Australian Digital Health Agency

Access To Source My Health Record Participation Data for Analytic Uses Solution

Privacy Impact Assessment

Final

19/07/2024

elevenM

Contents

Document control

Version	Date	Comments	Author
0.1	21/06/2024	Initial draft for ADHA review	elevenM
0.2	09/07/2024	Draft 2 for ADHA review	elevenM
1.0	19/07/2024	Final	elevenM

About this report

- In 2024, the Australian Digital Health Agency (**the Agency**) engaged elevenM (**we, us, our**) to deliver a Privacy Impact Assessment (**PIA**) on the access to My Health Record Data Analytics Platform/Capability participation source data for analytic uses, also known as Use Case 3 (**the solution**).
- This report contains our assessment against the laws detailed in our Scope (p 12). It is not legal advice.
- In the 'Privacy analysis' section of this report (p 17) we have made recommendations for management of privacy risk relating to the solution. These are summarised in the Executive summary (p 6).
- The Executive summary also contains recommended next steps for the Agency on acceptance of this report.

Executive summary

The Agency as the system operator of the My Health Record system (**MHR**) has engaged elevenM to undertake PIA to assess privacy risks associated with the handling of personal information for the National Participation (My Health Record Participation Data for Analytic Uses) initiative.

Recommendations

We have made 9 privacy recommendations in relation to this activity. These recommendations should be read in context with the analysis in the sections below.

Compliance recommendations

We have identified 3 Compliance recommendations.

COMPLIANCE REC. 1 The Agency must revise the MHR Privacy Policy to ensure that it is:

- up to date.
- open and transparent on how de-identified information will be used by the Agency and explain its purpose.

COMPLIANCE REC. 2 The Agency must identify and adopt appropriate de-identification methodologies to remove personal information including any health identifiers when cleansing data from different layers of the solution and take reasonable steps to minimise any risks of re-identification of data from publicly available sources.

COMPLIANCE REC. 3 The Agency must ensure that the on-going cyber security assessment is finalised after the solution has been completed and any risks arising out this assessment must be mitigated prior to the solution going live.

Best practice recommendations

We have made 6 Best Practice recommendations that are not compliance risks to the Agency but are worthy of being outlined in this context.

BEST PRACTICE REC. 1 The Agency should test how the data response plan applies to the new solution before going live in conjunction with the Risk Governance team.

BEST PRACTICE REC. 2 The Agency should change the location of the opt-out option within the MHR to be shown upon login, or within the first page of their record. Bringing the notice to the front of the MHR shows a level of transparency that will help support an informed decision for the individual.

BEST PRACTICE REC. 3 The Agency should consider implementing internal guardrails to ensure de-identified health information is not used for purposes that may be beyond what individuals may reasonably expect their health information to be used for.
BEST PRACTICE REC. 4 The Agency should ensure the existing data dictionaries for the three databases (OES, OSB and RLS) for this solution are complete and up to date to inform their understanding of the data in the solution and build robust data governance controls over the use of this data (including de-identified data) for all future secondary research and public health use cases.
BEST PRACTICE REC. 5 If there are any material changes to the technical solution or deviations from the proposed scope (including extraction of unstructured data), the use cases arising out of these modifications will need to be assessed through subsequent PIAs.
BEST PRACTICE REC. 6 The Agency should confirm the quality of information within the solution is high by ensuring any changes that occur in the MHR are reflected in the solution i.e. address details are updated, checking individuals who have deleted their MHR are not showing in the Solution.

Next steps

Under the *Privacy (Australian Government Agencies — Governance) APP Code* 2017 (Cth) (**Privacy Code**), Commonwealth Government agencies must conduct a PIA for all high-risk projects, and may publish the PIA, or a summary version or edited copy of it, on its website.[1]

This document is intended to satisfy any requirement to carry out a PIA under the Privacy Code.

Following receipt of this final version of this document, the Agency should:

1. Consider and respond in writing, at a senior management level, to the findings outlined in this document.
2. Ensure that the risks identified in this document are recorded and managed according to its risk management framework.
3. Ensure this PIA is included in the Agency's publicly available register of PIAs (as required under section 15 of the Privacy Code).
4. Consider publishing this document on its website or otherwise making its findings publicly available.

[1] See Privacy Code ss 12, 13.

Background

About the Agency

The Agency is a corporate Commonwealth entity established on 30 January 2016 under the *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016* (Cth) (Agency Rule). The Agency Rule establishes its functions, which are:

a) to coordinate, and provide input into, the ongoing development of the National Digital Health Strategy;
b) to implement those aspects of the National Digital Health Strategy that are directed by the Ministerial Council;
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;
e) to develop, monitor and manage specifications and standards to maximise effective interoperability of public and private sector digital health systems;
f) to develop and implement compliance approaches in relation to the adoption of agreed specifications and standards relating to digital health;
g) to liaise and cooperate with overseas and international bodies on matters relating to digital health;
h) such other functions as are conferred on the Agency by this instrument or by any other law of the Commonwealth;
i) to do anything incidental to or conducive to the performance of any of the above functions.

The Agency provides leadership, strategy and infrastructure to support Australia's move towards a more efficient and effective health system using digital technologies.[2] The Agency's responsibilities include the role of the MHR System Operator which can be viewed in *Annexure 1*.

MHR contains an online summary of a patient's health information and is designed to allow information about health recipients to be shared between health service providers. An individual's MHR is not one single 'record', but rather is a compilation of documents that health service providers have uploaded to the MHR. Discharge summaries, immunisation records and pathology and radiology records are examples of documents that an individual's MHR could contain.

As the System Operator, the Agency maintains and enhances the security and functionality of the MHR to encourage the digitisation of health services. It is estimated that around 90%

[2] The Agency's role is described in more detail in its Annual Reports. See, for example, https://www.transparency.gov.au/annual-reports/australian-digital-health-agency/reporting-year/2021-22-21.

of eligible Australians have a MHR since the system of 'consent' changed to an opt-out in early 2019, however a much smaller proportion of Australians actively use their MHR.[3]

About the solution

Rationale / benefits

The MHR National Participation (Healthcare Recipient and Provider Organisation Registration) and Usage Data to be extracted from the MHR source databases and ingested into the solution will maintain an up-to-date view of the participation levels of individuals, healthcare provider organisations and the types of activities that occur between them and the MHR at a national level.

The solution will involve the extraction of all MHR participation and system usage data (the registration, usage data and clinical documents metadata) for all healthcare recipients. The extracted data will be de-identified and used for the purposes of reporting and analysis. It is expected that this de-identified data will also be shared with Australian Institute of Health and Welfare (**AIHW**) as data custodian of MHR data for research or public health purposes (in the future). There could also be provisions for the data to be shared with the Department of Health and Aged Care (**DoHAC**) or other external stakeholders for additional purposes in accordance with other authorised functions of the System Operator.

Design

The infrastructure component of the technical solution is being built by DXC and the MHR data extraction engine by Accenture, the National Infrastructure Operators (**NIO**).

The solution is being built by the Agency to bring the reporting and analysis in-house and is currently in its design phase and therefore, this PIA is focused on a privacy by design approach, to embed privacy principles into the solution architecture.

