Department of Health & Department of Human Services joint submission to the Senate Standing Committee on Community Affairs: My Health Records System

14 September 2018

Introduction

This submission is provided by the Department of Health (the Department) and the Department of Human Services (Human Services) to inform the Senate Community Affairs References Committee's inquiry into the My Health Record (MHR). This submission provides a brief overview of the system, and addresses the Terms of Reference. The Australian Digital Health Agency (the Agency) is providing a separate submission to the inquiry in its capacity as the My Health Record System Operator[1], it's submission should be read alongside this submission.

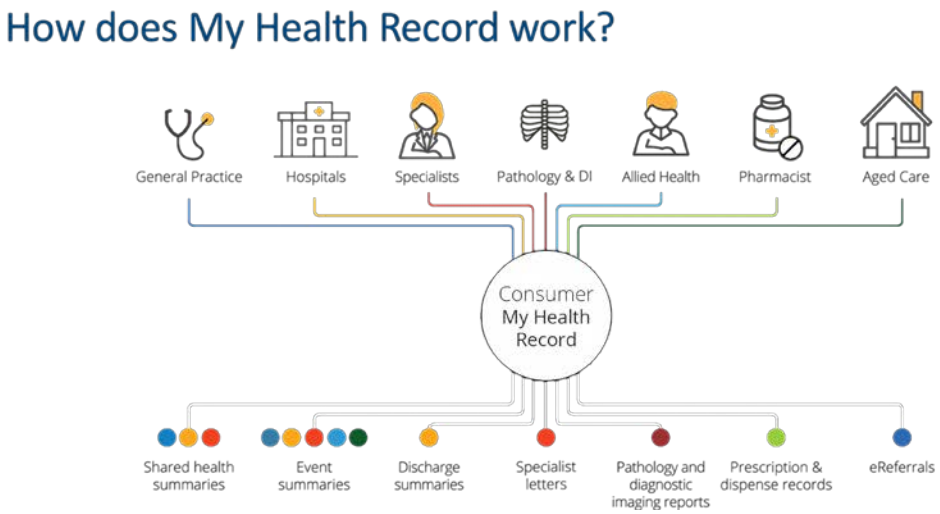
Background

What is My Health Record (MHR)?

The MHR is Australia's national digital health record system which has been operational since 2012. It is an electronic summary of an individual's key health information that can be shared securely online between the individual and their healthcare providers to support improved clinical decision making and continuity of care.

The MHR system enables the secure sharing of health information between a consumer's healthcare providers, while enabling the consumer to control who can access their record. Each MHR provides a view of the individual's information from distributed participating repositories (e.g. Medicare, Pharmaceutical Benefits Scheme) which hold summarised clinical information, as well as information directly provided by the healthcare provider.

The system is a key plank of modernising health infrastructure and connects key parts of the health system such as general practices, pharmacies, private and public hospitals, specialists and allied health professionals. It will improve co-ordinated care and health outcomes for individuals, and provide them with greater control and management of their health information.



[1] The System Operator has responsibility for operating the My Health Record system under a legislative framework that includes the *My Health Records Act 2012* and the *Privacy Act 1988*. The Australian Digital Health Agency is the My Health Record System Operator, as prescribed under the My Health Records Regulation *2012*.

Origin of the MHR

In June 2009, the National Health and Hospitals Reform Commission concluded a 16 month review of Australia's health system with publication of a final report *A Healthier Future For All Australians* which, among other things, recommended the implementation of a national personally controlled electronic health record to provide a central point to bring together an individual's health information from all parts of the health system.

The introduction of a personally controlled electronic health record for each Australian was identified by the *A Healthier Future for All Australians* report as an important systemic opportunity to improve the quality and safety of healthcare, reduce waste and inefficiency, and improve continuity and health outcomes for patients, as well as promote consumer participation, self-management and informed decision-making in their healthcare.

Known at that time as the Personally Controlled Electronic Health Record (PCEHR), the PCEHR was announced as a key component of the Government's national health reform agenda (*National Health and Hospitals Network for Australia's Future: Delivering the Reforms)* in the 2010-11 Budget.

In June 2012, the *Personally Controlled Electronic Health Records Act 2012* (PCEHR Act, now known as the MHR Act) took effect, and the PCEHR system began operating on 1 July 2012.

In November 2013, the Australian Government commissioned a review of the PCEHR to assess its implementation status and to work with health professionals and industry to prioritise further implementation.

The 2015-16 Budget announcement, 'My *Health Record - A New Direction for Electronic Health Records in Australia'* provided funding to strengthen eHealth governance arrangements consistent with the review. This included the transition of relevant activities and resources from the National E-Health Transition Authority (NEHTA), and also from the national PCEHR system operation activities managed by the Department of Health, to a new entity called the Australian Digital Health Agency (the Agency).

The review of the PCEHR also recommended that the PCEHR system be renamed. This recommendation was also actioned through the 2015-16 Budget, renaming the PCEHR to the My Health Record.

Foundational design

The initial design of the then PCEHR, was informed by international experience of implementation of electronic health record systems, and extensive public consultation.

A draft *Concepts of Operation*[2] was publicly released and consulted on in 2011, with refinements to the proposed implementation approach based on significant stakeholder feedback considered prior to the system commencing operation in July 2012.

