundamental principle applies to both categories – namely, the healthcare recipient has control of their MHR subject to the appointment of a representative. Combining those age categories would resolve some anomalies that have resulted from the creation of a separate 14–17 age category in the 2018 amendments.
- ***Recommendation 23:*** An unstated consequence of the 2018 amendments to the MHR Act is that a child aged between 14–17 may agree to a person of similar or lower age being their authorised or nominated representative. This proposed amendment addresses the issue directly by requiring that the System Operator must be satisfied that a minor who is nominated to be a representative is an appropriate person to perform that role.
- ***Recommendation 24:*** There is asymmetry at 3 points between MHR and Medicare information access practices regarding access to Medicare claims information of a child aged 14 or above. One of those points would be resolved by Recommendation 22. The other 2 points can probably be resolved at an administrative level following discussion between the Department of Health, Medicare and the Agency.

Recommendation 20

The MHR Act s 6(1)–(2) be amended to provide that a healthcare recipient aged under 14 may take control of their own MHR by establishing to the satisfaction of the System Operator that the recipient wants to manage his or her own record and is capable of making decisions for himself or herself.

Recommendation 21

The Department of Health consult with states and territories on any concerns they may hold that safety net powers in the MHR Act are ineffective in ensuring that the life, health or safety of a child is not put at risk by an unsuitable person being eligible to be a representative of the child under the Act.

Recommendation 22

The MHR Act be amended to apply the provisions of the Act that relate to healthcare recipients aged 18 or above to healthcare recipients aged 14–17 (and thereby removing the provisions of the Act that separately relate to healthcare recipients aged 14–17).

Recommendation 23

The MHR Act be amended to provide that the System Operator may recognise the appointment of a person aged under 18 as an authorised or nominated representative of a healthcare recipient if the System Operator is satisfied that the person would be an appropriate person to perform that role.

Recommendation 24

The Department of Health consult with the Chief Executive Medicare and the Australian Digital Health Agency on administrative changes that could be implemented to resolve any inconsistent practices that may exist between Medicare and MHR regarding access by a child age 14 above or their representative to Medicare claims information relating to the child.

Chapter 10. Status of a My Health Record upon a person's death

Explanation of the MHR Act provisions relating to a deceased record holder

The status of a MHR upon the death of the record holder gives rise to difficult issues that go to the heart of MHR design.

The MHR system is described in the MHR Act as 'a national public system for making health information about a healthcare recipient available *for the purposes of providing healthcare to the recipient*'.[257] A deceased person can no longer receive health care.

Another foundation principle is consumer control. It enables a healthcare recipient to manage their own privacy settings and control both the content of their MHR and which healthcare organisations may view their record. A deceased person can no longer exercise those controls.

Those principles are reflected in the MHR Act in several ways:

- The System Operator is to cancel a person's registration in the MHR system upon receiving formal notice of their death[258] (and their registration may be suspended if earlier knowledge of death is received[259]). Cancellation of registration upon death does not result in destruction of the record or any health information included in it. The record and information is retained for 30 years after death (or, if the date of death is not known, for 130 years after the person's date of birth).[260]
- Access by authorised and nominated representatives to a healthcare recipient's MHR is suspended upon the System Operator being notified of the recipient's death.[261] A representative's access ceases when the System Operator cancels the deceased's registration upon receiving formal notification of death.[262]
- The MHR Act provides for limited disclosure of a person's MHR following death – for example, a coroner may direct the System Operator to disclose health information in a person's record to the coroner;[263] and the Auditor-General for Australia, Commonwealth Ombudsman and Australian Information Commissioner may require disclosure of a person's MHR (before or after they have died) for the purpose of discharging their functions.[264]

Several issues relating to the MHR of a deceased person could be clarified or reconsidered:[265]

- An authorised or nominated representative may, while the person they represent is alive, cancel that person's MHR registration or remove health information from their record.[266]

---

[257] MHR Act s 4 (emphasis added).
[258] MHR Act s 51(6).
[259] MHR Act s 51(2)(a). See also s 54(a) on the effect of suspension; and MHR Rule 2016 r 12, note 1, on the difference between notice and formal notice of death.
[260] MHR Act s 17(2)(b).
[261] MHR Rule 2016 r 12.
[262] MHR Act s 51(6); MHR Rule 2016 r 12, note 2; see also MHR Act ss 6(7), 54(a).
[263] MHR Act s 69(2).
[264] MHR Act s 65.
[265] Several submissions to the inquiry referred to one or other of these issues: see submission Nos 4 (Anon), 19 (Defence), 23 (AIHW), 25 (Telstra Health), 28 (Agency), 29 (MIGA), 31 (Arnold), 35 (Avant), 36 (OAIC), 37 (Pharm Guild), 40 (AMA), 41 (RACGP).
[266] MHR Act ss 6(7), 7(2).

Cancellation of a person's registration leads to the destruction of all health information in their record.[267]

The representative cannot exercise those powers to cancel registration and destroy records following the death of the healthcare recipient. The record of health information is retained in the National Repositories Service for 30 years or longer.

There may be good reason why a representative would like to remove some or all information from a deceased person's record – for example, to ease trauma following the death of a child. There is also the broader issue of principle of whether a representative should retain the right to exercise powers on behalf of a healthcare recipient after that recipient has died.

- A related issue is that a representative cannot access the record of the person they represent following that person's death. That may cause concern to a representative, knowing that health information they could access before a person's death still exists but can no longer be accessed. A representative who is a biological relative of the deceased may have a direct interest in checking for information relevant to a family health or genetic condition.
- A broader issue, raised in the Royal Australian College of General Practitioners submission,[268] is whether a record holder should have power (consistently with the underlying MHR principle of consumer control) to specify who can access their record after death. For example, a person may grant (or deny) post-death access to next of kin and/or to representatives.
- The deceased person's record may currently be available for a particular purpose through one pathway but not another. For example, a coroner can require disclosure of health information from a person's record,[269] but the record is not otherwise available to support a clinical review of the cause of death. Similarly, an organ donor consent is accessible through the Australian Organ Donor Register but not through a deceased person's MHR.
- It is unclear whether a scheme to release MHR system data for public health research could include the health information of a deceased person. Section 109(7A) of the MHR Act provides that a Rule may be made to establish a data sharing framework applying to 'de-identified data and, with the consent of healthcare recipients, health information'. It is an open question whether a consent given (or presumed to have been given) before death has continuing force. It would be better if this issue was clarified expressly.

  Generally, it would be advantageous to public health research if MHR health information of deceased record holders could be used, either as a data subset or linked to other datasets and documents. The record may be more valuable if important post-death documents, such as a death certificate or autopsy report, can be added to it.
- A healthcare provider who is unaware of a person's death may have accessed their MHR in the period between death and the suspension and cancellation of the deceased's registration by the System Operator. An example given in the Pharmacy Guild of Australia submission[270] is that a community pharmacy, unaware of a person's death, may have accessed their MHR for the routine purpose of preparing a Dose Administration Aid (Webster Pack).
- The default access that a registered healthcare provider organisation has to records in the MHR system is 'for the purpose of providing healthcare to the registered healthcare recipient'.[271] That care can no longer be provided upon a person's death.

---

[267] MHR Act s 17(3).
[268] An option suggested in submission No 41 (RACGP).
[269] MHR Act s 69(2). Use and disclosure of the record is also authorised under MHR Act s 68 if the death gives rise to a medical indemnity cover issue.
[270] Submission No 37 (Pharm Guild).
[271] MHR Act s 61(1)(a).

Unauthorised collection or use of MHR health information is a criminal and civil penalty offence if a person undertaking that access knows or is reckless as to the fact of authorisation.[272] A healthcare provider who has accessed a deceased's record unaware of their death would likely have a good explanation and defence on the basis that they have not, knowledgeably or recklessly, accessed the record for an unauthorised purpose. On the other hand, the MHR Act could deal directly with this unique circumstance by removing any doubt that the healthcare provider incurs liability.

- A related question, raised in the Australian Medical Association submission,[273] is whether the MHR Act should contain a special authorisation for a person's nominated healthcare provider to access their MHR post-death in order to assist an inquiry into cause of death, to confirm an organ donation decision, or (consistently with the practitioner's ethical obligation) to explain the cause of death to a family member or carer.[274]
- A couple of submissions commented on the long period (between 30 and 130 years) for which the record of health information of a deceased person is retained in the National Repositories Service.[275] This issue is noted in Recommendation 25 as a matter that may warrant further consideration by the Department of Health.

Privacy laws and the death of a record holder

A comparative issue noted in a few submissions is that some but not all privacy laws apply to the personal information of a deceased person.[276] The following 2 examples are illustrative.

The *Privacy Act 1988* (Cth) does not apply to personal information 'about an identified *individual'*; the term 'individual' is defined to mean 'a natural person', which would not include a deceased person.[277] By contrast, special provisions in the Privacy Act that permit a departure from normal privacy principles when an emergency or disaster declaration is in force do apply to 'personal information [of] a person who is not living'.[278]

The *Privacy and Personal information Protection Act 1998* (NSW) does apply to the personal information of a deceased person but not if it is 'information about an individual who has been dead for more than 30 years'.[279] The same approach is adopted in the *Health Records and Information Privacy Act 2002* (NSW).[280]

Those examples illustrate the types of issues that can arise in devising how regulatory controls will apply to the personal information of deceased persons. This comparative law issue does not need to be taken further in this report, as there is no direct overlap between the MHR Act and those other Commonwealth and state/territory privacy law provisions.

---

[272] MHR Act s 59(1).
[273] Submission No 40 (AMA).
[274] See Medical Board of Australia, *Good medical practice: a code of conduct for doctors in Australia* (2014) para 3.12.11.
[275] Submission Nos 17 (Krieg), 36 (OAIC).
[276] Eg submission Nos 36 (OAIC), 37 (Pharm Guild).
[277] *Privacy Act 1988* (Cth) s 6(1), definitions of 'personal information' and 'individual'.
[278] *Privacy Act 1988* (Cth) s 80G(2).
[279] *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(a).
[280] *Health Records and Information Privacy Act 2002* (NSW) s 5(3)(a).

Recommendations

It is desirable that the MHR Act and MHR Rule 2016 are reviewed and possibly revised to address all or some of the issues discussed above. These matters could be addressed by legislative amendment without undermining the central objects of the MHR system – to support the provision of health care to individuals who have an MHR and who have control of the privacy settings in their record.

It is understandable that the operation of the MHR system has thrown up issues of unforeseen difficulty regarding the content of a record and access to it after the death of the record holder.

If the MHR Act or the MHR Rule 2016 is changed to allow an authorised or nominated representative to access a person's MHR after death, consequential changes may be necessary to preserve the integrity of the MHR system. The duties of a representative can no longer apply in the same terms following the death of the record holder. In particular, the representative cannot discharge their duty to take reasonable efforts to ascertain and give effect to the record holder's will and preferences or, if those cannot be ascertained, to act in a manner that promotes the personal and social wellbeing of the record holder.[281] Nor can the provisions of the MHR Rule 2016 that authorise the System Operator to suspend or cancel a representative's access to a person's MHR apply in the same terms following that person's death.[282]

The appropriate control to ensure that a representative does not misuse their access would be to confer a discretionary power on the System Operator to decide when access by a representative shall be allowed and to require a representative to agree to conditions of access that can be enforced.

Recommendation 25

The Department of Health consider whether amendments should be proposed to the provisions of the MHR Act and *My Health Records Rule 2016* that deal with managing and accessing the MHR of a deceased person, with particular reference to:

- whether an authorised or nominated representative should have continued access to the MHR of a deceased person and can request the System Operator to cancel the record or destroy information in the record
- the conditions that should apply to any access that an authorised or nominated representative has to a deceased person's MHR
- the criteria to be applied in releasing health information from a deceased person's records for matters such as public health research, clinical review of death and ascertaining organ donor consent
- access to and use by a nominated healthcare practitioner to the MHR of a deceased person
- the provisions of the Act that may result in an offence being committed by a healthcare provider who has accessed the MHR of a deceased person
- the length of the period (between 30 and 130 years) for which the record of health information of a deceased person is retained in the National Repositories Service

[281] MHR Act s 7A.
[282] MHR Rule 2016 rr 13, 14.