The intent is to build a technical solution which will extract a copy of the national participation data from the MHR and ingest it into a cloud-based analytics platform. The national participation data refers to the demographic information of an individual, how the individual and health providers interact with the MHR (discussed in detail below).

The solution will hold information extracted from three main databases – Oracle Entitlement Server (**OES**), Oracle Service Bus (**OSB**) and Oracle Health Sciences Information Manager – Record Locator Service (**HIM-RLS**) which contain participation data, activity logs and metadata for clinical documents respectively.

There are three main layers in the solution – bronze, silver and gold. Data in the first layer (bronze) is ingested in its raw form. In the second layer (silver) this data is cleansed and separated into personal information (**PI**) and non-PI (de-identified) data. The de-identified data is then moved into the third layer (gold) to be enriched to be used for the purposes of analysis and reporting. Information (demographic and health information) about health

[3] https://www.theguardian.com/australia-news/2022/jun/06/my-health-record-after-12-years-and-more-than-2bn-hardly-anyone-is-using-digital-service.

recipients will also be shared with AIHW for the purposes of public health and research, however, this is not in scope for this PIA.

Social licence for this use of MHR data

When assessing the privacy risks of a new project or initiative, there needs to be consideration of the societal context in which they operate. Given the widespread use of the MHR across Australia, it is imperative to consider the community's expectations in relation to the use of their personal and health information.

When considering how an organisation manages and protects their personal and health information, the Australian public rate health service providers as the most trustworthy, followed by federal government departments.[4]

Due to the nature of the project, it is important to also look at a broader view to gauge community attitudes toward how the information is used, the purpose and who it is used by.

Australians feel significantly more comfortable about government agencies sharing information with other Australian government agencies, as opposed to instances where a government agency would share information with an Australian business.[5]

When considering the government's use of personal information, 40% of Australians feel comfortable for their data to be used for research purposes and policy development, as opposed to 27% who do not.[6] When the scope is narrowed to the use of medical records for research purposes, we see that this figure increases with a rate of 93% in support.[7]

However, we also note:

- 84% of Australians consider supplying information to an organisation for a specific purpose and the organisation using it for another purpose to be misuse.[8]
- the health sector has consistently had the highest number of notifiable data breaches every year since 2018.[9]

There is the general acceptance that the sharing of health data is a community good, that will benefit the community and drive positive growth and change. Due to this, in essence, there is an overall level of support for the sharing of health data for the approved research purposes, however, it must also be acknowledged that the information in question is of a sensitive nature.

We are of the view that this highlights the need for the Agency to ensure that it maintains a focus on MHR information security, the appropriate de-identification of data, and testing

[4] Australian Community Attitudes to Privacy Survey 2020 | OAIC.
[5] 40% are uncomfortable with inter government sharing of information, versus 70% being uncomfortable with a government agency sharing information with an Australian business, per Figure 11, Australian Community Attitudes to Privacy Survey 2020 | OAIC.
[6] Figure 18, i*bid* – 30% feel neither comfortable or uncomfortable with this use, and 3% do not know how they feel.
[7] Microsoft Word - RA Submission Sec Use FINAL.docx (researchaustralia.org)
[8] Australian Community Attitudes to Privacy Survey 2020 | OAIC.
[9] Notifiable data breaches publications | OAIC. **NOTE-** the health industry is subject to more stringent requirements under the National Data Breach scheme than any other organisations given the type of personal or sensitive information held, however it is still a noteworthy point for consideration.

occurs prior to use or sharing of data, as well as clear communication to the user about the way in which their data will be used, and who it will be shared with. This is discussed in more details in subsequent sections of this PIA.

Potential impacts of privacy law reform

With the privacy law reform on the horizon, it is important to note that there will be impact to Australian Government Agencies and how they collect, handle and protect personal information.

In respect to the solution, the following proposed reforms are relevant to the Agency:

- changes to the definition of personal information, which may require an adjustment to the Agency's de-identification processes;
- acknowledging the risks associated with one entity handling multiple datasets, the proposed application of certain privacy controls to data that has been de-identified; and
- an obligation on entities to ensure that not only collections, but also uses and disclosures of personal information would be considered 'fair and reasonable'.

While not in scope for this PIA, the future development and implementation of the solution should be guided by any such new obligations under the Privacy Act, should they pass into law.

Scope

This PIA report focusses on the privacy impacts that the introduction of the solution will have on individual's privacy. This report also discusses compliance and other privacy issues affecting the Agency and recommends steps to mitigate negative impacts. Where we refer to the solution in this PIA, we are referring to:

- the MHR Data Analytics Platform/Capability,
- the management and operation of the platform/ capability, and,
- the assessment and approval of any data use cases including for monitoring and/or reporting on the performance of the MHR and any approved secondary research and public health purposes of MHR data.

As this is a privacy by design project, aspects of the solution may change. Any differences between the design of the solution as reflected in this document and the final design as deployed should be reflected in a new or updated PIA.

In scope

In this document, we have considered:

- the privacy risks and impacts of the solution, including risks of non-compliance with the *Privacy Act 1988* (Cth) (**Privacy Act**), *My Health Records Act 2012* (Cth) (**MHR Act**),
- relevant requirements to carry out a PIA under the Privacy Code.

We have also reviewed the social licence for this use of MHR data and identified any risks that the Agency should consider when designing this solution.

Out of scope

In this document, we have assumed that the Agency has existing privacy operations which are compliant with Privacy Act and the MHR Act and will continue to do so in future. Accordingly, this PIA does not consider the Agency's organisational privacy operations, except to the extent that the solution may impact on them.

Additionally, we have not:

- considered the Agency's privacy policies, processes and procedures for the MHR generally, beyond the controls that are directly relevant to the solution design;
- considered the impact of health information on the solution;
- assessed detailed technical security controls for the solution; or
- considered compliance requirements arising under legislation not identified as being in scope above.

Methodology

Information gathering

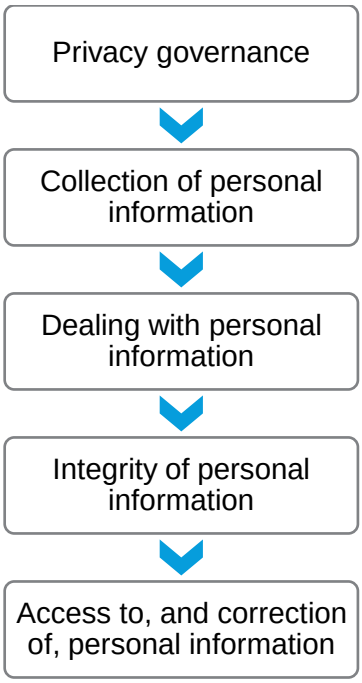
In our analysis, we have relied on information gathered through:

- documentation about the solution supplied by the Agency;
- notes recorded during remote meetings with the Agency;
- questions asked to the Agency out of session; and;
- consideration of publicly available materials.

See *Annexure 2* in this document for more information on sources.

Analysis

The analysis of privacy impacts in this document is organised by reference to the information lifecycle adopted in the Privacy Act:



Each stage of the information lifecycle is set out in a separate section of the analysis. The relevant considerations arising under the Privacy Act, the APPs, the Privacy Code and MHR Act are briefly summarised at the start of each section and are followed by a consideration of the corresponding issues that arise in relation to the activities.