The MHR system was designed to be implemented incrementally. Its initial focus was on building a strong infrastructure base, with a particular focus on overcoming interoperability problems to ensure computer systems from different health sectors can communicate structured clinical information with each other, strong system security provisions, and providing privacy protections sought by consumers.

The system commenced as a voluntary opt-in model for consumers and organisations (healthcare provider organisations, repository operators, portal operators and contracted service providers) meaning that any person or organisation wishing to participate in the system needed to register to participate in the system.

The MHR system is underpinned by two key pieces of legislation: the *Healthcare Identifiers Act 2010* (HI Act) and the *My Health Records Act 2012* (MHR Act).

The HI Act implemented a national system (the Healthcare Identifiers Service) for consistently identifying consumers and healthcare providers. It sets out clear purposes and restrictions for which healthcare identifiers can be used.

Using an individual healthcare identifier provides a way for healthcare providers to more accurately match the right records to the person they are treating and improve accuracy when communicating information with other healthcare providers. This helps to avoid medical mix-ups or one person's information being recorded on another person's file. Healthcare identifiers are part of the core national infrastructure required to support secure electronic communications across Australia's healthcare system.

The MHR Act established the MHR system. It provides a regulatory framework, delineates roles and responsibilities for operation of the system and provides a privacy regime specific to the system that generally operates concurrently with Commonwealth, and state and territory privacy laws.

Division of roles and responsibilities

The Agency is the MHR System Operator, as prescribed under the My Health Records Regulation 2012.

The Department is responsible for the policy direction and legislation that supports the operation of the MHR system, including decisions on the use of the system.

Human Services delivers MHR functions under an agreement with the Agency, including ICT infrastructure and provider registration and enquiry services. The agreement was signed on 30 June 2016, and sets out the agreed services and functions to be delivered by Human Services on behalf of the Agency for the MHR system.

[2] National E-Health Transition Authority, *Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record (PCEHR) System.* September 2011.

The Council of Australian Governments (COAG) Health Council, (through an Inter-Governmental Agreement) is the governance mechanism through which the Commonwealth, the Agency, and the states and territories work collaboratively to identify and agree national priorities for the MHR, and the broader digital health environment.

These priorities form the basis of *Australia's National Digital Health Strategy – Safe, Seamless and Secure (2018-2022)* and Work Programme, which outlines the implementation activities governments and the Agency will undertake to support these priorities.

Current Status

The Agency publishes regular reporting on a range of statistics about how the MHR is being used by healthcare provider organisations and consumers. As at 2 September 2018, the MHR had:

- 6,105,536 registered consumers;
- 13,708 registered health care provider organisations;
- 7,362,529 clinical documents uploaded;
- 23,363,409 prescription and dispense uploads;
- 196,174 consumer documents; and
- 762,338,468 Medicare documents.

Extension of Opt-out Period and MHR Act amendments

The Australian Government announced the decision to transition to an opt-out participation model as part of the 2017-18 Budget.

The opt-out period commenced on 16 July 2018, and was initially intended to run for a period of three months. On 9 August 2018, it was extended by one month, now ending on 15 November 2018. This extension will provide consumers with additional time to consider if they wish to opt-out of having a MHR created for them.

On 31 July 2018 the Minister for Health announced the Government would seek to strengthen the privacy framework of the My Health Record.

The My Health Records Amendment (Strengthening Privacy) Bill 2018 (the Bill) will specifically:

- remove the ability of the My Health Record System Operator to disclose health information in My Health Records to law enforcement agencies and government agencies without an order by a judicial officer or the healthcare recipient's consent; and
- require the System Operator to permanently delete health information stored in the National Repositories Service for a person if they have cancelled their registration with the My Health Record system – that is, they have cancelled their My Health Record.

Terms of Reference

This submission will now address each of the Inquiry's Terms of Reference.

(a) the expected benefits of the My Health Record system:

There is a growing amount of local and international research available showing the positive impact of electronic health records in delivering higher quality, safer, more accessible and more efficient healthcare. The opt-out trials undertaken in 2016 have also contributed to this evidence base.

Benefits for the consumer and their healthcare providers

A MHR puts consumers at the centre of their healthcare by enabling access to their key health information privately and securely, when and where it is needed, by the consumer and their healthcare provider. This will result in:

- improved continuity of care for healthcare recipients accessing multiple healthcare providers by enabling key health information to be available when and where it is needed for safe ongoing care;

- access to consolidated key health information about a healthcare recipient's medicines, leading to safer and more effective medication management and reductions in avoidable medication-based adverse events;

- enabling healthcare recipients to participate more actively in their own healthcare through improved access to their health information;

- improved diagnostic and treatment capabilities through enhanced access to health information; and

- improved care coordination for healthcare recipients with chronic or complex conditions by enabling the healthcare recipient's healthcare team to make better-informed decisions at the point of care.

Benefits of secondary use of My Health Record system data

The MHR Act provides that a consumer's MHR information may be collected, used or disclosed for any purpose with the consumer's consent. Further, a function of the System Operator is to prepare and provide de-identified data for research and public health purposes.

In May 2018, the *Framework to guide the secondary use of My Health Record system data* (the Framework) for research, policy and planning purposes was approved and released by the Minister for Health. The Department developed the Framework following national consultations including workshops in 13 locations around the country and two national webinars. This was followed by validation activities with industry experts, peak bodies and government to ensure a robust policy framework was achieved, balancing privacy and public benefit.

