Australian Digital Health Agency

My Health Record Mobile Vendor Changes

Privacy Impact Assessment

23 September 2022

Final Report

Contents

Document Control

Version	Date	Comments	Author
0.1	22/08/2022	Draft for client	elevenM
0.2	30/08/2022	Revised draft, incorporating preliminary feedback from Agency	elevenM
0.3	15/09/2022	Final draft for client	elevenM
1.0	23/09/2022	Final Report	elevenM

How to read this document

- In 2022, the Australian Digital Health Agency (the **Agency**) engaged elevenM (**we, us, our**) to deliver a Privacy Impact Assessment (**PIA**) for mobile vendor onboarding and expansion of functionality for third-party applications using My Health Record (**MHR**)
- The scope of this assessment is detailed in the 'About this PIA' section of this document.
- elevenM has provided the Agency with a set of recommendations:
    - Compliance recommendations are made where we have observed a gap between the proposed activity and a binding requirement that requires action.
    - Best practice recommendations are not designed to manage compliance but are suggested actions to mitigate an issue or to realise an opportunity.
    - We have also included a number of recommendations that are not compliance or best practice risks to the Agency with regard to its own privacy program, but they are risks to the Agency's reputation should an RPO not adhere to the Agency's requirements or their own obligations under the Privacy Act, or engage in practices that are contrary to community expectations.
    - Annexures 1 and 2 to this report contain recommendations relating to Agency documentation that are not otherwise addressed in the body of the document.
- We have included a list of abbreviations and key terms used in this report on page 40 of this document
- Annexure 3 contains a list of documents referenced and interviews conducted with Agency personnel.

Executive summary

Background

The Agency engaged elevenM to conduct a Privacy Impact Assessment (**PIA**) in relation to the expansion of functionalities for mobile app vendors accessing the My Health Record (**MHR**) system as Registered Portal Operators (**RPO**s).

The new functionalities being made available to third-party mobile app vendors that were in scope for this PIA are:

1. Get XML view (Pathology and Diagnostic Imaging) - App vendors will have access to structured data in Pathology and Diagnostic Imaging (DI) view. This can be presented in number of ways in their app, without altering the original contents.
2. Share function – This will be an in-app feature vendors can build in their app utilising the native sharing features of the mobile device. The Share function will enable consumers to share their MHR data outside of the app.

Compliance recommendations

We have identified 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 1988 or other Acts that are in scope for this assessment.

The table below sets out the compliance recommendations in the order they appear in the *Privacy analysis* section of this document.

COMPLIANCE REC. 1 We recommend a mobile app section be inserted into the MHR Privacy Policy including high-level plain English explanation of what RPOs offer (view, store, share, view images) and how RPOs will be required to manage MHR information. This would include explaining that RPOs are required to ask for permission for any use, that users can revoke access at any time, and that RPOs are not permitted to keep System Data for longer than 28 days.

COMPLIANCE REC. 2 The Agency should require that RPOs implement a rendering process that would ensure unnecessary personal information of third parties such as an individual doctor's home address is not rendered in xml view images.

Best practice recommendations

We have made two 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 take steps to ensure that changes to access permissions granted by an individual to a Nominated Representative are passed through to RPOs as rapidly as technically possible to mitigate risk where there is potential harm from either continuing access or lack of access.

BEST PRACTICE REC. 2 The Agency should ensure that public facing advice regarding what Nominated and Authorised Representatives may be able to do (depending, in the case of Nominated Representatives, on their access level) with regard to MHR information sharing is updated to accurately reflect the new Share feature.

RPO recommendations

We have made 10 recommendations that are not compliance nor best practice recommendations for the Agency with regard to its own privacy program, but are made to mitigate risks to the Agency's reputation should an RPO not adhere to the Agency's requirements or their own obligations under the Privacy Act, or engage in practices that are contrary to community expectations.

Implementation of such recommendations would demonstrate to the regulator and the public a high degree of care on the part of the Agency to ensure that RPOs are not only fit for handling MHR information at the time of registration but that over time they continue to meet the high standards expected of them. We have marked these using the prefix 'RPO'.

We note that the Agency has commenced work on a Portal Operator monitoring and audit framework[1]. Our recommendations should be considered for inclusion in this framework as it develops.

The table below sets out the recommendations in the order they appear in the *Privacy analysis* section of this document.