Findings

The findings in this document are presented as either being '**Compliance**' or '**Best Practice**'.

Where a specific recommendation is classified as 'Compliance', it means that this item alone may constitute a compliance gap and action should be prioritised. However, even recommendations classified as 'Best practice' have significance as they are all are aspects of privacy management and hence what may constitute 'reasonable steps' under APP 1.2.

Compliance recommendations

Compliance recommendations are made where we have observed a compliance gap that requires action. These may relate to compliance with the Privacy Act or other Acts that are in scope for this assessment.

Best practice recommendations

In our analysis, we have made privacy-related best practice recommendations which apply to the activities, but which do not pose compliance risk. Examples of these include recommendations that relate to:

- opportunities for improved privacy practices; and
- matters that may affect stakeholders but not the Agency.

Best practice recommendations are suggested actions to mitigate an issue or to realise an opportunity. Suggested actions may already form part of existing Agency plans and/or procedures to manage known issues.

Information flows

This section outlines how personal information will flow between different stakeholders and from one system to another for the solution.

Figure 1 describes high-level information flow from individual to the Agency to use de-identified information as part of My Health Record Data Analytics Platform (**MDAP**). This information may also be shared with AIHW for public health and research purposes for this solution and then to DoHAC for reporting purposes. We note that these future uses cases are not in scope for this PIA and have only been added to the information flow for completeness.

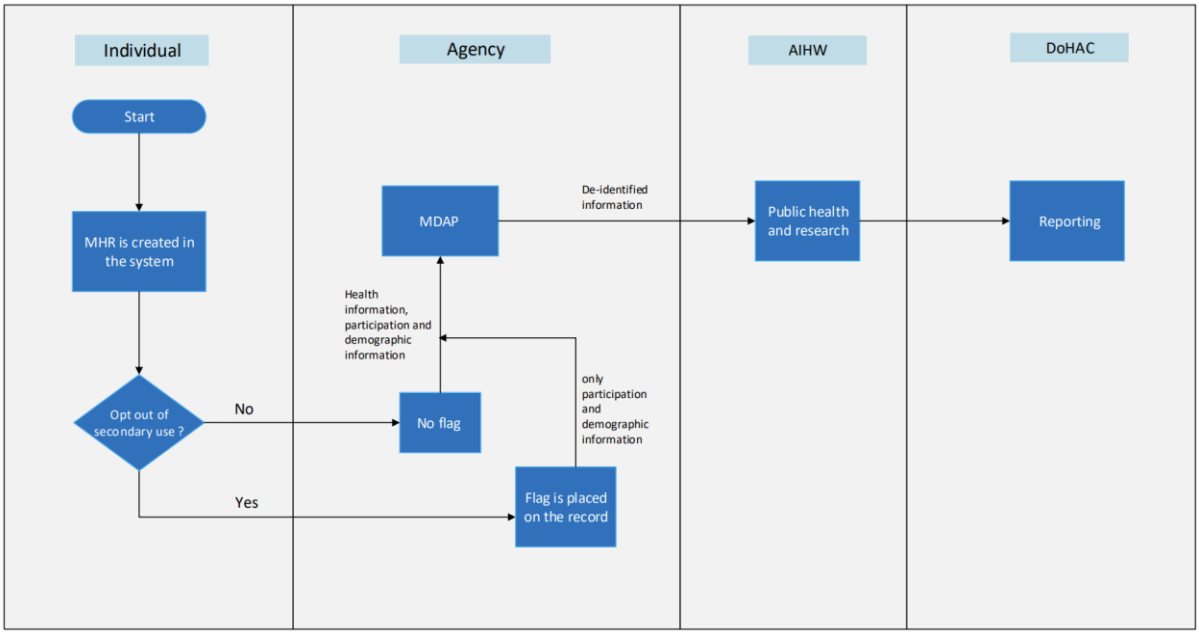


Figure 1 - High level data flow diagram of MHR and the solution

Figure 2 is a high-level diagram that outlines how information flows into MDAP and its three layers. The data extracted from the three databases is as follows:

Oracle Database (source)	Data description
OES	Participation and demographic data (such as IHI, name, address, DOB) of individuals (health recipients and healthcare providers) participating in the MHR.
OSB	Transaction log, audit logs and tracing logs.
RLS	Metadata for clinical documents, healthcare facility identification data.

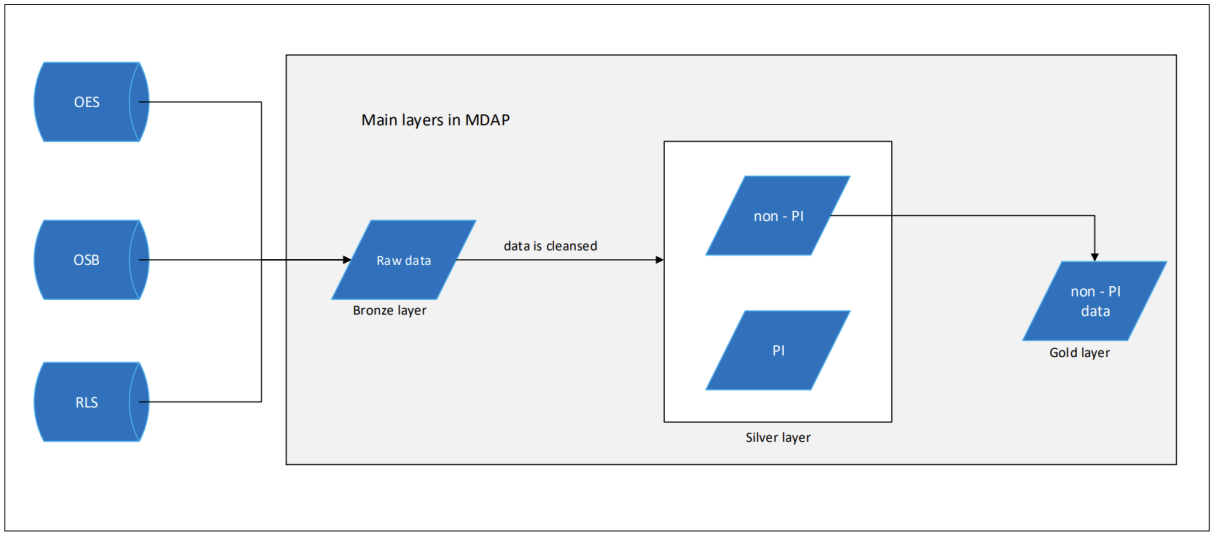


Figure 2 - High level data flow in MDAP

Privacy analysis

1. Privacy governance

1.1. Open and transparent management of personal information

Relevant considerations

APP 1 requires the Agency to manage personal information in an open and transparent way.