The purpose of the Framework is to guide the use of My Health Record system data for research and public health purposes. It will be applied by the My Health Record Secondary Use of Data Governance Board when making decisions about granting access to, and making available, My Health Record system data.

Custodianship of MHR data for secondary uses (for research and health purposes) rests with the Australian Institute of Health and Welfare (AIHW). The AIHW will be represented on the MHR Secondary Use of Data Governance Board (the Board). It will be the role of the Board to make decisions on applications for access to, and release of, MHR system data. Above all, the Board will ensure that MHR data is safe, that measures are in place to protect the privacy of individuals' health information, the quality of the data can be trusted and there are assurances around the release of data.

Other representatives will include the Agency (as the System Operator) and experts from population health/epidemiology, research, health services delivery, technology, data science, data governance and privacy, and consumer advocacy.

The use of data released in accordance with the Framework for research purposes has the potential to lead to new insights into the effectiveness and safety of medical treatments and clinical care across Australia's health system. It can assist with identifying service gaps resulting in the development of government health policies, improvement of existing health services, development of new health services and addressing any workforce gaps.

The Framework covers secondary use of de-identified data and the use of identifiable data with the consent of the healthcare recipient. Under the Framework, MHR system data cannot be used solely for commercial and non-health-related purposes. The provision of MHR data to insurance agencies is not permitted.

The first release of data for research or public health purposes is expected to commence from 2020 subject to establishment of the Framework's governance arrangements.

(b) the decision to shift from opt-in to opt-out:

A review of the PCEHR was undertaken in late 2013 by a panel of health and IT experts. The *Review of the Personally Controlled Electronic Health Record*[3] (the Review) was led by Mr Richard Royle, Executive Director, Uniting Care Queensland and supported by Dr Steve Hambleton, then President, Australian Medical Association (AMA), and Mr Andrew Walduck, Chief Information Officer, Australia Post. The Review examined issues with the existing PCEHR system including complexity, expectations and governance. The final report was released in May 2014.

The Review found strong support for a nationally shared electronic health record system which is usable and delivers real benefits, and made 38 recommendations aimed at realising the full benefits sooner for the individual, Australian public and healthcare system.

A key recommendation of the Review was moving to opt-out participation arrangements for individuals as the most effective way of achieving participation of both healthcare providers and individuals in the system, and through this delivering the objective of improving health outcomes. Additional recommendations and findings from the Review can be viewed in the Report.

Consultations were undertaken in mid-2014 with key stakeholders including healthcare providers, consumers and the health IT industry on the recommendations of the Review to better understand the complexities associated with implementing the recommendations. The consultation process was completed in mid-September 2014. Overall, there was broad support for the concept of a national shared electronic health record and for the recommendations of the Review.

The shift from opt-in to opt-out participation arrangements is consistent with broader international experience of successful implementation of electronic health record systems, and was supported by consumers and a wide range of peak bodies representing healthcare providers and other stakeholders throughout consultations.

While the Review recommended moving straight to national opt-out arrangements, the Government decided to trial opt-out arrangements first to confirm community acceptance and support of opt-out arrangements, and improve health outcomes.

2016 – Participation trials

From March to October 2016, trials of different participation arrangements were run. Opt-out arrangements were trialled in Northern Queensland, and the Nepean Blue Mountains area of New South Wales. Different approaches to opt-in were trialled in Western Australia and Ballarat. The aim of the trials was to understand consumer reaction to different participation arrangements, as well as healthcare provider use of the system, when most of their patients have a MHR.

The evaluation report (the Report) of the participation trials found there was a high level of support from both individuals and healthcare providers for the automatic creation of MHRs (opt-out). The Report found most individuals were positive about automatic creation once the process was explained and the benefits of the MHR system were understood. The Report noted participants considered not having to actively do anything to create a MHR as a benefit.

The Report concluded that, based on the data available to the evaluation, a national opt-out approach was not only acceptable to individuals, healthcare providers, participating health service and health department managers, but it was seen by participants as the only sustainable and scalable approach.

On 24 March 2017, COAG Health Council indicated support for a national implementation of opt out participation in the MHR system. The Australian Government announced the decision to transition to an opt-out participation model as part of the 2017-18 Budget.

(c) privacy and security, including concerns regarding:

i. the vulnerability of the system to unauthorised access;
ii. the arrangements for third party access by law enforcement, government agencies, researchers and commercial interests; and
iii. arrangements to exclude third party access arrangements to include any other party, including health or life insurers.

My Health Record privacy framework

The MHR legislation (i.e. the MHR Act and the HI Act) establishes a privacy framework for the MHR system that is largely based on the handling of information permitted by the *Privacy Act 1988*. The framework contains some additional access restrictions to reflect the unique nature and sensitivity of information that can be held in a MHR. These restrictions are further enhanced in the legislation currently before Parliament. Existing privacy and health information laws are leveraged to the extent possible and jurisdictional privacy laws are allowed to operate unless they are inconsistent with this framework.[4]

In terms of consumer privacy control, the *My Health Records Rule 2016* sets out the access controls the System Operator is required to provide to consumers. It specifies the default settings that apply to every My Health Record created (e.g. that any registered healthcare provider organisation involved in the consumer's care can access, that the consumer can remove documents, and that the consumer can elect to be electronically notified when a third party accesses) and advanced settings that a consumer can choose to apply. Theses settings enable a consumer to set a code to limit access to their whole MHR and to particular documents in it, and to prevent clinical information systems from automatically checking where a consumer has a MHR.