Chapter 11. Facilitating use of My Health Record system data for public health research

The commitment to public health research

The potential for use of MHR data for public health research[283] was recognised from the outset. The Act establishing the MHR system in 2012 provided that a function of the System Operator is 'to prepare and provide de-identified data for research or public health purposes'.[284]

A framework to exercise that function was launched in 2018 by a combination of executive and legislative action. The Department of Health published the *Framework to guide the secondary use of My Health Record system data* (the 2018 Framework), which had been developed through community consultation the previous year. Later in 2018 the MHR Act was amended to anchor the main elements of the 2018 Framework in the Act. This included the designation of the Australian Institute of Health and Welfare (AIHW) as the data custodian to prepare MHR information to be used for public health research. Work has commenced on shaping the AIHW role.

This chapter takes as its starting point that the development of a public health research framework as part of the MHR system is at an advanced stage, supported by a strong commitment within government.[285]

The next steps in making MHR system data available for public health research will be the appointment of members of the Data Governance Board, established in the 2018 legislative changes, and the making of a Rule to implement the 2018 Framework either as published or as modified.

A related development to be considered in that process is the Data Availability and Transparency (DAT) Bill that was released by the Australian Government in 2020 on an exposure draft basis. The DAT Bill will not apply to MHR data[286] but has the same aim as the MHR Act of sharing public sector data through a secure legal framework to enhance service delivery, policy development and related research.

Three recommendations later in this chapter endorse the action that is underway – appointing members of the Data Governance Board, making a Rule to implement the 2018 Framework, and having regard in doing so to the principles in the recent DAT Bill.

This chapter explains the background to the development of a public health research framework for MHR system data and the issues that have been addressed. Points raised in submissions to this inquiry are covered. Four themes are discussed:

- the rationale for making MHR data available for public health research
- privacy, security and other concerns that have been dealt with
- the elements of the 2018 Framework and MHR Act provisions on data release
- the elements of the DAT Bill and their relevance to the development of an MHR data sharing research scheme.

---

[283] The term 'public health research' is used in this section as a shorthand for the term used in the MHR Act, 'research or public health purposes'.
[284] *Personally Controlled Electronic Health Records Act 2012* (Cth) s 15(ma).
[285] The consultation paper for this inquiry adopted the same premise, asking (Question 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?'.
[286] Data Availability and Transparency Bill 2020 (Cth) (DAT Bill) cl 17(4)(a); Data Availability and Transparency Regulations 2020 (Cth) reg 5.

The rationale for making MHR patient data available for public health research

It is helpful to start by clarifying what is meant by 'data' and 'public sector data'. The MHR Act uses the term 'data' but does not define it. Both terms are defined expansively in the DAT Bill:

> ***Data** is any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means).*
> ***Public sector data** is data lawfully collected, created or held by or on behalf of a Commonwealth body, and includes … enhanced data.*[287]

In effect, the term 'data' refers to any information that an organisation holds. It is common nowadays that agencies hold information – or data – in digital form. Consequently, data sharing is customarily an electronic process of allowing another person to use or access a digitised (or curated or enhanced) agency dataset. Preparing the dataset for use by another provides an opportunity to remove any personally identifying information (also called de-identification or anonymisation).

Three data trends are interlinked: the range and size of government datasets has expanded exponentially, the knowledge value of those datasets has increased apace, and the pressure to share datasets with other agencies and researchers under strictly regulated conditions has intensified.

Those trends are propelled by a recognition that the value of information increases the more it is used. Data linkage enables problems, trends and options to be examined by a larger number of analysts and researchers. Different datasets can be integrated to provide a stronger evidence base for policy development. Services and products can be customised, coordinated and targeted. Program success and failure can be analysed and tracked. Cross-portfolio challenges and impacts can be identified and understood better.

As noted in a speech by the Australian Statistician, David Gruen:

> *The view that data is valuable is now an overwhelmingly accepted proposition … [T]he potential value of data increases many-fold when individual data sources are brought together to enable public policy issues to be examined from a range of different perspectives. For example, combining the health, education and employment circumstances of people can teach us a lot more than examining each individual characteristic on its own. … There are a growing number of integrated data assets being used across the public sector.*[288]

Many government programs demonstrate a commitment to data integration. A non-health example is smart city programs that guide urban planning and service delivery by collecting and integrating data from transport, workplaces, utilities, hospitals, schools, law enforcement and community services. Another example is the heavy reliance in Australia on data collection and analysis in government responses to crises such as bushfires and COVID-19.

The 2018 Framework document gave case study examples of how data linkage and analysis led to improvements in health service education, delivery and planning:[289]

---

[287] DAT Bill cl 10.
[288] D Gruen, 'The Promise of Data in Government' (Speech, Institute of Public Administration Australia, ACT, 11 March 2020).
[289] Department of Health, *Framework to guide the secondary use of My Health Record system data* (2018) Appendix A.

- In 1989 a Western Australian research project linked data from different registries and identified that a folate-enriched diet for an expectant mother could reduce the risk of a newborn baby having a neural tube defect (such as spina bifida). In 2007 all Australian governments agreed to introduce compulsory folate enrichment of bread-making flour, which led to a 14.4% decrease in neural tube defects in babies, including a 55% decrease in babies of teenage mothers and a 74% decrease in babies of Aboriginal and Torres Strait Islander mothers.
- A time series analysis of Pharmaceutical Benefits Scheme (PBS) data found a noticeable decrease in statin dispensing after an Australian television program that aired in 2013 (and was estimated to have been viewed by nearly 1.5 million people) questioned whether the benefits of statins had been overstated in reducing high cholesterol levels and cardiovascular disease. The statin dispensing rate decreased by 28.8% in the week following the program and 2.6% over time. The analysis of PBS data prompted a public education program to counter the trend away from statin dispensing that commenced after the television program.
- In 2014 a Northern Territory study that linked information on hospital admission, primary care and health funding found that diabetes was more effectively and inexpensively treated if at-risk patients regularly visited their doctor.

The 2018 Framework also gave examples of how de-identified MHR system data could play a similar role in healthcare analysis and forecasting:[290]

- The safety and effectiveness of new pharmaceuticals and medical devices could be tracked by monitoring healthcare patterns captured in MHR system data. This could provide a 'real world' perspective to supplement clinical trial results.
- MHR system data can provide a comprehensive picture of how people engage with and move through the health system. This can assist health service forecasting and planning.
- Specific health risks such as deep vein thrombosis from long-haul flights could be examined by data linkage (such as transport, immigration, residential, medical claims and hospital admission data).

Other examples given in the 2018 Framework[291] include the use of MHR system data to identify health service demands and gaps, accessibility of health services in different locations, effectiveness of particular health services and clinical interventions, links between health service demand and government welfare support, health education targets, self-care options and pathways, and recruitment of people to participate in clinical trials.

A landmark report by the Productivity Commission in 2017, *Data availability and use*, was strongly critical of Australian Government failure to make better use of existing data. Multiple points of failure were identified – lack of understanding of how data could be better used; failure to innovate in data linkage; legislative and cultural obstacles to data sharing that were 'choking the use and value of Australia's data';[292] failure to develop business models for better data use; and an undue data management focus on risk aversion and avoidance.

The Productivity Commission singled out underuse of health data as a prime area of concern. This was captured in 2 headings in the overview of the commission's report: 'Health data exemplifies the problem' and 'Australia's health data – an underutilised resource that could be saving lives'.[293] The commission noted that Australian health researchers can wait up to 8 years to get approved access to health data and that some researchers use United Kingdom health datasets instead.

---

[290] Ibid Appendix B.
[291] Ibid Appendix D.
[292] Productivity Commission, *Data availability and use* (Report No 82, 2017) p 2.
[293] Ibid pp 5, 6.

In 2018 the Australian Government broadly accepted the Productivity Commission's recommendations, committing to 'transform the data system in Australia and the way data is made available and used'.[294] Key steps that have since been taken are the publication of the DAT Bill in 2020 and the earlier appointment of an interim National Data Commissioner.

Privacy, security and other concerns in using MHR patient data for public health research

The potential use of MHR patient data for public health research encounters questions on 3 fronts – privacy, security and approved uses.

Privacy

Privacy has been raised both as an issue of *principle* and as a *practical concern*.

The issue of *principle* stems from a central tenet of privacy law that differentiates between the primary and secondary use of data collected by an agency. Tighter controls are imposed on the use and disclosure of personal information for a secondary purpose.

In an MHR context, the primary use of patient data is to provide health care to individuals. This is stated up-front in the MHR Act:

> *The MHR system is a national public system for making health information about a healthcare recipient available for the purposes of providing healthcare to the recipient.*[295]

Use of MHR data for public health research would be a secondary use. This is recognised in the title to the 2018 Framework – *Framework to guide the secondary use of My Health Record system data*.

The *Privacy Act 1988* (Cth) spells out the requirements that must be met in using/disclosing personal information for both primary and secondary purposes. The guiding principle, stated in Australian Privacy Principle (APP) 6, is that personal information is to be used/disclosed only for the purpose for which it was collected (the primary purpose), unless an exception applies.

Most of the requirements in the Privacy Act and the APPs regarding the collection, protection, correction, disclosure and destruction of personal information apply to use/disclosure for both primary and secondary purposes. However, an added restriction is that use/disclosure must not occur for a secondary purpose unless one of several conditions stated in APP 6 is met. Among those conditions are that the individual to whom the information relates has consented to the secondary use/disclosure, the use/disclosure is required or authorised by law, it is a reasonably expected use/disclosure that is related to the primary purpose, and the use/disclosure is done to lessen or prevent a serious threat to an individual's life, health or safety or to locate a missing person.

The Privacy Act also lists 'permitted health situations' for the use/disclosure of personal information for a secondary purpose.[296] One permitted situation is that the information is being used for public health research that will be conducted in accordance with government guidelines and without disclosure of the personal information used in the research.

---

[294] Department of the Prime Minister and Cabinet, *The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry* (2018) p 1.
[295] MHR Act s 4, 'Simplified outline of this Act'.
[296] *Privacy Act 1988* (Cth) s 16B; Australian Privacy Principle (APP) 6.2(d).

An example is the National Health and Medical Research Council (NHMRC) *Guidelines approved under section 95A of the Privacy Act 1988*. The guidelines outline the privacy considerations and procedures to be followed for human research ethics committee approvals of proposals to collect, use or disclose health information for research purposes, in the absence of any express consumer consent.

The 2018 Framework was aligned to those Privacy Act principles, as explained below. Among the stipulations in the 2018 Framework are:

- A special approval process is required for the secondary use of MHR system data for public health research.
- An MHR healthcare recipient can opt out of having their MHR health information used in the research.
- The researcher must sign an agreement specifying how the MHR system data and health information can be used.
- No personally identifiable information is to be released publicly or to others.

The *practical concern* is that there is an added risk of MHR patient information being improperly or inadvertently disclosed if it is released outside the MHR system for public health research.

The direct risk of disclosure is countered by the requirement in the MHR Act that personally identifiable health information can be used for public health research only if an individual has consented to that use.[297] Otherwise, only de-identified data can be used.

The MHR system implements those provisions of the MHR Act. An individual with an MHR can choose an MHR setting that does not permit their health information to be shared for public health research.

The indirect risk of disclosure is that de-identification may not be effective and it may be possible to re-identify a person from a dataset. That risk was shown in a University of Melbourne study in 2018[298] that managed to re-identify people from a dataset of de-identified Medicare Benefits Schedule (MBS) and PBS information that was published on the Australian Government open data website.[299] The dataset was a sample of medical billing records of about 2.9 million people over a period of 30 years from 1984 to 2014.