APP 1.2(a)	• The Agency must manage personal information in an open and transparent way. • The Agency must take reasonable steps to ensure it complies with the APPs and must otherwise comply with its obligations under the Privacy Act.
APP 1.2(b)	The Agency must take reasonable steps to enable it to handle privacy inquiries or complaints.
APP 1.3	The Agency must have a clearly expressed and up to date privacy policy.
APP 1.4	The Agency must ensure that its privacy policy contains specific information set out under APP1.4
APP 1.5, 1.6	The Agency must make its privacy policy free, publicly available and in an accessible form.
Privacy Code s 16	The Agency must carry out appropriate privacy training on induction of new staff, and annually where reasonable.
Privacy Code s 17	• The Agency must regularly review and update its privacy practices, procedures, and systems to ensure that they are current and adequately address the requirements of the APPs. • The Agency must monitor compliance with its privacy practices, procedures, and systems regularly.

Impact analysis

To assess the Agency's compliance with APP 1 (Open and transparent management of personal information) we reviewed the *My Health Record Privacy Policy*[10]. This policy explains how the Agency, as System Operator under the MHR Act 2012 (Cth), collects, uses, and discloses personal information to operate and manage the MHR.

We note that the MHR Privacy Policy is overdue for review as it has not been updated since 17 June 2022. The Agency informs us that the policy review remains pending due to an

[10] https://www.digitalhealth.gov.au/about-us/policies-privacy-and-reporting/privacy-policy#mhr-privacy-policy.

ongoing review by the Office of the Australian Information Commissioner (**OAIC**) and that it will be reviewed as part of the 2024-25 Privacy Management Plan.

While reviewing the policy, it was also observed that the Agency could be clearer to individuals on the use of their MHR information internally at the Agency i.e. monitoring how users interact with the MHR especially with the introduction of the solution.

Additionally, further transparency and clarity could be applied to the MHR data used for approved secondary research and public health purposes section, especially this paragraph which is available in the MHR Privacy Policy but has been extracted from the MHR Act.:

> *The Board's role also includes guiding and directing us to prepare and provide de-identified data for research or public health purposes and, with the consent of the healthcare recipient, health information for the same purposes.*

The Agency informs us that privacy training occurs across the organisation including MHR legislation training and what the Agency can and cannot do as the System Operator.

Findings

Recommendations	
COMPLIANCE REC. 1	The Agency must revise the MHR Privacy Policy to ensure that it is: • up to date. • open and transparent on how de-identified information will be used by the Agency and explain its purpose.

1.2. Data breach response management

Relevant considerations

The MHR Act requires the Agency to notify the Information Commissioner and affected individuals of eligible data breaches.

MHR Act s75	Breaches of health information contained in a healthcare recipient's MHR must be handled and notified in accordance with the MHR Act.

Impact analysis

The Agency has requirements under the *Guide to mandatory data breach notification in the My Health Record system*[11] for reporting a notifiable data breach. This includes if the notifiable data breach:

- directly involves the Agency;
- may have involved the Agency; or,

[11] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/my-health-record/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system#part-3-the-system-operators-requirements-for-notifiable-data-breaches.

- may involve the Agency.

It is also noted that the Agency has a general data breach response plan. This plan should be tested with the new solution especially with data being shared with other government agencies i.e. AIHW and DoHAC. It is also advisable that the Agency provide guidance to these agencies on the notification of a data breach if one was to occur.

Findings

Recommendations	
BEST PRACTICE REC. 1	The Agency should test how the data response plan applies to the new solution before going live in conjucntion with the Risk Governance team.

1.3. Anonymity and pseudonymity

Relevant considerations

APP 2 requires the Agency to give individuals the option of not identifying themselves, or of using a pseudonym (subject to limited exceptions).

APP 2	The Agency must allow individuals to be anonymous or pseudonymous, except if: • the Agency has legal reasons for not doing so; or • it would be impracticable for the Agency to do so.

Impact analysis

Individuals can interact with the MHR using a pseudonym in line with rules set out under the MHR Act. An individual can opt to use a different name or pseudonym and register for a new Individual Healthcare Identifier (IHI) if they consider themselves vulnerable or at risk.[12] Using the pseudonym IHI, an individual can apply for a new MHR.[13] We note that "a pseudonymous MHR is not linked to a MHR in your real name if there is one. Nothing in a pseudonymous MHR indicates it is a pseudonymous record." Essentially, the agency treats a pseudonymised record as a normal record and an individual can have two MHR accounts.

Findings

We have not made any findings in relation to anonymity and pseudonymity.

[12] https://www.servicesaustralia.gov.au/ms005.
[13] https://www.digitalhealth.gov.au/sites/default/files/documents/form-b-register-for-a-my-health-record-with-a-pseudonym-healthcare-identifier-v2.pdf.

2. Collection of personal information

2.1. Solicited personal information

Relevant considerations

APP 3 outlines when the Agency can collect personal information that is solicited. Higher standards apply to the collection of sensitive information. Sections 21-25A of the HI Act set out the circumstances in which the Agency may collect identifying information of healthcare practitioners and HPI-Is. Sections 36 and 36A of the HI Act provide authorisation for the Agency to handle identifying information for the purposes of providing information technology services.

APP 3.1	The Agency must only collect personal information that is reasonably necessary for its functions or activities.
APP 3.5	The Agency must only collect personal information by lawful and fair means.
APP 3.6	The Agency must collect information directly from individuals, unless if it is unreasonable or impracticable to do so.
HI Act s 21-25A	An entity should only collect HPI-Is and HPI-Os and identifying information of healthcare providers where it has a reason for doing so under the HI Act.
HI Act s 36	If the Agency is a contracted service provider (**CSP**) to a healthcare provider, then it may be authorised to handle information (including HPI-Is and HPI-Os) for the purposes of providing information technology services relating to the communication of health information, or health information management services, to the healthcare provider.
HI Act s 36A	If the Agency is a CSP to a healthcare provider for the purposes of providing information technology services relating to the communication of health information, or health information management services, to the healthcare provider, then entities that may disclose information to the healthcare provider may also be authorised to disclose that information to the Agency.

Impact analysis

The solution is designed to extract the ‘participation data’ in order to track and report on the national levels of participation and interaction with MHR. This use of data is authorised by the MHR Act, giving the Agency the lawful means of collection. The proposed data being extracted (as discussed in more detail below), would not be considered more than is reasonably necessary for its functions. If an individual does not wish their information to be used for research or public health purposes, they are able to opt out of this secondary use which is discussed in section 2.3.

With regard to the collection and disclosure of healthcare identifiers and health records, we note that the MHR Act authorises these activities where the System Operator (the Agency), is doing so for a purpose defined under the Act.[14]

Findings

We have made no findings in relation to the collection of solicited information.

2.2. Unsolicited personal information

Relevant considerations

APP 4 outlines how the Agency must deal with unsolicited personal information.

APP 4.1, 4.3	If the Agency receives unsolicited personal information that is not contained in a Commonwealth record, and which it could not have solicited, it must destroy or de-identify the information.
APP 4.4	If the Agency receives unsolicited personal information that is contained in a Commonwealth record, the Agency must handle the information as if it had solicited it.

Impact analysis

Given that the solution in its current state only ingests structured data that has been through quality assurance checks, it is unlikely unsolicited personal information would be extracted.

Findings

We have made no findings in relation to the collection of unsolicited personal information.