The Australian Information Commissioner is the key regulator for the system and has the capacity to conduct audits, undertake investigations and impose a range of sanctions, accept enforceable undertakings and investigate complaints.

Review

The MHR Act, when it was introduced into the Parliament in 2011 at that time known as the Personally Controlled Electronic Health Records Bill 2011, was the subject of a Senate inquiry. The report recommended several changes to the Bill which were largely made before the Bill was passed and enacted.[5]

In November 2013 the then Minister for Health announced a review of the system[6], prior to the Government's decision about the future direction of the program. The review report, which included consideration of the participation model (i.e. opt-in

[4] To recognise state and territory privacy interests and preferences, some provisions of state privacy laws were preserved (see subclause 9(3) of Schedule 1 to the MHR Act).
[5] The change recommended but not adopted related to the inclusion of preventative health in the definition of "healthcare" – changes were subsequently made to this definition in 2015.
[6] A statutory review of the system was required to be undertaken in 2014; however this was not undertaken since it would have unnecessarily duplicated the PCEHR Review in terms of scope and expenditure.

versus opt-out), made 38 recommendations including the system transition to an opt-out model – a majority of the recommendations were accepted.[7]

In 2015 when amendments were proposed to be made to the MHR Act (by the *Health Legislation Amendment (eHealth) Bill 2015*) to, among other things, enable an opt-out model to be implemented, a Senate inquiry was undertaken. The report recommended the Department consider recommendations made by the Office of the Australian Information Commissioner (the Information Commissioner) regarding privacy in developing the public awareness campaign about the opt-out trial. Accordingly, the Commissioner's recommendations informed the development and implementation of the participation trial communications in 2016.

The MHR Act requires that the MHR System Operator and the Information Commissioner deliver annual reports on the system insofar as it relates to their functions. For example, the Information Commissioner needs to report on the number of complaints and investigations relating to the system, and the System Operator must report on the number of consumers and other entities registered in the system, and the use of the system.

The MHR Act also requires that a review of the operation of the Act be undertaken and reported to the Minister for Health by 1 December 2020. The report must be tabled in Parliament and shared with state and territory health ministers.
The MHR system has been the subject of numerous privacy impact assessments, the first undertaken in 2011 while the system and the governing legislation was being developed. On each occasion a new functionality is added to the system which changes information flows, an assessment is undertaken. The 2011 assessment and the assessment of the opt-out model are available on the My Health Record website along with responses.

As a foundation of the MHR system, the Healthcare Identifiers Service has also been the subject of ongoing review. A Senate inquiry was undertaken when the proposed legislation was introduced into Parliament, a statutory review was undertaken in 2013[8], and the next statutory review is required to be completed by the end of 2018.

Consent under opt-out

The MHR system does not operate with any assumed or implied consent. The system recognises the importance of voluntary consent so where consent is required, express and informed consent is sought.

In order to transition to an opt-out model of participation, the MHR system will operate as a new individual consent. The MHR Act will authorise registered healthcare provider organisations to upload information except when a consumer expressly requests that a particular record or type of record not be uploaded, or if the organisation was prohibited from doing so by a jurisdictional law preserved by the MHR system unless they obtain consent in a specific manner.

[7] The government did not accept recommendations for a new regulatory body to monitor and ensure compliance against System Operator standards – opting instead to encourage inclusion of standards in software to improve sharing of information.

[8] The report of this review is available on the Department of Health website.

The MHR Act also authorises the Chief Executive Medicare to provide a consumer's Medicare-held information for inclusion in their MHR. A consumer can turn off this functionality if they wish not to include it.

A new functionality has also been included in the MHR system which allows a consumer to choose not to have their de-identified information used for research and policy planning purposes. Under no circumstances will identified information be used for these purposes unless the consumer gives express consent for a particular use.

i. the vulnerability of the system to unauthorised access:

The MHR system complies with all relevant government privacy, security and cyber security standards.

The misuse of information held by either the MHR system or Healthcare Identifiers Service, is prohibited and together with specified activities that relate to the security and integrity of the MHR system and Healthcare Identifiers Service, is subject to heavy penalties under the *My Health Records Act 2012* and *Healthcare Identifiers Act 2010* (Discussed below under *Penalties and sanctions*).

The *My Health Records Rule 2016* imposes additional obligations on participants in the system (i.e. the System Operator, a registered healthcare provider organisation, a registered contract service provider, a registered repository or a registered portal operator) to maintain a high security standard. These obligations include requirements to notify the System Operator of any system-related error encountered, to implement policies that address matters such as physical and electronic security measures, not to retain any access codes provided by consumers, and to ensure they employ certain restrictive user account management practices.

The Intergovernmental Agreement on National Digital Health requires the Agency to comply with the Australian Government's security and design standards (i.e. the Protective Security Policy Framework, Information Security Manual and Digital Service Standard). The MHR system also maintains multiple levels of security which are managed through the Agency's Cyber Security Centre.