The university researchers demonstrated that health practitioners and patients could be re-identified by using known information about a person obtained from other public records and linking it to the published record. For example, the researchers said they could identify 7 prominent Australians, including 3 members of parliament and an AFL footballer.

The dataset was taken offline as a result of the study. An own-initiative investigation of the incident by the Australian Information Commissioner concluded that the publication of the data involved a breach of APP 6.[300]

---

[297] MHR Act ss 15(ma), 83(1)(a), 109(7A), 109A.
[298] V Teague, C Culnane and B Rubinstein, 'The Simple Process of Re-identifying Patients in Public Health Records' (18 December 2017) *Pursuit*, University of Melbourne, https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records. The following year the same 3 researchers showed how individuals could be identified in a dataset of 15 million de-identified public transport ticketing occurrences: 'Two Data Points Enough to Spot You in Open Transport Records' (15 August 2019) *Pursuit*, University of Melbourne, https://pursuit.unimelb.edu.au/articles/two-data-points-enough-to-spot-you-in-open-transport-records.
[299] *data.gov.au* (Website) https://data.gov.au.
[300] Office of the Australian Information Commissioner, *Publication of MBS/PBS data* (March 2018).

The government also responded by introducing a Bill into the parliament to amend the Privacy Act to make it an offence to intentionally re-identify information that had been published by a Commonwealth agency on the basis that it was de-identified personal information.[301] The Bill has not been proceeded with.

More generally, the Melbourne study has highlighted the importance of differentiating online open data publication of a dataset (as occurred with the information examined in that study) from controlled release of a dataset to a secure research environment. The 2017 Productivity Commission report drew attention to this distinction and to the importance of developing systems and processes for data sharing that mitigate the risks of identification.[302]

A central recommendation in the Productivity Commission report was the need for a new data sharing structure that allows access and sharing arrangements to be tailored to the risks associated with different types of data, users and use environments.[303] This has been taken up in the DAT Bill. As explained below, the Bill will establish a framework that authorises sharing of public sector data by data custodians with accredited users for permitted data sharing purposes and when effective safeguards are in place. This is expected to ensure comprehensive and effective consideration of privacy risks in data sharing.

An internationally respected practice for assessing and managing disclosure risk in data use is the Five Safes Framework. It is applied by Australian Government agencies, including the Australian Bureau of Statistics (ABS).[304] The Five Safes Framework requires consideration of 5 aspects of disclosure risk in handling confidential data:

Safe People	Is the researcher appropriately authorised to access and use the data?
Safe Projects	Is the data to be used for an appropriate purpose?
Safe Settings	Does the access environment prevent unauthorised use?
Safe Data	Has appropriate and sufficient protection been applied to the data?
Safe Outputs	Are the statistical results non-disclosive?

The ABS uses the Five Safes Framework in the Multi-Agency Data Integration Project (MADIP), which combines information on health care, education, government payments, personal information tax and population demographics.

The Five Safes Framework has been adapted in the DAT Bill as 5 Data Sharing Principles to be applied when considering a data sharing arrangement:[305]

Project Principle	Data is shared for an appropriate project or program of work.
People Principle	Data is made available only to appropriate persons.
Setting Principle	Data is shared in appropriately controlled environment.
Data Principle	Appropriate protections are applied to the data.
Outputs Principle	Outputs are agreed.

---

[301] Privacy Amendment (Re-identification Offence) Bill 2016 (Cth).
[302] Productivity Commission, *Data availability and use* (Report No 82, 2017) p 9.
[303] Ibid p 14.
[304] Australian Bureau of Statistics, 'Managing the Risk of Disclosure: The Five Safes Framework' (Catalogue No 1160.0, ABS Confidentiality Series, August 2017) https://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017.
[305] DAT Bill cl 16. The consultation paper accompanying the DAT Bill explains that the Data Sharing Principles are based on the Five Safes Framework as implemented in the ABS: Department of the Prime Minister and Cabinet, *Data Availability and Transparency Bill 2020: exposure draft* (consultation paper, September 2020) p 17.

Security

The security of a data sharing arrangement overlaps with privacy protection but requires separate consideration of inherent risks.

The 2 principal security risks are criminal intent and human error – that is, malicious action to gain unauthorised access to a personal information database; and defective storage and management practices that result in loss or misuse of personal information. Security risks are accentuated by developments in digital technology.

The Safe Settings component of the Five Safes Framework – and, correspondingly, the Setting Principle in the DAT Bill – aim to ensure the security of data that is shared with others. For example, the ABS allows access to MADIP data only through a closed system in the ABS IT environment with secure login controls, auditing of activity, researcher training, and a prohibition against data being taken out of the system or brought into it.

A similar approach is proposed in both the 2018 Framework and the DAT Bill. Data will be shared in a secure and controlled environment, and only accredited users will have data access under the scheme.

Approved uses

The 2018 Framework proposes that research access to MHR patient information will be scrutinised and approved only if 'the application demonstrates that the proposed data usage will generate public health benefits for Australians'.[306] The same approach is adopted in the Five Safes Framework and the DAT Bill Data Sharing Principles. Both require consideration of whether data is being made available for an appropriate purpose, project or program of work. (The contrasting principle in open data access is that information made available to the community through a public access website can be accessed by any person and used for any purpose.[307])

The 2018 Framework also addresses some particular areas of concern by listing uses/purposes that will not be approved:

- use solely for commercial and non-health related purposes
- use by an insurance agency[308]
- use for clinical trials recruitment ahead of development of an appropriate consent mechanism.[309]

The 2018 Framework and related MHR Act provisions

This section explains the main features of the 2018 Framework and the relevant provisions of the MHR Act. This involves some repetition of points already made in order to provide a more complete explanation of the proposed scheme for allowing MHR system data to be used for public health research.

---

[306] Department of Health, *Framework to guide the secondary use of My Health Record system data* (2018) p 23.
[307] Eg Prime Minister the Hon Malcolm Turnbull MP, 'Australian Government Public Data Policy Statement' (Australian Government, 7 December 2015); NSW Information and Privacy Commission, *Open data* (Information Access Guideline 7, May 2019).
[308] See also MHR Act s 16, which provides that de-identified data or health information cannot be provided to a private health insurer.
[309] Department of Health, *Framework to guide the secondary use of My Health Record system data* (2018) p 7.

The MHR Act, as amended in 2018, provides that the System Operator has the following function:

> *in accordance with the guidance and direction of the [Data Governance Board], to prepare and provide de-identified data, and with the consent of the healthcare recipient, health information, for research or public health purposes.*[310]

The MHR Act establishes a Data Governance Board that has a function of overseeing a framework to be established by a Rule for:

- assessing applications to collect, use or disclose de-identified data and health information for public health research
- guiding and directing the System Operator on preparing and providing de-identified data and health information
- ensuring that de-identified data and health information is protected and used only for public health research.[311]

The members of the Data Governance Board have not yet been appointed. The Act prescribes that there will be between 9 and 12 members and that membership will include a representative of the System Operator; the data custodian; an Aboriginal or Torres Strait Islander person; and other members with experience in fields such as health and medicine, technology, privacy and consumer advocacy. The MHR Act contains detailed provisions[312] relating to the appointment and responsibilities of board members, the conduct of meetings, annual reporting, and the System Operator's obligation to comply with the directions and guidance of the board.

The MHR Act designates AIHW as the data custodian.[313] The data custodian is to act under the direction of the Data Governance Board in discharging the functions of receiving and – to the extent necessary – de-identifying MHR data and health information, providing data linkage services, preparing and providing de-identified data and health information to users approved by the board, and ensuring that use conditions are observed.[314]

A new Rule is yet to be made to establish the framework for permitting MHR system data to be used for public health research and to spell out the responsibilities of the System Operator, the Data Governance Board and the data custodian.[315] The MHR Act specifies several mandatory requirements for a new research Rule:

- in the absence of individuals' consent, information from the MHR system that is to be used for public health research must be de-identified[316]
- information that identifies a healthcare recipient cannot be used for public health research without their consent[317]
- data and health information cannot be provided to a private health insurer, regardless of whether the healthcare recipient would consent.[318]

The 2018 Framework was published prior to the 2018 amendments of the Act relating to the Data Governance Board, the data custodian and the proposed new research Rule. There is some difference in terminology, but the expectation is that the proposed new Rule will be based on the 2018 Framework. The provisions of the 2018 Framework are therefore informative.

---

[310] MHR Act s 15(ma).
[311] MHR Act ss 82, 83.
[312] MHR Act Pt 7.
[313] MHR Act s 5.
[314] MHR Act s 109A(2).
[315] The Rule is to be made under MHR Act ss 109(7A), 109A.
[316] MHR Act s 109A(2).
[317] MHR Act ss 15(ma), 109(7A), 109A(3)(a).
[318] MHR Act s 109A(3)(b).

The 2018 Framework restates many of the elements that are now set out in the MHR Act, such as the roles of the System Operator, the Data Governance Board and the data custodian. Other points to note include the following:

- The Data Governance Board assesses applications to use MHR system data.
- An application can be received from any Australian-based entity except an insurance agency.
- The board will use the Five Safes Framework principles in assessing applications.
- MHR data that is made accessible for public health research must not leave Australia.
- A healthcare recipient may opt out of having their MHR data used for public health research by clicking on a 'withdraw participation' button in their MHR.
- Use of MHR data for clinical trials recruitment will not be considered until a consent option is available in the MHR access controls.
- An application for the use of data solely for commercial purposes will not be approved.
- Specific consideration will be given to use of data pertaining to Aboriginal and Torres Strait Islander people and communities.
- Ethics approval for the use of identified data must be granted by the data custodian and may be required for other applications.
- An approved applicant must agree to a conditions of use agreement that will include monitoring processes, data breach notification to the Office of the Australian Information Commissioner (OAIC), and a requirement for some bodies that are not subject to OAIC oversight to opt in to Privacy Act coverage.
- Linkage of MHR system data to other data sources may be approved if that is assessed to be of public benefit.
- Protection of the privacy of individuals will be a central consideration. Special measures, including a recommendation for penalties to be applied for a privacy breach, will be put in place to ensure adequate protection.
- The OAIC will exercise its privacy regulatory oversight functions in relation to actions taken under the 2018 Framework by entities that are covered by the Privacy Act.
- Transparency will be built into the scheme, including through a public register of requests for research access to MHR system data.
- A review of the 2018 Framework is to be undertaken after 2 years. The list of permitted and non-permitted purposes will be reconsidered as part of that review.

The 2018 Framework explains at the beginning that it 'deliberately takes a cautious approach to the secondary use of MHR data … to build public trust in the process through transparent decision making and wide sharing of the results'.[319] The 2018 Framework notes changes that may be implemented based on experience and periodic review of the Framework. These include:

- redefining the list of permitted purposes for public health research
- adding a dynamic consent mechanism to allow healthcare recipients to consent to use of their health information on a case-by-case basis
- adding a consent mechanism for a healthcare recipient to participate in a clinical trial.

[319] Department of Health, *Framework to guide the secondary use of My Health Record system data* (2018) p 3.

The Data Availability and Transparency Bill 2020

This section briefly outlines (with some repetition) the main features of the DAT Bill.[320] The Bill was released in September 2020 on an exposure draft basis to invite public comment. The final form of the Bill (and any subsequent Act) may differ.

The DAT Bill will establish a framework to authorise and regulate controlled access to Commonwealth data – also called public sector data sharing. It is optional for a Commonwealth agency to share data under the DAT scheme. Alternatives for an agency are to share data through a private access arrangement with a researcher (also called administrative access) or to share data publicly on the agency website or on the government open data / release website.

Data sharing under the DAT scheme has some benefits over other options:

- The DAT scheme applies across government and thus provides a known, streamlined, transparent and accountable framework for data sharing.
- Data sharing under the scheme occurs in a secure and controlled environment to allay privacy and security concerns. This may facilitate greater public sector data sharing in line with the 2017 Productivity Commission report *Data availability and use.*
- A decision to approve a data sharing arrangement is principles based. This allows flexibility to tailor each arrangement to the particular research setting. It also allows arrangements to evolve in line with technology changes and community expectations.
- The scheme provides legal authority to share data, notwithstanding a non-disclosure requirement in another law.