2.3. Notification of collection

Relevant considerations

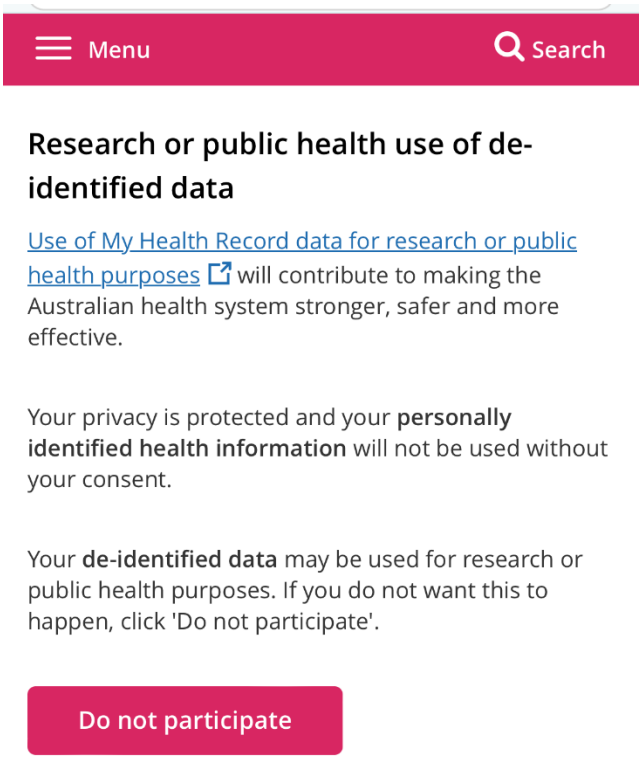
APP 5 outlines how the Agency must notify individuals when it collects personal information about them.

APP 5	The Agency must take reasonable steps to notify individuals of relevant matters (set out in APP 5.2) when it collects their personal information (or as soon as practicable after).
APP 3.3	The Agency must obtain consent from individuals before it collects sensitive information (including biometric information) about them.

[14] s15 *My Health Records Act 2012* (Cth).

Impact analysis

The secondary use of de-identified data in the MHR for research or public health purposes works on an opt-out basis. In order for an individual to opt-out, or access information relevant to the secondary use, they must login to their MHR, select the record they wish to access, click to 'Profile & Settings', select 'profile' from the drop-down list, then scroll down until they are shown the following screen.



The ease of which an individual can find notification of the use of their data and the ability to opt-out within their record may not be considered best practice when considering APP 5. As detailed above, there are 5 steps to locate this information, if an individual knows what they are looking for.

While we recognise the preference for a large dataset and the decision to change to an opt-out method of collection, it does raise some points for consideration.

The opt-out model assumes a level of implied consent applies to the population, yet there is doubts that this can be assumed, particularly in relation to disadvantaged or vulnerable groups of Australians.[15] The lack of withdrawn consent, may not mean the individual is making an informed choice, but could instead mean that they have no understanding of what a MHR is, how to opt out or even have the ability to access the system in order to do so.

As of May 2024, there were 23.71 million records which held data in them, yet there were only 7.94 million views of any record in that month.[16] While the number of views does not directly determine how many individuals use or have a proactive knowledge of their MHR,

[15] Chapter 5 – Parliament of Australia (aph.gov.au)
[16] Statistics (digitalhealth.gov.au)

there is a consistently large disparity in numbers of views vs total records in any given month.

There are large groups of vulnerable and disadvantaged groups of individuals in Australia, as well as a disparity in levels of access to technology and a sound ability to use technology who must be considered in the design process of this consent model. In light of this, there is a need for appropriate ongoing education to ensure communities have a clear understanding of the MHR, how the MHR handles their personal information, and what controls they can put in place to mitigate any concerns they have.

We note that it could be useful to consider running a campaign about the MHR, especially for the use of data for approved secondary research and public health purposes. However, we acknowledge that the research and public health program is led by AIHW (as data custodian) in collaboration with the Agency and DoHAC and that there is a 5-year roadmap under a different workstream in engagement and communication that this campaign should fall under.

Findings

Recommendations	
BEST PRACTICE REC. 2	The Agency should change the location of the opt-out option within the MHR to be shown upon login, or within the first page of their record. Bringing the notice to the front of the MHR shows a level of transparency that will help support an informed decision for the individual.

3. Dealing with personal information

3.1. Use and disclosure

Relevant considerations

APP 6 outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 6.1, 6.2	The Agency must not use or disclose the personal information for a secondary purpose, except where individuals have consented to the secondary purpose, or the secondary purpose is related to the primary purpose (or directly related in the case of sensitive information).
HI Act s 25	The Agency may use and disclose: • identifying information of a healthcare provider, or • the healthcare identifier of a healthcare provider so that it can enable the healthcare provider's identity to be authenticated in electronic transmissions.

HI Act s 25, 26	The Agency must not use or disclose an HPI-I or HPI-O, or any identifying information obtained under the HI Act, for a purpose that isn't permitted under the HI Act. For example, the Agency may use or disclose identifying information of a healthcare provider, or the healthcare identifier of a healthcare provider, so that it can enable the healthcare provider's identity to be authenticated in electronic transmissions.
HI Act s 36	If the Agency is a CSP to a healthcare provider, then it may be authorised to handle information (including HPI-Is and HPI-Os) for the purposes of providing information technology services relating to the communication of health information, or health information management services, to the healthcare provider.
HI Act s 36A	If the Agency is a CSP to a healthcare provider for the purposes of providing information technology services relating to the communication of health information, or health information management services, to the healthcare provider, then entities that may disclose information to the healthcare provider may also be authorised to disclose that information to the Agency.
MHR Act s 15, 16	The Agency, in accordance with the guidance and direction of the Board (established under section 82), may prepare and provide de-identified data or health information for research or public health purposes with the consent of the healthcare recipient.

Impact analysis

The Agency has informed us that the current preparation of data (data copying and extracting) for the purpose of reporting is completed by Accenture and the reporting is completed by the Agency data analytics team. This process is a limiting and time-consuming. The introduction of the solution will enable the Agency to complete the end-to-end process internally and improve the data lineage, transparency and quality in the data analysed. As per the MHR Act, the Agency is able to use the MHR data for the following uses (there are additional uses outlined in the MHR Act (refer to *Annexure 1*), however these are the ones which relate to the Solution):

- to establish and maintain a reporting service that allows assessment of the performance of the system against performance indicators;
- to establish and maintain an audit service that records activity in respect of information in relation to the My Health Record system;
- to establish a mechanism for handling complaints about the operation of the My Health Record system;
- to ensure that the My Health Record system is administered so that problems relating to the administration of the system can be resolved;
- to advise the Minister on matters relating to the My Health Record system, including in relation to the matters to be included in the My Health Records Rules (see section 109);

- to educate healthcare recipients, participants in the My Health Record system and members of the public about the My Health Record system;
- in accordance with the guidance and direction of the Board established under section 82 of the MHR Act, to prepare and provide de - identified data, and, with the consent of the healthcare recipient, health information, for research or public health purposes.

We understand that the Agency has sought legal advice on the permissibility of the solution in relation to its role as an operator. We have not sighted the legal advice but have assumed that the Agency has satisfied itself of the legality of the solution and its uses.