The Australian Government's Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) manage governance, physical and information security, including information and communications technology systems. A directive issued by the Attorney-General in 2014 requires all agency leads to apply the PSPF which itself includes a requirement to comply with the ISM.

The Digital Service Standard (DSS) ensures government services are simple, clear and fast. All new and redesigned government services, whether information or transactional, and all existing, new or redesigned high volume transactional services, must be assessed against the DSS.

Penalties and sanctions

The MHR System Operator and the Information Commissioner have power to act against perpetrators of any unauthorised or non-compliant activity. Any unauthorised collection, use or disclosure of health information in a MHR is subject to heavy penalties – the civil penalty is up to $126,000 for an individual ($630,000 for a body corporate), and the criminal penalty is up to two years' imprisonment and/or up to $25,200 for individuals ($126,000 for bodies corporate).[9] Other sanctions available are enforceable undertakings, the imposition of conditions on a participant's registration, and injunctions.

Unauthorised or non-compliant activity may also attract penalties under other laws – for example, an action that is found to compromise a consumer's privacy may be subject to a penalty under the *Privacy Act 1988*, or an action that knowingly breaches restricted data may be subject to a penalty under the *Criminal Code Act 1995*.

This framework is complemented and reinforced by the professional obligations that apply to healthcare providers (e.g. the Ethical Guidelines for Doctors on Disclosing Medical Records to Third Parties 2010 (revised 2015)) regarding the protection of patient privacy and health information, and which may themselves lead to impose sanctions or consequences for improper activity.

ii. the arrangements for third party access by law enforcement, government agencies, researchers and commercial interests

Authorisations for the use, collection and disclosure of My Health Record data

A person or organisation can only collect, use or disclose health information in a consumer's MHR[10] if they are authorised to do so by the MHR Act. Consumers can collect, use and disclose information in their MHR for any purpose (section 67).

For participants in the system (ie. the System Operator, a registered healthcare provider organisation, a registered contract service provider, a registered repository or a registered portal operator), the MHR Act currently provides the following authorisations:

- for the purpose of providing healthcare to the consumer (in accordance with their access controls) (section 61);
- for the purpose of operating the MHR system (if reasonably expected) – for example, when a consumer accesses their MHR, the System Operator will obtain the consumer's health information from various registered repositories in order to compile that MHR (section 63);
- to lessen or prevent a serious threat to the consumer, and the consumer consent cannot reasonably be obtained – this authorisation limited to 5 days (section 64)[11];

[9] When the system began operating in 2012 a high civil penalty applied to the unauthorised collection, use or disclosure of this information. This penalty had the same value as those imposed by other Commonwealth laws such as the *Healthcare Identifiers Act 2010* (HI Act) to reflect the potential seriousness of the activity. In 2015 the civil penalty was increased by 500 per cent and a criminal penalty was introduced. These changes were made in response to some stakeholder concerns that the penalty was not severe enough, and to more closely align with the HI Act.

[10] A consumer's notes in their My Health Record cannot be collected, used or disclosed other than by or to the consumer.

[11] For example, if an individual arrives by ambulance to the emergency department of a hospital. They are unconscious and in a critical condition. The treating health care provider checks their identification to see if they have a MHR. The healthcare provider

- to lessen or prevent a serious threat to the public (section 64) [12];
- if authorised to do so by another Australian law (section 65);
- for any purpose with the consent of the consumer (section 66); or
- for purposes relating to the provision of indemnity cover for a healthcare provider (section 68).

A participant may also disclose information to the consumer and to the consumer's nominated representative (in accordance with their access controls) (sections 62 and 66).

In addition to the above authorisations, the System Operator can:

- disclose information if ordered to do so by a court or tribunal if the proceedings relate to the MHR Act, unauthorised MHR access or healthcare provider indemnity cover, or with the consent of the consumer (section 69);
- disclose information if ordered to do so by a coroner (section 69); and
- use or disclose information if the System Operator considers it is reasonably necessary for an enforcement body to undertake particular enforcement activities (section 70); and
- use or disclose information if the System Operator suspects unlawful activity in relation to the system and consider the information is necessary for investigation or reporting to authorities (section 70).

Participants in the system are also obliged to contribute to assuring the privacy of health information in a MHR, namely:

- registered healthcare provider organisations must provide enough information when accessing a consumer's MHR to enable the System Operator to identify the accessing individual (section 74);
- entities must notify the System Operator and Information Commissioner if there is an actual or potential unauthorised collection, use or disclosure of information, contravention of the MHR Act compromising the security or integrity of MHR system (section 75);
- entities must notify the System Operator that they are no longer eligible to be registered (section 76);
- entities that hold information for the purposes of the MHR cannot take or process that information outside Australia (section 77); and
- entities must comply with the My Health Records Rules (section 78).

A third party that is not a participant in the MHR system may be able to obtain health information from a consumer's MHR, however they do not have direct access to the MHR system. For example, the Information Commissioner cannot log into a consumer's MHR as part of an investigation of a privacy breach. Any request for information must be directed to the System Operator (or another participant), and the information can only be disclosed if the circumstances are under these authorisations.

---

discovers the individual does have a MHR and asserts to the System Operator that an emergency exists, and access to the individuals MHR is required.

[12] For example, where a dangerous infection has been detected within a hospital and it is necessary to identify the source of the infection to prevent its spread.