The main features of the DAT scheme are as follows:

- The scheme is administered by the National Data Commissioner, who is an independent statutory office holder. The commissioner is supported by a National Data Advisory Council. Among the commissioner's functions are to advocate the scheme; monitor its operation; publish data codes of practice and guidelines; provide advice on data sharing; accredit users and data service providers; handle complaints and conduct investigations; and exercise regulatory compliance powers.
- An accredited user may apply to a Commonwealth body (a data custodian) to access a dataset that is controlled by the custodian. The custodian may approve the application:
    - if it is for a permitted purpose – which is defined broadly to include government policy formulation and review, program administration, service delivery and research and development
    - after considering the application by reference to the 5 Data Sharing Principles (noted above) that enable risks to be assessed and managed – the Project Principle, People Principle, Setting Principle, Data Principle and Outputs Principle
    - by requiring the accredited user to accept a data sharing agreement that will be individually framed around minimum mandatory terms and the matters assessed under the Data Sharing Principles.
- Special consideration will be given to the interests of Aboriginal and Torres Strait Islander peoples in decisions that affect them or data that relates to them.
- A data custodian may obtain assistance from an accredited data service provider (ADSP) to perform data services such as data integration and to be the conduit for sharing data with an accredited user.

[320] The following discussion is drawn from the Explanatory Memorandum to the DAT Bill and the accompanying consultation paper on the Bill published by the Department of the Prime Minister and Cabinet.

- The National Data Commissioner is to accredit users and data service providers in accordance with a published ministerial rule that will stipulate accreditation requirements relating to security, privacy, infrastructure and governance. An accredited user may be a government agency, a private sector body or a research centre.
- The Privacy Act (or an equivalent state or territory law) will apply to the actions taken under the scheme by accredited users and ADSPs; the data breach notification scheme in the Privacy Act also applies on a modified basis.
- There is to be a public register of accredited entities (users and ADSPs) and data sharing agreements.
- There are limitations and exclusions on the scope of the scheme. For example, the scheme does not apply to data held by intelligence agencies, material received by courts, tribunals and oversight bodies, or MHR system data; and a data sharing arrangement cannot override intellectual property rights or a contractual arrangement.
- While data sharing under the scheme will override a non-disclosure requirement in another law, a range of offences and penalties are either preserved or built into the scheme to prevent unauthorised data sharing. An example is that penalties can apply to the failure of an accredited user or provider to comply with the conditions of its accreditation.

Recommendations

The settled intent and commitment within government is to implement a secure framework that enables MHR system data to be used for public health research. This aligns with other government developments – such as government acceptance of the 2017 Productivity Commission recommendations on data availability and use; a commitment in Australia's second Open Government National Action Plan 2018–20 to 'Improve the Sharing, Use and Reuse of Public Sector Data';[321] and the publication of a DAT Bill in 2020.

A 2018 report on the MHR system by the Senate Community Affairs References Committee expressed support for use of MHR system data for population health research purposes.[322] Strong support was also expressed by health researchers participating in the public consultations from which the 2018 Framework was developed: the process of community consultation for the 2018 Framework engaged 714 individuals in webinars (159 people), workshops (256), survey responses (274) and interviews (25), as well as 80 written submissions.[323]

Some of the submissions to this inquiry also expressed support.[324] The AIHW submission observed:

> *AIHW believes there exists significant potential for MHR secondary use data to assist research and government and general community responses to future public health emergencies, such as COVID 19. … AIHW is already actively involved in undertaking and facilitating COVID-related research …*[325]

---

[321] See Department of the Prime Minister and Cabinet, 'Improve the Sharing, Use and Reuse of Public Sector Data', *Australia's Second Open Government National Action Plan 2018–20* (Commonwealth of Australia, 2018) https://ogpau.pmc.gov.au/national-action-plans/australias-second-open-government-national-action-plan-2018-20/improve-sharing.
[322] Senate Community Affairs References Committee, Parliament of Australia, *My Health Record system* (October 2018) para 2.109.
[323] Department of Health, 'Developing a Framework to Guide the Secondary Use of My Health Record System Data – 2017 Submissions' (2018) https://www1.health.gov.au/internet/main/publishing.nsf/Content/eHealth-framework-development.
[324] Eg submission Nos 1 (Anon), 11 (Anon), 19 (Defence), 23 (AIHW), 25 (Telstra Health), 37 (Pharm Guild), 39 (Anon), 40 (AMA).
[325] Submission No 23 (AIHW).

The Senate committee reported on 3 areas of concern that were raised in submissions to its inquiry – the risk of personal privacy being jeopardised by re-identification of data that is released for health research; potential inappropriate use of MHR data by insurers and commercial entities; and the requirement for healthcare recipients to opt out rather than opt in to research use of their MHR health information.[326] Some submissions to this inquiry also noted the importance of privacy protection in any data sharing scheme.[327]

Those concerns are addressed in the 2018 Framework[328] in the following ways:

- The framework prevents MHR system data being used by an insurance agency or solely for commercial and non-health related purposes.
- The Data Governance Board is to apply the Five Safes Framework principles.
- The AIHW will be the data custodian.
- A dynamic consent mechanism is envisaged.

It is noteworthy too that only 0.1% of MHR recipients have opted out of having their health information used in public health research.

Generally, the issues relating to the development of a framework to permit the use of MHR information for public health research have been extensively canvassed. The matter could suitably be taken forward by the (interim) appointment of members to the Data Governance Board. Board members would then be well placed to contribute to the development of a Rule to implement the 2018 Framework. They would also have an opportunity to review the proposed MHR framework in light of the principles and procedures that have subsequently been proposed in the DAT Bill.

The following observations, drawn from the analysis in this chapter, may warrant consideration in developing a new research Rule:

- It is appropriate (as proposed) that the use of MHR system data for public health research should occur under a separate scheme that is based in a Rule made under the MHR Act rather than under the proposed DAT Act. There is keen community interest in ensuring that sensitive MHR health information is managed according to the privacy and security requirements of the MHR Act. The overlap between the MHR and DAT data sharing schemes would doubtless be a matter of joint interest to the Data Governance Board and the National Data Advisory Council.
- The Rule to permit release of MHR system data for public health research should take account of the terminology and principles of the DAT Act (when enacted). Examples are the proposed Data Sharing Principles and template conditions for data sharing agreements. It is desirable that there is consistent practice across government in assessing data access applications and monitoring compliance with access conditions.
- A term used in the 2018 Framework that should be reconsidered is ‘secondary use of MHR system data’. Though that term is taken from the Privacy Act, it may be misinterpreted as referring to a non-conforming data use.

---

[326] Senate Community Affairs References Committee, Parliament of Australia, *My Health Record system* (October 2018) paras 2.88–108.
[327] Eg submission Nos 9 (Anon), 17 (Krieg), 24 (Fernando), 31 (Arnold), 35 (Avant), 36 (OAIC), 40 (AMA), 41 (RACGP).
[328] They are also discussed in the Office of the Australian Information Commissioner’s submission on the consultation paper for the development of the 2018 Framework: Office of the Australian Information Commissioner, *Consultation paper on the development of a framework for secondary use of My Health Record data – submission to HealthConsult* (21 November 2017) https://www.oaic.gov.au/engage-with-us/submissions/consultation-paper-on-the-development-of-a-framework-for-secondary-use-of-my-health-record-data-submission-to-healthconsult.

- Another term used in the 2018 Framework and the MHR Act that should be reconsidered is 'de-identify'. There is a degree of community scepticism about the effectiveness of de-identification. An alternative approach (as reflected in the DAT Bill) is to place emphasis on risk minimisation that is achieved by releasing data into a controlled environment that is accessible only by accredited researchers who have given a written undertaking as to how data will be used.
- The 2018 Framework uses the term 'MHR system data', whereas later amendments to the MHR Act use the term 'de-identified data and health information'.
- The MHR Act and MHR Rule 2016 should retain the present settings that MHR documents with a Restricted Access Code should not be released under the data release scheme and that a healthcare recipient may opt out of having their MHR health information released under the scheme.

  Consideration should be given to whether the *National Health Act 1953* (Cth) s 135AA would impede a data sharing scheme by precluding MBS and PBS information that has been uploaded to the MHR system from being linked to other data.

Recommendation 26

The Australian Government appoint as early as practicable – and, if appropriate, on an interim basis – the members of the Data Governance Board established in Part 7 of the MHR Act.

Recommendation 27

The Minister for Health make a Rule under the MHR Act s 109(7A) to prescribe a framework to guide the collection, use and disclosure of MHR patient health information for research or public health purposes. The Rule should take account of the data sharing frameworks outlined in the *Framework to guide the secondary use of My Health Record system data* (2018) and the Data and Transparency Bill 2020.

Recommendation 28

The Department of Health consider the desirability of amending the MHR Act ss 15(ma), 82–96J, 109(7A) and 109A to ensure consistency with the provisions and terminology in the Data and Transparency Bill 2020.

Chapter 12. Revising, updating and clarifying the My Health Records Act

This section considers the proposals made in submissions to this inquiry for amending the MHR Act to address gaps, anomalies and other issues that have been highlighted during the 8 years of operation of the Act. Many of the proposals that are discussed were made in the submission from the Australian Digital Health Agency (the Agency)[329] and in other submissions also.

Many of these proposals were aired publicly for the first time in this inquiry and have not had exposure to wider analysis and commentary. For that reason, it is recommended at the end of this section that some proposed changes endorsed in this report should nevertheless receive further consideration and consultation, led by the Department of Health. That will also provide an opportunity to examine whether there is stronger merit in some other proposals that have not been endorsed.

Simplifying the MHR Act by consolidating the opt-out provisions

When enacted, the *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act) (now titled the MHR Act) was framed on the assumption of an opt-in model for healthcare recipients. The opt-out model, which was enacted in 2015[330] and commenced in 2018, was framed as Schedule 1 to the Act. The Schedule provided that the Minister could introduce the opt-out model by an MHR Rule[331] but was first to conduct a trial of the opt-out model to gauge if it provided value for those using the MHR system[332] and also to consult the Ministerial Council.

A consequence of that staged introduction is that there is substantial overlap and repetition between the original provisions of the MHR Act and the later additions in Schedule 1 that support the opt-out model.[333] This partly frames the MHR Act as a historical narrative. It also makes it difficult to navigate the Act and to decide which provisions to apply. For example:

- Schedule 1 states[334] that, if the opt-out model has commenced, specified sections of the Act no longer apply to a healthcare recipient and other specified sections are to be read as referring instead to a relevant provision in Schedule 1.
- Separate (though largely similar) eligibility rules for registering as a healthcare recipient are set out in both the body of the MHR Act and in Schedule 1.[335]
- It is unclear whether the authorisations in the MHR Act that empower nominated entities to collect, use or disclose particular information derive force from the table in s 58A or from a matching table in Schedule 1, cl 8.

The opt-out model is now firmly embedded in the MHR Act, in the operation of the MHR system and in the understanding of the Australian community. No submission to this inquiry has argued for a return to an opt-in model.[336]

It would therefore seem appropriate to update and modernise the MHR Act by merging and reconciling the provisions designed to introduce an opt-out model with the original provisions of the Act. Recommendation 29 below is made along those lines.

---

[329] Submission No 28 (Agency).
[330] *Health Legislation Amendment (eHealth) Act 2015* (Cth) s 106.
[331] MHR Act Sch 1 cls 1, 2. See *My Health Records (National Application) Rules 2017.*
[332] See also *My Health Records (Opt-out Trials) Rule 2016*.
[333] Eg MHR Act ss 58, 58A and Sch 1, cls 7, 8.
[334] MHR Act Sch 1 cl 17.
[335] MHR Act s 40 and Sch 1 cl 4.
[336] Cf submission No 17 (Krieg) proposing that record holders should be notified annually that they can cancel their registration.