Use and performance of the MHR

The use of de-identified data for the purposes of reporting and analysis on the performance of the system is a permissible use under s15 of the MHR Act.

As outlined in the earlier sections, the solution will hold information extracted from three main databases OES, OBS and RLS, which contains participation data, activity logs and metadata respectively.

There are three main layers within the solution – bronze, silver and gold. Data in the first layer (bronze) is ingested in its raw form. In the second layer (silver) this data is cleansed and separated into PI and non-PI (de-identified) data. The de-identified data is then moved into the third layer (gold) to be enriched with reference data and used for the purposes of analysis and reporting.

It is our understanding that reference data will be held within the intermediate layers of the solution for the purposes of processing information e.g. SNOMED CT - AU codes, Statistical Area level 2 (SA2) identifiers which when combined with other sources of data (such as demographic data) could be used to re-identify individuals. For example, if the condition is rare and specific to a certain demographic or public figure. As illustrated in the MHR review, various studies have been conducted the demonstrate that it is possible to re-identify individuals from a dataset particularly from public records.[17] A study conducted by the University of Melbourne revealed that a de-identified dataset containing information about Medicare Benefits Schedule (MBS) and Pharmaceuticals Benefits Scheme (PBS) information could be used to identify health recipients and providers from publicly available records.[18] This must be taken into consideration when using de-identified data for approved secondary research and public health purposes.

Research and Public Health Purposes

Under the guidance and direction of the Data Governance Board per the MHR Act, de-identified information may be used for the approved secondary purposes of research and public health unless an individual opts out of their data being used for approved secondary research and public health purposes. Additionally, de-identified information will be shared to support AIHW in its function as the data custodian to report on MHR users.

It has been identified that personal information of healthcare recipients may be shared with DoHAC for monitoring and reporting on compliance of healthcare providers uploading

[17] https://www.health.gov.au/sites/default/files/documents/2021/02/review-of-the-my-health-records-legislation-final-report.pdf
[18] https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records

pathology and radiology results. However, we note that this is a future use case subject to authorisation and not in scope for this PIA.

It is our understanding that when an individual opts out of their information being used for public health and research purposes, a flag will be placed on their record in the solution and their health information will be deleted from the solution. However, their demographic and transactional data is retained in the solution and may be used for reporting purposes.

De-identification as a 'use' as discussed in the MHR Act review is a permitted use under 63(a) of the MHR Act and APP 6 so long as the Agency in its role as the System Operator uses health information from the MHR that is within the limits of 'reasonable expectation' of health recipients in terms of how their information is used including for all approved future secondary research and public health purposes.[19]

According to the OAIC, personal information that has undergone rigorous process of de-identification is not considered to be personal information and is permitted to be shared or released under the Privacy Act provided the context in which it is released is thoroughly assessed and risk of re-identification is minimal. For this, the Agency must update its privacy policy to directly explain how de-identified health information may be used by the System Operator and its purposes to health recipients (Refer to compliance recommendation 1).

To securely transfer de-identified data, we have been advised that the Agency intends to develop a separate platform in the protected environment of National Infrastructure for AIHW, along with any other third-party research recipient, for the data sets to be ingested. The solution and this new data custodian environment will co-exist in the same cloud infrastructure within separate tenancies. Any new solution will need to be assessed in subsequent PIAs to assess privacy risk and compliance.

Findings

Recommendations	
COMPLIANCE REC. 2	The Agency must identify and adopt appropriate de-identification methodologies to remove personal information including any health identifiers when cleansing data from different layers of the solution and take reasonable steps to minimise any risks of re-identification of data from publicly available sources.
BEST PRACTICE REC. 3	The Agency should consider implementing internal guardrails to ensure de-identified health information is not used for purposes that may be beyond what individuals may reasonably expect their health information to be used for.
BEST PRACTICE REC. 4	The Agency should ensure the existing data dictionaries for the three databases (OES, OSB and RLS) for this solution are complete and up to date to inform their understanding of the data in the solution and build robust data governance controls over the use of this data (including de-identified data) for all future secondary research and public health use cases.

[19] https://www.health.gov.au/sites/default/files/documents/2021/02/review-of-the-my-health-records-legislation-final-report.pdf

BEST PRACTICE REC. 5	If there are any material changes to the technical solution or deviations from the proposed scope (including extraction of unstructured data), the use cases arising out of these modifications should be assessed through subsequent PIAs.

3.2. Direct marketing

Relevant considerations

APP 7 describes the conditions that an organisation must meet when it uses or discloses personal information for direct marketing purposes.

Impact analysis

We have not considered compliance with APP 7 as this principle only applies to agencies in very limited circumstances which do not apply here.

Findings

We have not made any findings in relation to direct marketing.

3.3. Cross-border disclosure

Relevant considerations

APP 8 outlines the steps the Agency must take to protect personal information before it is disclosed overseas.

APP 8.1	If disclosing personal information to a recipient outside of Australia, the Agency must: • take reasonable steps to ensure that any overseas recipients will not breach the APPs; or • reasonably believe that the recipient is subject to enforceable laws substantially like the APPs; or • inform recipients that overseas recipients may not apply the APPs to the information and obtain user consent to the disclosure.

Impact analysis

We note that APP 8 may not apply as there are no intended cross border disclosures in scope for this solution.

Findings

We have not made any findings in relation of cross border disclosures.

3.4. Government related identifiers

Relevant considerations

APP 9 outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

Impact analysis

APP 9 is not applicable as this principle only applies to Commonwealth agencies in very limited circumstances, which do not apply here.

Findings

We have not made any findings in relation to Government related identifiers.

4. Integrity of personal information

4.1. Quality

Relevant considerations

APP 10 requires the Agency to take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. The Agency must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 10	The Agency must take reasonable steps to ensure that personal information collected, used and disclosed through the solution is accurate, up-to-date, complete, relevant and not misleading.

Impact analysis

The design of the solution involves the use of personal information from the MHR. It is noted that the MHR is a downstream system and predominately receives information from external sources. Currently, the MHR performs various conformance checks i.e. checks on incoming clinical data, format checks and data integrity on personal information coming from Services Australia and reference data validation. As data can be updated in the MHR, it is essential these updates are reflected in the solution.

Quality checks for corrections/ updated to individuals MHR

We discussed with the Agency how it will action updates to the Solution when as individual makes changes/ updates to the data held within their MHR. The Agency has explained that through a daily delta, the solution will receive an update when an individual makes any change to their information in the MHR i.e. address details. For the solution, this includes changes to the ‘opt-out’ status and deletion of the record entirely. It is our understanding that once these changes have been received, they will be updated and amended accordingly within the solution. Where a user deletes their MHR, their information will be deleted from the

Solution. Where a user changes to opt-out of the use of their MHR data for research or public health purposes (after the original ingestion), the 'health information' will be deleted from the analytics platform so that it is not used for research and public health purposes moving forward.

We have been informed by the Agency, there is the exception for de-identified data already shared with AIHW. Where de-identified data about an individual has already been shared or disclosed as part of the purpose of research or public health purposes, the Agency is unable to retract this. The individual's de-identified data will simply no longer be included in datasets for research and public health purposes from the date the individual has rescinded their consent (i.e. opt-out). Given this is a privacy by design approach, it is imperative that, as identified, the Agency ensures this feature is built into its final solution architecture to ensure that the quality of information within the solution is of high quality.