Medicare and PBS

The Deputy Secretary, Health and Aged Care Group in Human Services holds the statutory office of the Chief Executive Medicare and is responsible for a number of functions that support the MHR system. One of these functions include being a registered repository operator supporting the MHR system. A registered repository operator means a person that holds, or can hold, records of information for inclusion in the MHR system. The Chief Executive Medicare has unconditional registration as a repository operator for the MHR system, through a decision of the System Operator.

Human Services operates a data repository by providing agreed health program data, which is largely from the Medicare and Pharmaceutical Benefits Scheme (PBS) claiming systems, to the Agency for inclusion in the MHR system.

Unlike a MHR that can contain a person's clinical information added by their healthcare professional and personal notes added by the individual, Medicare and PBS data is only a record of claims made and paid to individuals or their healthcare providers and does not contain clinical information. For absolute clarity, Medicare and PBS claiming data is less than and different to, the full suite of information that can be captured in a person's MHR.

The Chief Executive Medicare has no legislative powers to access or release MHR information to a third party. The powers for the Chief Executive Medicare are governed by the *Health Insurance Act 1973* and the *National Health Act 195*3 which provide the legal authority to release Medicare and PBS claiming information in the Public Interest in certain circumstances.

Human Services can only release data under long-standing Public Interest Guidelines issued by the Secretary for Health to consider requests from law enforcement agencies seeking health programme information. These guidelines also cover requests from other authorities, such as child protection agencies and medical boards.

Data breaches

A data breach under the MHR Act is unauthorised collection, use or disclosure of health information in a consumer's MHR. Human Services has robust systems and procedures in place to identify and respond effectively.

There are two schemes for reporting data breaches:

- under the *Privacy Act 1988*, which mandates data breach notifications; and
- under the *My Health Records Act 2012*, which by definition is specific to MHR breaches.

Human Services works closely with OAIC and the Agency to ensure it complies with the requirements of both the *Privacy Act 1988* and the *My Health Records Act 2012*.

There have been no instances which have required Human Services to notify the OAIC of any data breaches under the Privacy Act since the start of the *Notifiable Data Breach* amendments in February 2018.

Data breaches reported by the Department of Human Services under the My Health Records Act 2012

The Chief Executive Medicare, as a registered repository operator, is required to notify data breaches to the OAIC under the MHR Act. A potential data breach or data integrity issue can arise when a person's MHR is populated with incorrect health program information sourced from the person's Medicare record. This can happen in the following ways:

- an intertwined Medicare record – this can occur when the Medicare record of a person has inadvertently been used interchangeably with another person with the same first name and surname, and incorrect claiming data then flows to the person's MHR; or
- fraudulent Medicare claiming, such that fraudulent Medicare claim data then appears in a person's MHR.

These events are rare. With over six million people registered for a MHR, these cases relate to an exceptionally small proportion of records – in the order of 0.0014 per cent. This equates to 82 cases since Human Services began reporting these in 2014. Since this time, no personal clinical information was misused.

Human Services has proactive compliance and data integrity programs to identify and investigate potential data breaches. All cases of potential data breaches are actioned immediately. The affected MHR consumers are notified and their MHRs are corrected quickly.

A data integrity issue can occur when a person's MHR is populated incorrectly, and Human Services reports this administrative error to the OAIC and the Agency as potential data breaches for their determination.

Other instances of incorrect claiming data in My Health Records

There have been some reports of incorrect PBS data being placed on a person's MHR. Human Services has investigated these cases and identified they are the result of a processing error by the claimant (the pharmacy) submitting the PBS claim under the wrong Medicare card number or having selected the wrong patient from the Medicare card. These are not defined as "data breaches" given they arise from an administrative error.

Once Human Services become aware of the event the healthcare provider is informed of the error, the claiming information in Human Services' health systems (Medicare/PBS system) is corrected. As a result, the corrected information flows to the MHR.

Strengthening privacy – proposed changes to legislation

On 22 August 2018, *the My Health Records Amendment (Strengthening Privacy) Bill 2018* (the Bill) was introduced in Parliament. The Bill proposes to require the System Operator to permanently delete health information stored in the National Repositories Service for a person if they have cancelled their MHR.

The Bill also proposes to remove the ability of the MHR System Operator to disclose health information in MHRs to law enforcement agencies and other government agencies without an order by a judicial officer or the healthcare recipient's consent. This means that the scope of some authorisations for the release of MHR system information listed above will be substantially reduced, specifically access, under the following sections of the MHR Act will require a court order under:

- section 65 (where another Australian law authorises the release of information); and
- section 70 (where the System Operator considers it reasonably necessary for an enforcement body to undertake particular enforcement activities, or where the System Operator suspects unlawful activity and considers the information is necessary for investigation or reporting to authority).

On 23 August 2018 the Bill was referred to the Senate Community Affairs Legislation Committee. The Department's submission to that inquiry is at **Attachment A** for your information.

iii. arrangements to exclude third party access arrangements to include any other party, including health or life insurers:

Under subsection 14(2) of the HI Act, healthcare providers and other entities are not authorised to collect, use or disclose a healthcare identifier for the purpose of communicating or managing health information of a healthcare recipient as part of:

- employing the healthcare recipient;
- underwriting a contract of insurance that covers the healthcare recipient;
- determining whether to enter into a contract of insurance that covers the healthcare recipient; or
- determining whether a contract of insurance covers the healthcare recipient in relation to a particular event.