That would also provide an opportunity to update and reconcile other features of the MHR Act that add to its complexity. For example, the discussion in Chapter 8 of the prohibited purposes provisions noted the complexity stemming from 2 sets of similarly worded provisions in the MHR Act on use and disclosure.

Repeal of the assisted registration provisions

The Agency submission drew attention to one legislative item that was tied to the introduction of an opt-out model but may now be redundant.

The *My Health Records (Assisted Registration) Rule 2015* (Cth) (Assisted Registration Rule) prescribes a procedure for a registered healthcare provider organisation to assist a healthcare recipient to apply to register for an MHR. The Assisted Registration Rule places obligations on the provider organisation to identify the healthcare recipient, obtain the person's consent and provide advice on alternative methods of registration.

The Agency submission advises that no work has been required under the Assisted Registration Rule since January 2019 (that is, since the conclusion of the national opt-out transition period). Alternative sources of assistance, such as the Agency website, the Agency telephone assistance line and Medicare offices, are now available to people who do not currently have an MHR but wish to register.

Recommendation 30 below is that the Assisted Registration Rule be repealed.

One aspect of the Assisted Registration Rule that may have continuing relevance is r 8, which provides that a healthcare provider organisation must exercise reasonable care in making a declaration to support a healthcare recipient's assertion of parental responsibility for a person. An assertion to that effect may be made by a person who seeks to be recognised as the authorised representative of a child aged under 14.[337] Consideration should be given to expressly saving r 8, either in another rule or in an administrative instruction issued by the System Operator.

Safeguarding the security and integrity of the MHR system

An important responsibility of the System Operator is to protect the 'security' and 'integrity' of the MHR system. Both terms are used in numerous provisions of the MHR Act:

- The System Operator has several powers that are expressly conditioned on action being taken to prevent compromise to the security or integrity of the MHR system – such as refusing to register a healthcare recipient or entity, cancelling or suspending their registration, or suspending their access to the MHR system.[338]
- Access to the MHR system can be suspended if there is a security problem with the information technology system of a participant or a failure by a participant to maintain interoperability with the MHR system in accordance with the System Operator's interoperability requirements.[339]
- The System Operator may remove a record in the MHR system that may affect the security or integrity of the system.[340]
- The data breach notification scheme in the MHR Act applies to any event (regardless of whether it is a contravention of the MHR Act) that may compromise the security or integrity of the MHR system.[341]

---

[337] MHR Act s 6(1).
[338] MHR Act ss 41(2), 44(2), 49(2), 51(2)(c), 51(3)(b)(iii); Sch 1 cls 3(2)(a), 6(4)(a); MHR Rule 2016 r 17.
[339] MHR Rule 2016 rr 17(2)(a), (c), 31.
[340] MHR Rule 2016 r 21.
[341] MHR Act s 75(1)(b)(iii).

- The term ‘security’ is used in a provision of the MHR Act authorising the Australian Information Commissioner to disclose to the System Operator any information acquired during a privacy investigation of an MHR matter if the information will enable the System Operator to monitor or improve the security of the MHR system.[342]

The Agency submission raises 3 issues relating to the terms security and integrity:

- the absence of a definition of those terms in the MHR Act
- additional powers that could be given to the System Operator to safeguard security and integrity
- the use of those terms in the data breach notification scheme (a matter discussed in Chapter 5 of this report).

Defining ‘security’ and ‘integrity’

The terms ‘security’ and ‘integrity’ are words of broad meaning. They are used in a diverse range of Commonwealth statutes, generally without definition apart from examples they give of matters that may fall within either term when the statute is being administered. As that indicates, the words derive meaning from the context in which they are used.

It would be difficult to define the words in the MHR Act in a way that would satisfactorily resolve ambiguity. Indeed, the risk is that any definition will be confining and later need to be extended as unforeseen situations arise.

Three other measures are ordinarily adopted to clarify the meaning of statutory terms of indefinite meaning that play a pivotal role in a regulatory scheme.

The first measure is to give substance to an indefinite term by specifying relevant criteria or events in a subordinate rule. The MHR Act adopts that approach in several provisions that state, for example, that the System Operator may refuse to register a person or entity to avoid compromise to the security or integrity of the MHR system, ‘having regard to the matters (if any) prescribed by the My Health Records Rules’.[343]

Rule 17 illustrates that approach by listing events that may compromise the security or integrity of the system for the purpose of suspending access by a person or entity. These are:

- a security problem with the IT system of a participant
- an issue with verifying the identity of a healthcare recipient or their representative
- an MHR system participant failing to maintain interoperability with the MHR system in accordance with the MHR Rule 2016.

That same approach could be adopted for other powers in the MHR Act that are exercisable on the grounds of security or integrity. Circumstances that are deemed to compromise security or integrity could be spelt out in the MHR Rule 2016.

A second mechanism that is frequently adopted to clarify the meaning of statutory terms of indefinite meaning is to provide a right of appeal against a decision applying the term to an independent body such as the Administrative Appeals Tribunal (AAT). On a case-by-case basis, the AAT can then elaborate on the meaning of the term.

The MHR Act provides for a right to appeal to the AAT against decisions to refuse to register, or to cancel or suspend the registration of, a healthcare recipient, healthcare provider organisation, repository operator or contracted service provider.[344]

---

[342] MHR Act s 73A.
[343] Eg MHR Act ss 41(2), 51(2)(c).
[344] MHR Act s 97.

A third mechanism for clarifying statutory meaning is to publish a regulatory guidance policy or manual that outlines matters that the regulator may consider when exercising its powers. A relevant example is the Office of the Australian Information Commissioner (OAIC) *Privacy regulatory action policy* (2018). The publication of a regulatory guide can open a dialogue with those whose conduct may be regulated.

The Agency already publishes an extensive range of guides that are tailored to the needs of the different communities that it interacts with. Consideration could be given to elaborating on the meaning of 'security' and 'integrity' in either a new or an existing guide. Recommendation 31 below is to that effect.

Based on those considerations, this review does not recommend that the terms 'security' and 'integrity' be defined in the MHR Act. The indefinite meaning of those terms may be less of an issue if (as recommended above) the data breach notification scheme in the MHR Act is amended to remove any reference to security and integrity.

Additional powers to safeguard security and integrity

The Agency proposes that explicit authority be conferred on the System Operator to disconnect any clinical software connected to the MHR system that may compromise its security or integrity.

It is understandable that the System Operator should have such a power. However, a threshold issue is whether that power is currently lacking or, for example, is covered by the incidental power in the MHR Act.[345] A tenable view is that removing a threat to the security or integrity of the MHR system is incidental or conducive to the System Operator's specific functions of establishing and maintaining that system.

For that reason, no recommendation is made at this stage that the MHR Act be amended along the lines suggested.

Definition of 'My Health Record system'

The MHR Act defines the term 'My Health Record system'[346] as a system comprising 3 elements:

- the collection, use, disclosure and retention of information in accordance with a healthcare recipient's wishes or as specified in the MHR Act
- assembling that information so that it can be made available, in accordance with a healthcare recipient's wishes or as specified in the Act, to facilitate provision of health care to the recipient or for other authorised purposes
- the performance of functions by the System Operator.

The Agency submission proposes that the boundaries of this definition be clarified, as the System Operator has numerous obligations under the MHR Act that relate to the MHR system.

This proposal may need further explanation as to the practical problems the current definition poses for the System Operator. There may be other ways of addressing any such problems – such as an MHR rule or regulation that describes more extensively how and when the System Operator's responsibilities are to be discharged. Several recommendations in this report support the need for a less complicated and more explanatory MHR framework.

Definition of 'National Repositories Service'

A function of the System Operator is 'to operate a National Repositories Service that stores key records that form part of a registered healthcare recipient's My Health Record'.[347]

---

[345] MHR Act s 15(o), discussed in Chapter 4.
[346] MHR Act s 5.
[347] MHR Act s 15(i).

The Agency submission proposes that it be made clear that the National Repositories Service can include various parts.

The statutory term 'Repositories' (rather than 'Repository') suggests that a division into parts (or multiple registries) is already permitted. For that reason, no recommendation is made at this stage that the MHR Act be amended along the lines suggested.

Definition of 'the Register'

A function of the System Operator is to establish and maintain the Register,[348] which 'may be maintained in electronic form and may be divided into separate parts'.[349]

The Agency submission comments that this definition is circular and should be clarified.

This proposal may need further explanation, as the circularity is not apparent.

Definition of 'use' of health information

Many provisions of the MHR Act refer to the 'use' of health information included in a person's MHR. That word is defined in the MHR Act to include accessing, viewing, modifying and deleting the information.[350]

The Agency submission proposes that the definition should exclude the process adopted by the System Operator of de-identifying information. The rationale is not explained, but presumably it is to take the de-identification process outside the operation of regulatory controls that would otherwise apply, such as the provisions of the MHR Act that specify when a participant is authorised to use health information.[351]

The proposal to redefine 'use' is endorsed in Recommendation 33 below as a matter that warrants further consideration in reviewing the MHR Act. The following 3 matters should be noted in any consideration process.

First, the term 'use' also appears extensively in the *Privacy Act 1988* (Cth) but is not defined in that Act. There is benefit in the term having a consistent meaning and operation in both the MHR Act and the Privacy Act. Any redefinition of 'use' for MHR Act purposes should consider that overlap.

Secondly, a common phrase in both the MHR Act and the Privacy Act is 'use or disclose'. The term 'disclose' is not defined in either Act. The OAIC Australian Privacy Principles (APPs) guidelines[352] note that in most situations it is unnecessary to distinguish 'use' from 'disclosure', as the same actions frequently come within both terms.

Thirdly, there is a separate definition of 'use' in s 71AA of the MHR Act that was added as a parliamentary crossbench amendment to the Act in 2018. Recommendation 33 proposes that this separate definition be deleted as anomalous and potentially confusing.

---

[348] MHR Act s 15(e).
[349] MHR Act s 56.
[350] MHR Act s 5.
[351] MHR Act Pt 4, Div 2, Sub-div B.
[352] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines* (July 2019) para B.142.

Shared health summary prepared by a nominated healthcare provider

The MHR Act makes special mention of the shared health summary, in anticipation of it being a key document that will provide a holistic health overview at a particular point in time of a patient's medical history.[353] A shared health summary commonly includes information on a patient's medical conditions, medications, immunisations, allergies and adverse reactions.

The MHR website attests to the importance of the shared health summary, observing that it 'is likely to be the first document accessed by any other healthcare professional viewing a patient's My Health Record'.[354] A participation requirement for the Practice Incentives Program eHealth Incentive (ePIP), which provides an incentive payment for participating general practices to use the MHR system, is that a practice upload a shared health summary for a minimum of 0.5% of the practice's standardised patients each quarter.

The MHR Act provides that a shared health summary can be prepared only by a healthcare recipient's nominated healthcare provider.[355] Three features of the definition of 'nominated healthcare provider'[356] have been questioned:

- ***Who can be a nominated healthcare provider?*** The only health professionals who qualify to prepare a shared health summary are registered medical practitioners, registered nurses, Aboriginal or Torres Strait Islander health practitioners with a specified qualification, or a class of individuals specified in the Regulations.

  There are competing views on whether that restriction is appropriate. On the one hand, it is supported by the Australian Medical Association (AMA) and the Royal Australian College of General Practitioners (RACGP).[357] Their view is that preparation of a shared health summary is appropriately the responsibility of a health practitioner who is likely to have an ongoing clinical relationship with the patient and a broader familiarity with their health status. Prepared by such a group, the shared health summaries are more likely to be consistent and reliable over time.

  The option available to other categories of healthcare provider is to upload an event summary that can share information about a significant clinical event relating to an individual and include information such as medicines, diagnoses, immunisations, allergies and interventions.

  On the other hand, there is a view that expansion of the range of eligible providers is likely to increase the number of shared health summaries uploaded to the MHR system. Other professional groups can play a significant role in providing primary health care to consumers. An example is midwives, who are not registered nurses but form a large and growing profession that is represented by the Australian College of Midwives and who provide an essential maternity service to many women. (The AMA and RACGP submissions said a better option may be the development of a national digital pregnancy health record linked to MHR, which is being led by Queensland.)