Identified individuals for research

It is advisable to contact individuals to verify the quality of their information before using and disclosing the information for identified individuals, particularly if there has been a lengthy period since collection. However, this is recommended to be addressed in a future PIA.

Findings

Recommendations	
BEST PRACTICE REC. 6	The Agency should confirm the quality of information within the solution is high by ensuring any changes that occur in the MHR are reflected in the solution i.e. address details are updated, checking individuals who have deleted their MHR are not showing in the Solution.

4.2. Security

Relevant considerations

APP 11 requires the Agency to take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

APP 11.1	The Agency must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure.
HI Act s 27	The Agency must take reasonable steps to protect healthcare identifiers that it holds from misuse and loss and from unauthorised access, modification or disclosure.

Impact analysis

It is our understanding that the Agency takes information security extremely seriously, and the nature and volume of the information held within the MHR.

Cyber assessments

In relation to the solution, a cyber security assessment was conducted prior to the beginning of the project. As the solution is developed, there is an ongoing assessment that occurs though a live TRA risk register to action anything that is flagged throughout the development process. We have been advised that production halts if there are any high risks flagged, only to recommence once the risk has been resolved.

Further, every time a data set is produced, it will be penetration tested by simulating attacks to ensure appropriate deidentification has occurred, without compromising the utility of the data for its intended purpose. To further confirm the process has been successful, a disclosure risk assessment will also be conducted on the data sets produced.

It is noted that, prior to going live, the solution will undergo another cyber risk assessment once it is completed.

Access Control

While sharing of data to stakeholders will occur from the gold layer in the solution, direct access to the environment will not be provided. The solution environment is classified as Protected and as such, can only be accessed through Privilege Access Workstations (PAWs) or Agency laptops with Windows Cloud PC, with Multi Factor Authentication (MFA) using biometrics/authentication codes as per Agency standard and approved patterns to access resources in the solution. This access is only available to Agency staff, along with admin and platform engineers from DXC and Accenture. There will be role-based access policies in place where access to data and other platform resources is provided based on an individual's role within the Agency as a staff member or a vendor partner.

Where an admin user requires access to the environment, there is a robust process in place to grant access, which includes an automated process to revoke access after a designated time period.

Audits

Audit trails are maintained in all layers of the solution to log and check access, a process supported by identity access management. These audits are accomplished via telemetry logs through Azure, allowing a view of all access occurrences.

To ensure stringent access controls, any new user that requires access must go through four levels of approvals to gain access to the system and audit trails are captured to ensure that unauthorised access does not occur. The agency currently uses ServiceNow to manage approvals.

Findings

Recommendations	
COMPLIANCE REC. 3	The Agency must ensure that the on-going cyber security assessment is finalised after the solution has been completed

	and any risks arising out this assessment must be mitigated prior to the solution going live.

4.3. Retention

The Agency has obligations to destroy or de-identify personal information in certain circumstances.

Relevant considerations

MHR Act s 17	The System Operator must ensure that the record is retained for the period: (a) beginning when the record is first uploaded to the National Repositories Service; and (b) ending: (i) 30 years after the death of the healthcare recipient; or (ii) if the System Operator does not know the date of death of the healthcare recipient—130 years after the date of birth of the healthcare recipient.

Impact analysis

We note that when an individual deletes their MHR (as per MHR Act) that their information will also be deleted from the solution. There are no other arrangements to delete data from the solution at this point and it will be retained as per the requirements of the MHR Act.

Findings

We have not made any findings in relation to retention at this stage.

5. Access to, and correction of, personal information

5.1. Access and correction

Relevant considerations

APP 12 outlines the Agency's obligations when an individual seeks access to personal information that the Agency holds about them. This includes a requirement to provide access unless a specific exception applies. APP 13 outlines the Agency's obligations in relation to correcting the personal information it holds about individuals.

APP 12	The Agency must, on request, give individuals access to the information it holds about them (subject to specific exceptions), in the manner specified in APP 12.

APP 13	The Agency must allow individuals to request their personal information be updated and must take reasonable steps to correct personal information that is inaccurate, out of date, incomplete, irrelevant or misleading. The Agency must provide individuals with a simple means to review and update their personal information on an ongoing basis. The Agency must respond to correction requests in the manner described in APP 13.
MHR Act s52	The Agency may decide on the request of a healthcare recipient or other entity, to vary the registration of the healthcare recipient or other entity to correct an error or omission in the registration.

Impact analysis

We note that APP 12 and APP 13 does not apply to the solution.

Findings

We have not identified any findings in relation to access and correction.

References and key terms

References to documents and key terms in this document are described below.

Accenture	National Infrastructure Operator (NIO)
Agency	Australian Digital Health Agency.
Agency Privacy Policy	means the privacy policy published by the Agency which describes how it handles personal information and made available at https://www.digitalhealth.gov.au/privacy
AIHW	means the Australian Institute of Health and Welfare
Australian Privacy Principles or **APPs**	means the 13 Australian Privacy Principles set out in Schedule 1 of the Privacy Act.
Authorised Appendix 1Representative	means someone who can apply for and manage a My Health Record on behalf of another person. For the purposes of the My Health Record system someone can be an authorised representative if they: • have parental responsibility for a person under 14; or • have legal authority to act on behalf of a person who is at least 14 and who is not capable of making his or her own decisions. If there is no one with parental responsibility or legal authority, a person who is otherwise appropriate to act on behalf of the individual can be an authorised representative. An individual can have more than one authorised representative.
Compliance recommendations	Compliance recommendations are made where we have observed a compliance gap that requires action. These may relate to compliance with the Privacy Act or other Acts that are in scope for this assessment.
Best practice recommendations	Privacy-related best practice recommendations which apply to the Activities, but which do not pose compliance risk. Examples of these include recommendations that relate to: • opportunities for improved privacy practices; and • matters that may affect stakeholders but not the Agency.
Individual Healthcare Identifier or **IHI**	has the meaning given in the HI Act.
Health Information	has the meaning given in subsection 6(1) of the Privacy Act.
HI Service	means the Health Identifier Service operated by the Chief Executive Medicare under the HI Act.
Healthcare Identifiers Act or **HI Act**	means the Healthcare Identifiers Act 2010 (Cth).

Information Commissioner	means the Australian Information Commissioner.
HPI-I	Health Provider Identifier – Individual
HPI-O	Health Provider Identifier – Organisation
MHR	means the My Health Record system operated by the Agency.
NIO	means the National Infrastructure Operator
Personal Information	has the meaning given in section 5 of the Privacy Act.
Privacy Act	means the *Privacy Act 1988* (Cth).
Privacy Code	means the *Privacy (Australian Government Agencies — Governance) APP Code* 2017 (Cth).
Registered partners	means participants in the MHR other than the Agency; that is: registered healthcare provider organisations, registered repository operators, registered portal operators and registered contracted service providers.
Secondary use	means any purpose other than the primary purpose for which the APP entity collected the personal information, including the Agency's use for research and public health purposes.
'solution, the'	means the My Health Record Data Analytics Platform/Capability and data uses, also known as Use Case 3.