The HI Act is critical to the operation of the MHR system. Healthcare identifiers are numbers that uniquely identify healthcare recipients (and providers). Like MHRs, healthcare identifiers are subject to stronger than usual privacy protections. Access to an individual's MHR is not possible without collecting, using or disclosing a healthcare identifier. The act of a healthcare provider accessing a healthcare recipient's MHR involves collecting the recipient's healthcare identifier using identifying information in the first instance, and then disclosing the healthcare identifier in order to obtain information held in the recipient's MHR.

The National eHealth Security and Access Framework for the MHR allows an individual to monitor who has accessed their MHR and when it was accessed. For example, through audit logs, a consumer can see what organisation has accessed their

MHR, including when they accessed the MHR, and whether they uploaded any additional documents.

The MHR Act also draws heavily on the existing provisions of the Privacy Act. As such, using or disclosing a healthcare identifier in order to access a healthcare recipient's MHR information as part of employment or insurance assessment is an offence and subject to severe penalties – as described above this can include up to $25,200 if not a body corporate and up to $126,000 for bodies corporate, and/or up to two years' imprisonment for a natural person. A person who uses or discloses a healthcare identifier in this way will also be liable to a civil penalty of $126,000 if not a body corporate and up to $630,000 if the person is a body corporate.

Under the *Framework to guide the secondary use of My Health Record system data* (the Framework*)*, the provision of MHR system data to insurance agencies is prohibited as are secondary uses that would be considered 'solely commercial'. Examples of 'solely commercial' uses are identified in the framework, and include:

- "direct marketing to consumers"; and
- "assessment of insurance premiums and/or claims."

A detailed description of the proposed ethics and approvals processes for the release of MHR data for research or public health purposes is contained in the Framework.

The first release of data for research or public health purposes is expected to commence from 2020, following establishment of the Framework's governance arrangements.

(d) the Government's administration of the My Health Record system roll-out, including:

iv. the public information campaign, and

v. the prevalence of 'informed consent' amongst users

Overview of the system roll-out

The Government's roll-out of the My Health Record system and communication with consumers and providers has been informed by extensive and regular consultation, including through undertaking the opt-out trials.

From 1 July 2012 to 30 June 2016 the System Operator of the then PCEHR was the Secretary of the Department of Health (the Department).

The Department was also responsible for the policy and legislation that supported the operation of the then PCEHR system. The Department was supported in the operation of the system by: Accenture, as the National Infrastructure Operator, and the Department of Human Services (Human Services), to provide the day to day operation and management of the PCEHR system, and The National E-Health Transition Authority (NEHTA), to establish the policy and ICT foundations to enable interoperability between providers and use of the PCEHR system.

Registration to the then PCEHR was opt-in. Individuals could register for an electronic health record by phone, face-to-face in Human Services service centres, by mail, online, or via assisted registration by healthcare providers. Consumer information on the benefits of a PCEHR and how to register for one was distributed through Medicare's communication channels.

In November 2013, the Minister for Health announced a review of the PCEHR by a panel of health and IT experts, to consider the implementation, uptake and use of the PCEHR system by consumers and healthcare providers.

The 2015-16 Budget, in response to the 2013 Review of the PCEHR provided for redeveloping the system to improve its usability and clinical utility, strengthen digital health governance and operations, and trial new participation arrangements.

The PCEHR was renamed the My Health Record and the the Agency was established to manage the governance, operation and ongoing delivery for digital health and commenced operation on 1 July 2016.

The 2017-18 Budget measure *A My Health Record for Every Australian* provides $374.2 million over two years to the Agency to support the expanded rollout of the opt-out model to all Australians, and continue to improve operations of the MHR system, with the Department providing ongoing support to the Agency through legislative and policy oversight.

Communications

The 2016 Evaluation of the Participation Trials, found that general consumer awareness of the MHR would be best supported by information being provided about My Health Record when they were in a healthcare setting, compared with mass communication such as letters sent to every household.

The current strategy, informed by the trials, focuses on delivering a nationally driven but locally supported campaign, where information is developed centrally, but media strategies and advertising run at a local level.

The Agency works in partnership with Primary Health Networks, the Australian Medical Association, the Royal Australian College of General Practice, the Australian College of Rural and Remote Medicine, the Consumers Health Forum, and other non-health channels to implement its national opt-out communications strategy.

Human Services supports the Agency by providing further options for communication activities through Human Services' existing channels during the opt-out period. Human Services' physical communication materials - including Agency-developed MHR posters and flyers - have been placed in the Human Services' service centres. MHR brochures have been included in high volume health programme customer letters. These include Medicare and Australian Immunisation Register correspondence (about three million letters).

Human Services' communication activities also include digital news articles for health professionals in periodical publications, messages on the Human Services' *Your Health* website and on the Medicare Online Account landing page. Social media promotion has also been included via myGov twitter feed.

Opt-out portal

To support the opt-out process, Human Services provided the opt-out portal and functions to enable people to opt-out securely online and through the Agency's staff-assisted channel. These functions have performed well with excellent performance results and no system capacity issues have been experienced.

Hard to Service

The 2016 opt-out trials identified certain individuals as 'Hard to Service' as they did not have access to mainstream communication channels and were unable to effectively exercise their choice to opt-out over the phone or online.