  A few submissions also argued for recognition of other groups that could author a shared health summary, such as pharmacists.[358]

- ***How many nominated healthcare providers can a healthcare recipient have?*** The singular expression 'nominated healthcare provider' suggests that there can only be one such provider at any point in time.

---

[353] MHR Act s 10.
[354] Australian Digital Health Agency, My Health Record, 'Shared Health Summaries' www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/shared-health-summaries.
[355] MHR Act s 10; MHR Rule 2016, r 29.
[356] MHR Act s 5.
[357] Submission Nos 40 (AMA), 41 (RACGP). See also submission No 31 (Arnold).
[358] Submission Nos 19 (Defence), 27 (PSA), 37 (Pharm Guild).

This has been criticised as restrictive and at odds with healthcare consultation patterns. It is common nowadays that people consult a range of healthcare providers or consult different clinicians within a group medical practice.

- ***How is a nominated healthcare provider appointed?*** The nominated healthcare provider is defined in the MHR Act as a person who has 'an agreement in force' with the healthcare recipient to be the nominated healthcare provider for the purposes of the MHR Act.[359]

  There is no elucidation in the MHR Act of what form the agreement must take. The MHR website advises that the agreement can be verbal or written.

The ambiguity in the current procedure for nominating a healthcare provider was criticised in several submissions.[360] The uncertainty can hinder the upload of shared health summaries and deter a practitioner from stepping forward as the nominated provider. An element of the problem is that a provider cannot ascertain through the MHR system whether another provider has been nominated, and a patient may also be unsure on that point. A preferred option in some submissions was that a healthcare recipient could informally nominate a practice as the nominated provider.

As that analysis indicates, there are several elements to be considered in devising criteria and procedures for the upload of shared health summaries to MHR. It is possible that views on those elements may change over time.

It would therefore seem preferable that the criteria and procedures for preparation and uploading of shared health summaries can be defined (and redefined) in a flexible manner. The MHR Act currently provides that a regulation can be made to prescribe an individual or class of individuals as a nominated healthcare provider.[361] A more extensive and flexible option would be to amend the MHR Act to provide that a shared health summary may be prepared and uploaded in accordance with guidelines published by the System Operator. Recommendation 32 is to that effect.

Disclosure by the System Operator in relation to unlawful activity

The MHR Act specifies the circumstances in which participants are authorised to disclose health information included in a person's MHR.[362] One circumstance that applies specifically to the System Operator is that it may report suspected unlawful activity in relation to its own functions 'to relevant persons or authorities'[363] but can report 'only the information the relevant person or authority … needs to identify the matter or concerns' that may require investigation.[364]

The Agency's view is that further clarification of what can be disclosed is required. This proposal may need further explanation. The System Operator has additional authority, once an investigation has commenced, to disclose health information that it 'reasonably believes … is necessary for the purposes of an investigation of the matter'.[365] That broader authority to disclose may adequately cover areas of potential doubt.

---

[359] MHR Act s 5, definition of 'nominated healthcare provider'.
[360] For example, submission Nos 19 (Defence), 29 (MIGA), 35 (Avant), 37 (Pharm Guild), 40 (AMA), 14 (RACGP).
[361] MHR Act s 5, definition of 'nominated healthcare provider', para (c)(iv), and s 112(1)(a).
[362] MHR Act Pt 4.
[363] MHR Act s 70(3).
[364] MHR Act s 70(3A).
[365] MHR Act s 70(3)(b).

Notification of data breaches to the Australian Information Commissioner

With one exception, entities that are subject to the data breach notification scheme in the MHR Act must notify a data breach (as defined in the Act) to both the System Operator and the Australian Information Commissioner.[366]

The exception is that the MHR Act requires a state or territory authority to notify the data breach only to the System Operator.[367] The Agency submission proposes that the MHR Act specify whether the System Operator is in turn required to notify that data breach to the Australian Information Commissioner.

It appears that the obligation to do so is already implicit in the MHR Act. Section 75(3)(b) provides that the System Operator is to notify the Australian Information Commissioner of a data breach of which the System Operator 'becomes aware'. This is broad enough to encompass a data breach of which the System Operator has been made aware by a state or territory authority. On that basis, no clarification of the terms of the MHR Act would be required.

Enforceable undertakings and injunctions

The *Regulatory Powers (Standard Provisions) Act 2014* (Cth) sets out the criteria for exercising a standard range of regulatory powers. The exercise of those powers must be triggered by another statute that designates who is an authorised person to exercise those powers in a particular regulatory context.

The MHR Act provides that both the System Operator and the Australian Information Commissioner are authorised persons to exercise 2 standard regulatory powers – to accept an undertaking to comply with the MHR Act, which is then enforceable in a court;[368] and to apply for an injunction to restrain a person from contravening the MHR Act.[369]

The MHR Act does not explain the role of the System Operator in exercising those regulatory powers and, in particular, it does not explain which provisions of the MHR Act can be enforced by those powers. Nor does the MHR Act differentiate the roles of the System Operator and the Information Commissioner.

The Agency proposal that these matters be clarified is endorsed in Recommendation 33.

Delegation

The MHR Act authorises the System Operator to delegate a function or power under the Act to an APS employee in the Department of Health and to the Chief Executive Medicare.[370]

The Agency submission proposes that consideration be given to whether the System Operator should also have authority to delegate a function or power to 2 other bodies:

- the data custodian (the Australian Institute of Health and Welfare), which will play a key role in any scheme allowing MHR system data to be used for public health research[371]
- the Australian Commission on Safety and Quality in Health Care, which undertakes projects jointly with the Agency on clinical safety that aim to encourage more regular use of MHR by clinicians.

---

[366] MHR Act s 75(2)(d).
[367] MHR Act s 75(2)(c).
[368] MHR Act s 80(1); *Regulatory Powers (Standard Provisions) Act 2014* (Cth) Pt 6.
[369] MHR Act s 81(1); *Regulatory Powers (Standard Provisions) Act 2014* (Cth) Pt 7.
[370] MHR Act s 98(1).
[371] MHR Act s 109A(2).

This proposal is endorsed in Recommendation 33.

Organisation types in the MHR Act

The Agency submission notes that both the MHR Act and the *Healthcare Identifiers Act 2010* (Cth) adopt a similar prescriptive approach in authorising the collection, use and disclosure of information that an entity has acquired under the Act. The MHR Act defines the scope of authority to use information of each category of participant in the MHR system – healthcare provider organisations, contracted service providers, repository operators and portal operators.[372]

That approach lacks flexibility in several ways. It restricts those existing entities to using information in the specified way, often reinforced by a penalty for unauthorised use. It does not provide authorisation for information use by other categories of entity that are not specified – such as software vendors and primary health networks that support but do not provide health care. And it does not extend to new types of information flow.

The Agency's view is that this is an unsuitable approach to support digital innovation in the health system and to recognise other organisation types in the MHR system. An alternative approach would be a system of principles-based authorisations. That is the approach adopted in the *Privacy Act 1988* (Cth), which prescribes 13 APPs to regulate how personal information is to be managed.

The approach suggested by the Agency is one that can be explored further, as an appropriate topic for an Agency roadmap or strategic plan to cover future planning directions for MHR: see Chapter 3. A foremost challenge is to articulate the principles that will regulate how information can be used and to define the range of entities that are required to observe those principles. Another important issue is how to combine a principles-based approach with the current structure of the MHR Act, which imposes penalties for unauthorised use. Other regulatory mechanisms – of the kind available to the Australian Information Commissioner under the Privacy Act – may be more suited to a principles-based regulatory framework than penalties for breach of a principle.

Authorisations to contractors

The MHR Act authorises participants in the MHR system to undertake various activities – for example, to collect, use and disclose health information for the purpose of providing health care to a healthcare recipient;[373] or to disclose health information in a person's record to that person.[374]

The MHR Act clarifies the scope of those authorisations by indicating who can exercise them. For example, an authorisation to an entity can be exercised by an employee of the entity acting within the scope of their employment[375] or by contractor that is performing services for the entity under a contract that relates to the MHR system.[376]

The Agency submission makes 2 proposals on the extension of the authorisation to contractors:[377]

- the authorisation should also extend to subcontractors
- the MHR Act provision should apply not only to services provided under contracts that relate to the MHR system but also to memoranda of understanding.

---

[372] MHR Act Pt 4.
[373] MHR Act s 61.
[374] MHR Act s 66.
[375] MHR Act s 99(a).
[376] MHR Act s 99(c).
[377] The same revisions could also be considered to the *Healthcare Identifiers Act 2010* (Cth) s 36, which contains similar wording to the MHR Act s 99.

This proposal is endorsed in Recommendation 33. Consideration should also be given to whether supplementary legislative changes are necessary to ensure that a person exercising an authorisation pursuant to a memorandum of understanding is subject to the same obligations as the entity regarding the use and security of MHR health information.

Review of decisions

The MHR Act provides for internal reconsideration and independent AAT review of different categories of decision made by the System Operator[378] – such as:

- a decision that a person is not an authorised representative of a healthcare recipient
- a decision refusing to register a person in the MHR system, or varying, suspending or cancelling their registration
- a decision refusing to register a healthcare provider organisation or portal operator, or varying, suspending, or cancelling their registration.

Upon making such a decision, the System Operator is to provide written notice (if practicable) to a person affected by the decision. The person may apply within 28 days to the System Operator to reconsider the decision. The System Operator must do so within 28 days and provide written reasons for the decision. If the person is dissatisfied with the System Operator's decision, they may apply to the AAT for review of that decision.

The Agency submission raises 3 issues regarding the suitability of those arrangements.

The first issue is that it may not be practicable for some decisions to be reviewable. The example given in the Agency submission is a decision of the System Operator to cancel a person's MHR registration to resolve an administrative error, such as a duplicate Medicare enrolment and Individual Healthcare Identifier (IHI). A decision of that kind can be appealed to the AAT under the general right of appeal against decisions by the System Operator cancelling a healthcare recipient's registration if satisfied that a person is ineligible to be registered.[379]

A difficulty in giving effect to the Agency proposal is that it would involve carving out a specific exception from a provision that is framed broadly. It is not uncommon that broadly framed rights of appeal can have an inappropriate operation in particular circumstances. That can usually be resolved efficiently through the reconsideration or appeal process.

For example, the System Operator's notice to a person whose registration is cancelled in order to resolve an administrative error could explain that there is a formal right to seek reconsideration of the decision but point to the unlikelihood of the decision being changed by that process. That view would be tested (and potentially affirmed) in the unlikely event that a person sought internal reconsideration or external AAT review of the cancellation decision.

A second issue raised in the Agency submission is that there may be situations in which it is impractical to notify a person of a proposed decision to cancel, suspend or vary their MHR registration. No examples were given.

The MHR Act requires the System Operator (except in cases of urgency) to provide a person with written notice of a *proposed* decision to cancel, vary or suspend and invite the person to make a submission in reply within the period specified in the notice.[380] Upon making an *actual* decision to cancel, vary or suspend, the System Operator is required to 'take such steps as are reasonably necessary in the circumstances' but is not required to do so if giving notice may 'put at risk the life, health, or safety of a person'.[381]

---

[378] MHR Act s 97.
[379] MHR Act s 51(2)(a).
[380] MHR Act s 53.
[381] MHR Act s 97(2), (2A). See also MHR Act s 53(4), requiring notice of a decision if notice of a proposed decision was not earlier given because of urgent circumstances.

An option to give effect to the Agency's proposal is to frame the obligation to notify a *proposed* decision in similar terms to the obligation to notify an *actual* decision – that is, for the System Operator to 'take such steps as are reasonable in the circumstances'. This option is endorsed in Recommendation 33 below.