Annexure 1: System Operator functions

The *My Health Records Act 2012* (Cth) (**MHR Act**), establishes the functions of the System Operator, which are:

(a) to establish and maintain an index service, for the purposes of the My Health Record system, that:

(i) allows information in different repositories to be connected to registered healthcare recipients; and

(ii) facilitates the retrieval of such information when required, and ensures that registered healthcare recipients, and participants in the My Health Record system who are authorised to collect, use and disclose information, are able to do so readily;

(b) to establish and maintain mechanisms (***access control mechanisms***) that, subject to any requirements specified in the My Health Records Rules:

(i) enable each registered healthcare recipient to set controls on the healthcare provider organisations and nominated representatives who may obtain access to the healthcare recipient's My Health Record; and

(ii) specify default access controls that apply if a registered healthcare recipient has not set such controls; and

(iii) specify circumstances in which access to a healthcare recipient's My Health Record is to be automatically suspended or cancelled;

(c) without limiting paragraph (b), to ensure that the access control mechanisms enable each registered healthcare recipient to specify that access to a healthcare recipient's My Health Record is only to be:

(i) by healthcare provider organisations and nominated representatives specified by the healthcare recipient; and

(ii) in accordance with any limitations specified by the healthcare recipient, including limitations on the kind of health information to be collected, used or disclosed by such healthcare provider organisations and nominated representatives;

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

(e) to establish and maintain the Register (see section 56);

(f) to register healthcare recipients and participants in the My Health Record system (see Part 3) and to manage and monitor, on an ongoing basis, the system of registration;

(g) to establish and maintain an audit service that records activity in respect of information in relation to the My Health Record system;

(h) without limiting paragraph (g)—to establish and maintain mechanisms:

(i) that enable each registered healthcare recipient to obtain electronic access to a summary of the flows of information in relation to his or her My Health Record; and

(ii) that enable each registered healthcare recipient to obtain a complete record of the flows of information in relation to his or her My Health Record, on application to the System Operator;

(i) to operate a National Repositories Service that stores key records that form part of a registered healthcare recipient's My Health Record (including the healthcare recipient's shared health summary);

(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;

(j) to establish a mechanism for handling complaints about the operation of the My Health Record system;

(k) to ensure that the My Health Record system is administered so that problems relating to the administration of the system can be resolved;

(l) to advise the Minister on matters relating to the My Health Record system, including in relation to the matters to be included in the My Health Records Rules (see section 109);

(m) to educate healthcare recipients, participants in the My Health Record system and members of the public about the My Health Record system;

(ma) in accordance with the guidance and direction of the Board established under section 82, to prepare and provide de-identified data, and, with the consent of the healthcare recipient, health information, for research or public health purposes;

(n) such other functions as are conferred on the System Operator by this Act or any other Act;

(o) to do anything incidental to or conducive to the performance of any of the above functions.

Annexure 2: Interviews and documentation

Interviews

Date	Meeting	Attendees
29 May 2024	Kick off meeting PIA – Use case 3 of MHR data	Jerin Mathew Chadi Tahan, Supriya Prakash, Adil Mehmood, Marcel Kwantes, Oscar Ben, James Kearton, Cassie Findlay, Laura McVey, Georgia Brinkworth, Chaitalee Sohoni
05 June 2024`	PIA for Use case 3 of MHR data	Chadi Tahan, Supriya Prakash, Adil Mehmood, Rahul Shandil, Jerin Mathew, James Kearton, Snow Khaing, Cassie Findlay, Laura McVey, Georgia Brinkworth, Chaitalee Sohoni
06 June 2024	Weekly Catch up re MHR data PIA	Jerin Mathew, Chadi Tahan, Laura McVey, Cassie Findlay
12 June 2024	PIA for Use case 3 of MHR data – elevenM/ADHA	Chadi Tahan, Supriya Prakash, Adil Mehmood, Rahul Shandil, Jerin Mathew, Edward Hernanadez, Ken Fielding, Laura McVey, Georgia Brinkworth, Chaitalee Sohoni
13 June 2024	Weekly Catch up re MHR data PIA	Jerin Mathew, Chadi Tahan, Laura McVey, Cassie Findlay
19 June 2024	General discussion: PIA for Use case 3 of MHR data - elevenM/ADHA	Chadi Tahan, Supriya Prakash, Adil Mehmood, Rahul Shandil, Jerin Mathew, Laura McVey, Georgia Brinkworth, Chaitalee Sohoni
20 June 2024	Weekly Catch up re MHR data PIA	Jerin Mathew, Chadi Tahan, Laura McVey, Chaitalee Sohoni

Date	Meeting	Attendees
26 June 2024	Walk through of draft 1: PIA for Use case 3 of MHR data - elevenM/ADHA	Chadi Tahan, Supriya Prakash, Adil Mehmood, Rahul Shandil, Jerin Mathew, Laura McVey, Georgia Brinkworth, Chaitalee Sohoni, Cassie Findlay
27 June 2024	Weekly Catch up re MHR data PIA	Jerin Mathew, Chadi Tahan, Laura McVey, Cassie Findlay
4 July 2024	Weekly Catch up re MHR data PIA	Jerin Mathew, Chadi Tahan, Laura McVey, Cassie Findlay
17 July 2024	ADHA PIA catch up	Chadi Tahan, Rahul Shandil, Snow Khaing, Laura McVey, Georgia Brinkworth, Chaitalee Sohoni

Documents supplied by the Agency

- Background documents
  - ADHA - RBAC Model Solution Design – v2.1 (1)
  - Agency Data Governance Framework.DOCX
  - Attachment 1 – Rationale for using real-life data for MDAP's non-production Environment(ARMS).docx
  - CDA schematic diagram.png
  - Conceptual Solution Architecture v1.1.docx
  - Data Sharing Deed-Blank template V1.0.approved12012023.docx
  - Framework-to-guide-the-secondary-use-of-my-health-record-system-data.pdf
  - IIS PIA – ADHA Data Analytics Infrastructure PIA 2022-12-05 Final.PDF
  - MDAP De-identification Approach V0.6.docx
  - myHR Logical ER 1.png
  - Requirements Analytics Data Extraction and Ingestion Engine v0.6.0.docx
  - Review – Response WP191.2 – Phase 2 MHR Data Extraction s&Q_v0.2.0_AgencyFeedback (2).docx
  - Transaction log vs audit log Events Tranche4.xlsx
  - TSC Paper – EDAP-MDAP Merger.docx
  - Use Case 3 – MHR Participation & Usage.pptx
- MHR Data Dictionary v1.0
  - OES Data Dictionary v1.0.xlsx
  - OSB Data Dictionary v1.0.xlsx
  - RLS Data Dictionary v1.0.xlsx

- MHR Overview
  - MHR – System overview – Q&A.pdf
  - MHR – WS2-DB-Q&A.pdf
  - MHR WS1 – System overview 1.pdf
  - WS 2 OSB_OES_HDR,Databases overview 1.pdf
  - WS 3 – CDA – HDR – MyHR View – Grant +KH v0.0.5.1.pdf