As part of the 2017-18 Budget, adult prisoners, juvenile detainees between the ages of 14 and 17 years, and Defence personnel deployed overseas were confirmed as 'Hard-to-Service'.

Under the auspice of the Corrective Services Administrative Council (CSAC), in 2017-18, the Department consulted with correctional services staff in all jurisdictions

to develop a strategy to ensure that adult and juvenile detainees are given the opportunity to opt-out if they do not want a MHR. Health also took advice from each state and territory about internal mechanisms available to communicate with prisoners in each jurisdiction (for example, Tasmania has a newsletter service for prisoners, while the ACT enables limited internet and email access).

The Department also consulted with the Department of Defence to determine the most appropriate way for Australians on military deployment to opt-out.

The strategy resulted in cohorts being provided with a bespoke opt-out mechanism as required, as well as communications materials tailored to their needs.

System enhancements

Human Services has also implemented new services for healthcare providers and healthcare organisations on behalf of the Agency for the expansion of the MHR system. The new services remove previous paper-based registration processes and introduce new digital services. This has reduced the amount of time it takes for providers to authenticate to the MHR provider portal (operated by the Agency) and for healthcare organisations to register with the Healthcare Identifiers Service (which is operated by Human Services and is a pre-requisite for accessing the MHR system).

ePIP Program

The eHealth Practice Incentives Program (ePIP) Incentive aims to encourage general practices to keep up to date with the latest developments in digital health and adopt new digital health technology as it becomes available. It aims to help practices improve administration processes and patient care.

The ePIP incentive was first introduced in 1999 and initially focussed on incentivising general practices to keep up to date with the latest developments in electronic health and adopt new information and communications technology, including clinical software systems.

These requirements were revised in 2013, and again in 2015, to encourage general practices to register for and connect to the MHR system.

(e) measures that are necessary to address community privacy concerns in the My Health Record system:

Stakeholder consultations

The Department and the Agency,[13] have consulted with stakeholders and the public on the development of a national electronic health record system since 2011.

Government response to concerns raised during the 2018 opt-out period

In August 2018 the Minister for Health extended the opt-out period by one month, to end on 15 November 2018. The Minister also introduced into Parliament amendments to the MHR Act to strengthen the privacy protections of the MHR system. Specifically, the *My Health Records Amendment (Strengthening Privacy) Bill 2018* (the Bill) will:

- remove the ability of the MHR System Operator to disclose health information in MHRs to law enforcement agencies and government agencies without an order by a judicial officer or the healthcare recipient's consent; and

- require the System Operator to permanently delete health information stored in the National Repositories Service for a person if they have cancelled their registration with the MHR system – that is, they have cancelled their MHR.

The Royal Australian College of General Practitioners (RACGP), the Australian Medical Association, the OAIC and the Australian Human Rights Commissioner were consulted in mid-August on an exposure draft on the proposed amendments.

Existing measures established under the MHR's policy and legislative frameworks are subject to ongoing review and reporting on operations of the system, to enable continuous consideration of concerns or issues being raised by system users, such as privacy concerns.

All health ministers reaffirmed their support for the MHR system and the opt-out model at the 2 August 2018 COAG Health Council meeting, and supported the strengthening of the privacy provisions of the MHR Act.

[13] The National E-Health Transition Authority was responsible for a large proportion of this consultation during its existence between 2005 and 2016.

(f) My Health Record compares to alternative systems of digitising health records internationally.

Other countries with electronic health record initiatives include Canada, Switzerland, China, Denmark, Germany, France, England, India, Israel, Italy, Japan, the Netherlands, Norway, New Zealand, Singapore, Sweden, Taiwan, and the United States.

Seven of these countries have a system which enables citizens to view their records through a national digital platform (like Australia) these include: Austria, Denmark, Estonia, Finland, France, Norway and Sweden. Of these seven, France is the only country to utilise an opt-in model.

While the broader aims for implementing national electronic health record systems have a similar rationale across countries (i.e. to use IT-enabled change to improve the quality, efficiency and sustainability of the country's healthcare) the type of system countries chose to implement is influenced by an array of contextual factors, including the structure, funding and ethos of the country's healthcare system, past experience, available technologies, the existing IT infrastructure and resources, and domestic economic factors.[14]

While approaches to implementation may differ, international comparisons show that there are common issues with the implementation of digital health initiatives, these include:

- overcoming interoperability problems to ensure computer systems from different health sectors can communicate structured clinical information with each other;
- coding patient clinical information at the time of entry; and
- managing the legal and practical concerns regarding privacy and confidentiality of patient information[15]

[14] Zoe Morrison, MSc1*; Ann Robertson, PhD1; Kathrin Cresswell, MSc1; Sarah Crowe, PhD2; Aziz Sheikh, FRCP. *'Understanding Contrasting Approaches to Nationwide Implementations of Electronic Health Record Systems: England, the USA and Australia and resources and, importantly, domestic political and economic factors.'*. Journal of Healthcare Engineering. Vol. 2, No. 1. 2011 . pp25–41.
15 National E-Health Transition Authority (NeHTA). *'Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record System'*. September 2011.URL: https://www.privacy.org.au/Campaigns/MyHR/docs/PCEHR_110912_Concept_of_Operations.pdf Last accessed 10/9/2018