A third issue is that a person may not have a right to seek either internal reconsideration or independent AAT review of a decision if the System Operator decides that giving notice of that decision would put at risk the life, health or safety of a person.[382] The right to seek reconsideration of a decision only applies if a person 'is given notice' of the decision.[383] The subsequent right to seek AAT review is a right to seek review of a reconsidered decision.[384]

There is no obvious way of resolving that lacuna so long as the System Operator can decide not to notify a person of an initial adverse decision. The person would still have the right to initiate action to overtake the decision – for example, to apply afresh for registration if the adverse decision had cancelled their registration.

Civil liability connected to the use of MHR

The submissions from the Agency and the AMA[385] stated that healthcare providers have expressed anxiety about their potential civil liability when accessing or relying upon a patient's MHR.

Under the tort of negligence, a clinician can be liable for loss or injury to a patient that is caused by the clinician's failure to provide reasonably competent medical treatment to the patient. Because the boundaries of negligence are not closed, it is possible that a clinician could face a civil liability claim for compensatory damages after accessing a patient's MHR. For example, the clinician may rely on an inaccurate entry in the MHR or fail to identify a relevant item of information among a large volume of MHR documents.

The anxiety is less about actual liability and more about the flow-on consequences of apprehended liability: that a claim will be made and have to be defended; that a clinician will minimise their legal risk by opting not to access a patient's MHR; or that a clinician providing emergency treatment will spend inordinate time examining the patient's MHR as a protection against legal risk.

Civil liability is commonly limited by statute on practical and public interest grounds to deter claims and provide reassurance to those providing services to the community. For example, a civil liability statute in most Australian jurisdictions[386] provides partial civil liability immunity for volunteers, food donors, good Samaritans and public authorities as regards their allocation of resources or failure to exercise regulatory functions; and for an apology to an injured person.

In principle, it is appropriate that the MHR Act should grant immunity to a healthcare provider for any civil liability that would stem from accessing a person's MHR in order to provide health care to them. There is a strong public interest in limiting the obstacles, real or imagined, to practitioner use of the MHR system. Recommendation 33 is to that effect.

It is important to note, however, that civil liability immunity clauses customarily attract probing analysis by legal and consumer groups, particularly as to the scope and conditions for the immunity. For example, an immunity clause should only apply in respect of civil liability exposure arising from a provider's access to a person's MHR and not any other actions of the provider. It would therefore be necessary, in implementing this proposal, to frame a draft immunity clause as a basis for further consultation.

---

[382] MHR Act s 97(2A).
[383] MHR Act s 97(4).
[384] MHR Act s 97(8).
[385] Submission No 40 (AMA).
[386] Eg *Civil Liability Act 2002* (NSW).

Disclosure relating to the provision of indemnity cover for an MHR system participant

The MIGA submission[387] drew attention to the unclear meaning of s 68 of the MHR Act. It provides that a participant in the MHR system may collect, use and disclose patient health information 'for purposes relating to the provision of indemnity cover for a healthcare provider'.[388]

The probable intention of s 68 is to authorise a participant – particularly a registered healthcare provider organisation – to rely upon MHR patient health information in responding to a complaint or civil proceeding against the healthcare provider.[389]

On that basis, MIGA proposes that s 68 should be expressed more clearly to refer to the use of MHR patient health information in a proceeding in which the provider's actions in providing health care to the MHR record holder are under scrutiny. MIGA's view is that the proceedings to which this applies should be cast broadly to include civil damages claims, disciplinary proceedings and hospital and health service administrative inquiries.

This proposal is endorsed in Recommendation 33.

Disclosure for professional regulatory and disciplinary purposes

The MIGA submission recommended that the provisions in the MHR Act authorising a court, tribunal or designated judicial officer to order disclosure of health information in a person's MHR should be widened in scope. There are 2 provisions:

- Section 69 authorises a court or tribunal to direct the System Operator to disclose health information to the court or tribunal for the purpose of proceedings before the court or tribunal that relate either to the MHR Act, to unauthorised access to MHR information, or to the provision of indemnity cover to a healthcare provider.
- Section 69A provides that a designated magistrate or judge may make an order requiring the System Operator to provide health information to a government agency in circumstances where the MHR Act prevents the government agency from exercising its coercive information-gathering powers to obtain health information that is required for a current agency matter, and disclosure to the agency would not unreasonably interfere with the privacy of the healthcare recipient.

MIGA proposes an additional power, exercisable by a professional board or council, to require the System Operator to disclose MHR health information that is relevant to a regulatory or disciplinary matter currently before the board or council regarding the actions of a healthcare provider in providing health care to a person. The rationale for this proposal is that disclosure of the health information could be required by a court or tribunal under s 69 if the particular professional matter was before that court or tribunal rather than the professional board or council.

A weakness in the MIGA proposal is that it would enable a non-judicial body of uncertain composition or stature to order disclosure in the same circumstances that a court or tribunal could do so. That would be a distinct change to the underlying privacy and security settings in the MHR Act.

---

[387] Submission No 29 (MIGA) p 8.
[388] The phrase is also used in s 69.
[389] The Explanatory Memorandum to the Personally Controlled Electronic Health Records Bill 2011 comments: 'This provision is intended to allow collection, use and disclosure for indemnity cover purposes regardless of whether the matter involves court or tribunal proceedings or is the subject of a complaint'.

The MIGA proposal may meet less objection if the order was made (as in s 69A) by a designated judicial officer requiring disclosure of the MHR health information to the professional board or council. A remaining problem nonetheless is that the MHR health information would be released into the hands of a non-government body that may not be subject, as a government agency would, to statutory privacy or secrecy obligations.

While MIGA has pointed to an incongruity in the MHR Act provisions on disclosure, there is no easy way of reconciling the incongruity consistently with underlying MHR principles.

Condition of healthcare provider registration – non-discrimination among patients

The MIGA submission[390] was critical of a standard condition that is imposed by s 46 of the MHR Act on the registration of healthcare provider organisations. The purpose of the condition is to prevent discrimination against healthcare recipients who do not have an MHR. A provider must agree to the non-discrimination condition to be eligible to be registered in the MHR system.[391] A breach of the condition after registration is a ground for suspension or cancellation of the provider's registration.[392]

There are 2 parts to the non-discrimination condition. A healthcare provider must not refuse to provide health care to a person or discriminate against them because:

- the person has not registered in the MHR system[393]
- the person has set access controls on their MHR.[394]

MIGA disagrees with only the second part of the condition. The reason given is that it conflicts with a principle of professional practice that (except in an emergency situation) a medical practitioner may refuse to provide healthcare services to a person who declines to provide necessary information to the practitioner. A person's MHR access control could pose the same barrier to relevant health information being made available to the practitioner.

MIGA's proposal is that this part of the condition should be qualified rather than removed. For example, the MHR Act could provide that a healthcare provider must not 'unreasonably' refuse to provide health care to a person on the basis that an access control prevents the provider from obtaining information that the provider believes may be necessary for the purposes of providing health care on a particular occasion.

There is merit in the MIGA proposal. It accepts that a non-discrimination condition should potentially apply to a refusal to provide healthcare services to a person who has an access control in place. There is good reason why a healthcare recipient may not want health information of a particular kind to be shared with a health practitioner who is consulted on an unrelated matter. Accordingly, the MIGA proposal directs attention to whether there is a reasonable basis for the practitioner's refusal to see a patient who has an access control in place.

Recommendation 33 is that MIGA's proposal should receive further consideration in any review of the MHR Act undertaken by the Department of Health.

---

[390] Submission No 29 (MIGA) p 8.
[391] MHR Act s 43(c).
[392] MHR Act s 51(3).
[393] MHR Act s 46(1).
[394] MHR Act s 46(2).

Reporting errors

The MHR Rule 2016 places an obligation on participants in the MHR system to notify the System Operator (within 2 business days of becoming aware) of a non-clinical MHR system related error in a record that has been accessed in the MHR system.[395] An example given in the MHR Rule 2016 is reporting of a record which appears to have been corrupted during upload to the MHR system.

The Agency submission suggests that this reporting procedure could be extended to other errors of which a participant becomes aware – for example, an error in relation to clinical safety.

It appears this could be done without amending the MHR Act. The System Operator may impose conditions on a participant when approving its registration in the MHR system.[396] A condition requiring the participant to report errors or defects in the operation of the MHR system would fall within the scope of the power to impose conditions. A reporting obligation of that kind would fall within the purposes of the MHR Act.[397]

Freedom of information

The *Freedom of Information Act 1982* (Cth) (FOI Act) applies to the Agency and to all documents in its possession, including MHR system data. It is therefore open to any person to make a request under the FOI Act to obtain access in documentary form to any of that information.[398]

The FOI Act provides an exemption if disclosure 'would involve the unreasonable disclosure of personal information about any person' and disclosure 'would, on balance, be contrary to the public interest'.[399]

It is likely that MHR health information would be exempt from disclosure under that provision (except to the record holder or their representative[400]). It is relevant that the Privacy Act provides that 'health information about an individual' is 'sensitive information' that gains added protection under the APPs.[401]

The possibility is nevertheless open that a third-party request for access to another person's MHR would succeed, at least in special circumstances. This is because of the discretionary criteria in the personal privacy exemption in the FOI Act: a document is exempt only if disclosure would be 'unreasonable' and 'contrary to the public interest' at the time the request is made. An FOI decision maker must also consider any submission by an FOI applicant as to their reasons for seeking access and their intended or likely use and dissemination of the information.[402]

As to some categories of personal information, the FOI Act puts beyond doubt that the information is exempt by giving effect to a secrecy provision in another statute.[403] For example, client personal information acquired by officers of Services Australia in the course of their duties is exempt from FOI Act disclosure.[404]

---

[395] MHR Rule 2016 r 30 (healthcare provider organisation), r 38 (contracted service provider), r 55 (repository or portal operator).
[396] MHR Act s 43(c) (healthcare provider organisation), s 48(b) (repository operator, portal operator, contracted service provider).
[397] Eg *Shanahan v Scott* (1957) 96 CLR 245, 250.
[398] *Freedom of Information Act 1982* (Cth) (FOI Act) s 11.
[399] FOI Act ss 47F(1), 11A(5).
[400] FOI Act s 47F(3).
[401] *Privacy Act 1988* (Cth) s 6, definition of 'sensitive information'.
[402] *'FG' and National Archives of Australia* [2015] AICmr 26.
[403] FOI Act s 38, Sch 3.
[404] *Health Insurance Act 1973* (Cth) s 130(1); *National Health Act 1953* (Cth) s 135A(1).

The Agency submission proposes that a similar approach be adopted for MHR system data. This would be consistent with the legislative and policy underpinnings of the MHR system which strive to protect personal health information through measures such as healthcare recipient access controls; penalty offence provisions; and tightly defined procedures for access, use and disclosure of MHR health information.

The Agency proposal for a special FOI exemption is endorsed in Recommendation 33. Two FOI Act options for achieving that result can be noted. The first option is to list the Agency in Schedule 2 as an exempt agency in relation to MHR system data. The second option is to devise a new MHR Act secrecy provision for personal health information that is then listed in Schedule 3 (there is currently no MHR Act secrecy provision akin to the secrecy provision that applies to officers of Services Australia). Either way, a tailored FOI exemption should apply only to MHR personal and health information and not to other documents relating to the administration of the MHR Act or created by the System Operator.

The Agency receives a small number of FOI requests each year – 54 in 2018–19 and 13 in 2019–20.[405]

Complaints process

A function of the System Operator is 'to establish a mechanism for handling complaints about the operation of the My Health Record system'.[406]

The MHR Act also applies the complaint mechanism in the Privacy Act to conduct that contravenes the MHR Act in connection with health information.[407] The Privacy Act has a 2-stage procedure for complaints alleging interference with privacy contrary to the APPs. The first stage is for a person to complain to the entity responsible for the conduct complained about.[408] If the person is dissatisfied with the response, the second stage is to complain to the OAIC.[409]

The Agency submission queries whether a similar independent complaint process should be established for non-privacy matters (for example, a complaint about clinical safety) and, if so, whether legislative authority is required for a new mechanism of that kind.

It is not apparent that such a step is needed. As to complaints about the conduct of the Agency (as System Operator), a complainant may approach the Agency in the first instance, and if dissatisfied, complain to the Commonwealth Ombudsman.[410] The same procedure would apply to a complaint about the actions of any other Commonwealth agency under the MHR Act.

As to complaints about the conduct of private sector bodies under the MHR Act, the Agency has authority as System Operator to prescribe a procedure allowing a person to complain to the System Operator if dissatisfied with how a private entity has handled a matter. The System Operator could in appropriate cases exercise its powers to suspend or cancel the registration of an entity or its access to the MHR system.

A person dissatisfied with how the Agency (as System Operator) had dealt with the matter could complain to the Ombudsman. The Ombudsman's jurisdiction extends only to the conduct of the Agency and not that of the private sector body – nevertheless, it provides an opportunity for an external oversight body to examine whether the conduct of the private sector body has been well handled by the System Operator.

---

[405] The figures are reported in the Agency annual reports, under 'External scrutiny'. Details of the requests are given in the Agency Disclosure Log on the Agency website.
[406] MHR Act s 15(j).
[407] MHR Act s 73.
[408] *Privacy Act 1988* (Cth) s 40(1A).
[409] *Privacy Act 1988* (Cth) s 36.
[410] *Ombudsman Act 1976* (Cth) s 5(1)(a).

It would also be open to the System Operator to establish a committee with external membership to play a role in reviewing complaints about private sector bodies and providing advice and recommendations to the System Operator. Legislative authority would be required if the external committee was to have a stronger and determinative role in complaint handling. However, before that step is taken, consideration should be given to whether there is already an effective external mechanism, such as a professional oversight and disciplinary process.

Statutory anomalies

The Agency submission lists several provisions of the MHR Act that are anomalous and warrant correction (a proposal that is endorsed in Recommendation 33):

- Section 6(1A) refers to 'a healthcare recipient aged under 18', whereas the subsection heading refers to 'Healthcare recipients aged under 14'. (This matter is discussed in Chapter 9.)
- Section 71AA extends the definition of 'My Health Record' for the purposes of Part 4, Division 3A of the Act to include an MHR that has been cancelled. That is incorrect, as the MHR Act authorises cancellation of a person's *registration* in the MHR system, not cancellation of a *record*.[411] Further, it may not be practicable to extend the definition of 'My Health Record' as done in s 71AA, as the assumption that a cancelled record still exists is incorrect. The System Operator is required to destroy any record of health information if a recipient requests the System Operator to cancel their registration in the MHR system.[412] (Section 71AA was added in 2018 as a parliamentary crossbench amendment.[413])
- Section 71AA contains a definition of 'use'. That term is already defined in s 5 of the MHR Act, in different but compatible terms. It may be confusing for the MHR Act to have 2 different definitions of a common term.
- Section 77 provides that repository and portal operators, and contracted service providers, must not hold or take outside Australia a record from the MHR system. It is possible that this prohibition could apply to technical information that may need to be provided to a foreign organisation that provides software or system support to an entity. A similar prohibition applying to the System Operator only applies to records from the MHR system that contain personal information about a healthcare recipient.[414]

Recommendations

The following recommendations are made to give effect to the findings reached in this chapter. As explained at the beginning of this chapter, the style of Recommendation 33 is that the Department of Health consider (and consult on) the desirability of the proposed legislative amendments, bearing in mind that many of them have not previously had exposure to wider analysis and commentary.

Recommendation 29

The MHR Act be amended to merge the provisions in Schedule 1 of the Act (introducing the opt-out model) with other provisions in the Act dealing with the same issues.

Recommendation 30

The *My Health Records (Assisted Registration) Rule 2015* be repealed for the reason that it is redundant following the implementation of the opt-out model. Consideration should be given to preserving r 8 of the Rule, which requires a healthcare provider organisation to exercise

[411] MHR Act s 51(1).
[412] MHR Act s 17(3).
[413] *My Health Records Amendment (Strengthening Privacy) Act 2018* (Cth) s 16B.
[414] MHR Act s 77(2).

reasonable care in making a declaration to support a healthcare recipient's assertion of parental responsibility for a person.

Recommendation 31

The Australian Digital Health Agency consider publishing more extensive guidance on how the terms 'security' and 'integrity' may be applied in the different contexts in which those words are used in the MHR Act.

Recommendation 32

The MHR Act ss 5 and 10 be amended to provide that the System Operator may publish guidelines that prescribe which registered healthcare providers may prepare a shared health summary and the procedure to be followed to upload the shared health summary to a healthcare recipient's MHR.

Recommendation 33

The Department of Health consider the desirability of amending the MHR Act to:

- exclude de-identification of health information in a healthcare recipient's MHR from the definition of 'use' in s 5 of the Act
- clarify the roles of the System Operator and the Australian Information Commissioner in exercising powers listed in the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)
- authorise the System Operator to delegate relevant powers to the data custodian (the Australian Institute of Health and Welfare) and the Australian Commission on Safety and Quality in Health Care
- provide that an authorisation that can be exercised under the MHR Act by a contractor can also be exercised by a subcontractor, and (in like circumstances) it can also be exercised under a memorandum of understanding as well as under a contract
- provide that the obligation of the System Operator under s 53 of the MHR Act to notify a healthcare recipient of a proposed decision to cancel, vary or suspend their MHR registration is an obligation to take such steps as are reasonably necessary in the circumstances to notify the proposed decision
- provide immunity in civil proceedings for healthcare providers in respect of action taken by a provider under the MHR Act to collect, use or disclose health information in a healthcare recipient's My Health Record for the purpose of providing health care to the recipient
- clarify the meaning of the reference in s 68 of the MHR Act to 'the provision of indemnity cover for a healthcare provider'
- provide that a healthcare provider organisation is in breach of the non-discrimination condition in s 46 of the Act only if the organisation unreasonably refuses to provide healthcare services to a person when an access control is in place
- exempt personal and health information in the MHR system from a request for access under the *Freedom of Information Act 1982* (Cth)

resolve the statutory anomalies in the MHR Act as listed above.

Appendix A: Terms of reference

LEGISLATION REVIEW TERMS OF REFERENCE

MHR Act 2012

The reviewer is to provide a report to the Minister by 1 December 2020.[415] The reviewer must:

a) Consider the extent to which the purpose of the Act is enabled by the legislation (including its rules and regulations), particularly in regard to:

   i. improved continuity and coordination of healthcare for healthcare recipients accessing multiple providers; and

   ii. enhanced availability and quality of a consumer's health and medicine information and its relationship to:

      - reducing duplication of treatment;
      - avoiding adverse events; and
      - the ability for consumers to participate more actively in their own healthcare.

b) Advise how the Act might be improved to better address;

   i. how consumers use the MHR system;

   ii. how health service providers and consumers interact with the MHR system and each other;

   iii. use of MHR data for research and public health purposes (with particular reference to the *Framework to guide the use of My Health Record system data for research and public health purposes*); and

   iv. trust and confidence in the system including appropriate exclusions for, and practical issues arising from, access by law enforcement and government agencies, employers and insurers.

c) Consider how the Act and its rules and regulations support:

   i. compliance and enforcement activities, and the effectiveness of penalties where these have been enforced;

   ii. the handling of complaints where these have been made;

   iii. the operation of the Act within the scope of the *Privacy Act 1988* and related laws; and

   iv. the effectiveness of the oversight role of the COAG Health Council.

d) Address the appropriateness, effectiveness and efficiency of the legislation and make particular reference to issues which have arisen as a result of the legislation, including but not limited to:

   i. the role of the Office of the Australian Information Commissioner, including its functions in overseeing the privacy and data handling aspects of the MHR system;

   ii. how the provisions regarding minors' information are addressed under the Act and the extent to which the Act interacts with related national, state or territory legislation;

   iii. whether the System Operator has sufficient authorisations to carry out its functions;

---

[415] This date was determined by the Act as the latest possible date for a review report to be provided to the Minister. 1 December 2020 is three years after the Minister made a Rule under Clause 2, Schedule 1 of the Act. The MHRs (National Application) Rules which rendered the MHR (MHR) an opt-out system commenced on 2 December 2017.

iv. the interaction of the Healthcare Identifiers Service with the MHR system (taking into account the findings of the 2018 Healthcare Identifiers Act and Service Review); and

v. access for healthcare providers whose ability to author Shared Health Summaries and become nominated healthcare providers in the MHR system is currently restricted.

e) Consult with and/or invite submissions from stakeholders with a demonstrated interest in the Act and the effect of its operation within healthcare settings.

f) Make recommendations for changes to the Act, or its rules and regulations, to support the MHR system enabling improved healthcare outcomes in line with the objective of the Act.

i. Outline where changes outside of the scope of MHR legislation review might be considered in order to better enable the MHR legislation to achieve its objectives, whether those changes are legislative or achievable through other means, regardless of whether those changes are solely a matter for Commonwealth action or not.

ii. Make interim recommendations during the review period if serious concerns or significant barriers are identified and such recommendations would enable urgent action to be considered by Government.

g) Any other matter that the reviewer considers relevant to the purpose of the review.

Appendix B: List of submissions

No	Submission	Category
1.	Anonymous (ID 732804315)	Healthcare consumer
2.	Anonymous (ID 632007670)	Healthcare consumer
3.	Anonymous (ID 693552023)	Healthcare consumer
4.	Anonymous (ID 401923221)	Healthcare consumer
5.	Anonymous (ID 898284201)	Healthcare consumer
6.	Anonymous (ID 857240879)	Healthcare consumer
7.	Anonymous (ID 125556554)	Healthcare consumer/advocacy
8.	Anonymous (ID 158125606)	Healthcare consumer/Primary Health Network
9.	Anonymous (ID 506791868)	Healthcare consumer/advocacy
10.	Shaheen Badat	Healthcare consumer/healthcare practitioner
11.	Anonymous (ID 118943824)	Healthcare consumer
12.	Anonymous (ID 326944697)	Healthcare consumer/industry and technology sector
13.	Anonymous– Requested not to publish	Healthcare consumer/healthcare practitioner
14.	Anonymous (ID 17346544)	Healthcare consumer
15.	Anonymous – Requested not to publish	Healthcare practitioner
16.	Advance Care Planning Australia (ACPA)	Advocacy
17.	Benjamin Krieg	Healthcare consumer
18.	WA Primary Health Alliance (WA PHA)	Healthcare provider/Primary Health Network
19.	Department of Defence (Joint Health Command) (Defence)	Government
20.	Jennifer Carroll	Healthcare consumer
21.	Val Fell	Healthcare consumer
22.	Public Pathology Australia (PPA)	Healthcare provider peak
23.	Australian Institute of Health and Welfare (AIHW)	Government
24.	Juanita Fernando	Healthcare consumer
25.	Telstra Health	Industry and technology sector
26.	The Society of Hospital Pharmacists of Australia (SHPA)	Advocacy/healthcare provider peak
27.	Pharmaceutical Society of Australia (PSA)	Healthcare practitioner/healthcare provider peak
28.	Australian Digital Health Agency	Government
29.	MIGA	Healthcare provider peak

30.	Australian Privacy Foundation (APF)	Advocacy
31.	Dr Bruce Baer Arnold (Independent)	Healthcare consumer/healthcare practitioner
32.	Anonymous – Requested not to publish	Healthcare consumer
33.	The Royal Australian & New Zealand College of Psychiatrists (RANZCP)	Healthcare provider peak
34.	Department of Health and Human Services Victoria (Victoria)	Government
35.	Avant	Healthcare provider peak
36.	Office of the Australian Information Commissioner (OAIC)	Independent Regulator
37.	The Pharmacy Guild of Australia (Pharm Guild)	Advocacy
38.	MLC Ltd	Insurance Organisation
39.	Anonymous – Requested not to publish	Anonymous
40.	Australian Medical Association (AMA)	Advocacy
41.	The Royal Australian College of General Practitioners (RACGP)	Healthcare provider peak

All information in this publication is correct as at December 2020