RPO REC. 1 Pre-registration point-in-time risk assessments and attestations do not provide ongoing assurance of compliance. The Agency should implement regular post-registration audits where any changes to risks and the data handling practices disclosed in pre-registration are actively sought out and understood by the Agency with a view to ensure continuing compliance with key mandatory requirements and recommended guidelines outlined in the Interoperability Requirements.

RPO REC. 2 The Agency should periodically review the privacy policies and notices of RPOs with respect to their apps to ensure they are in plain English and make necessary disclosures generally. The RPO onboarding documents should specify the Agency's role in monitoring privacy policies.

RPO REC. 3 The Agency should provide RPOs with a recommended list of clauses that should be used in privacy policies applicable to their mobile apps.

[1] *My Health Record Mobile Gateway - Portal Operator Monitoring and Audit Framework* (Draft)

RPO REC. 4 The Agency should insert a clause in the customer communications section of the PORA prohibiting the use of deceptive or manipulative practices including factual omissions, visual design features and any other factors relevant to app user decision-making.

RPO REC. 5 In pre-registration application documents including the PEAR and the CCD Risk Questionnaire, in the user stories sections, the Agency should require applicants to provide examples of the design and visual features surrounding the presentation of user decision points such as the decision to share an MHR.

RPO REC. 6 The Agency should provide RPOs with a recommended list of plain English alerts that should be displayed prior to common scenarios of user sharing. We recommend a prominent 'Before you share or save' header on these alerts. The alerts should be, for example, 'your data will be stored on your device/sent to your email address. MHR won't be protecting the data once you've downloaded it. Are you ok with this? Ok or go back'.

RPO REC. 7 The Agency should require as a condition of registration that that RPO privacy policies applicable to their apps alert or remind users that after MHR data is saved on their device it is subject to any automated cloud backup or other data handling enabled or agreed to by users for their devices with Apple iOS and Google Android operating systems.

RPO REC. 8 Create plain English communications, separate from contractual documents, targeted at staff of RPOs, highlighting among other obligations that retention of System Data after 28 days is a blanket prohibition.

RPO REC. 9 Ensure resourcing of Agency audit or conformance functions so that regular reviews of data retention and handling practices of RPOs are maintained over time and RPOs are incentivised to comply with deletion and handling requirements.

RPO REC. 10 Perform periodic technical audits of RPOs to test cyber security measures. Such audits should include penetration testing.

Recommendations relating to Agency documents

We have made a number of recommendations relating to the Interoperability guidelines, Developer Centre materials, the Portal Operator Registration Agreement and related forms. These are presented in Annexures 1 and 2.

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.[2]

[2] See Privacy Code ss 12, 13.

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

Following receipt of the 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.

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 is designated as System Operator of the My Health Record system. The privacy framework for the MHR system is currently set out in the My Health Record Act (**MHR Act**) and the Privacy Act.

The role of the OAIC

The OAIC has a range of regulatory functions and enforcement powers under both the Privacy Act and MHR Act to ensure compliance with these privacy requirements.

We note that the OAIC's submission to the Department of Health's 2020 review of the *My Health Record Act 2012*[3] made a recommendation designed to address what the OAIC regarded as limited compliance and assurance checks over healthcare providers who are in receipt of MHR information. In particular, the OAIC proposed that the Agency be obliged to monitor and collect evidence from providers to ensure that they are meeting their obligations under the MHR Act. It is our view that this recommendation by the OAIC, while relating in

[3] OAIC, Legislation review of the My Health Records Act 2012 - Submission to the Department of Health https://www.oaic.gov.au/engage-with-us/submissions/legislation-review-of-the-my-health-records-act-2012-submission-to-the-department-of-health

that instance to healthcare providers, demonstrates a desire from the regulator for greater accountability over the uses of MHR information after it has been shared with Portal Operators and should be taken into consideration in managing mobile app vendors who are RPOs.

Mobile apps for consumers of My Health Record healthcare information

Under the implementation plan for the National Digital Health Strategy, the *Framework for Action*, the goal that "All Australians will be able to access their information at any time online and through mobile apps" was proposed to be achieved by 2022[4]. A strategic priority in the Agency's *Corporate Plan 2021 - 2022* is to "provide consumer access to My Health Record through mobile applications and products"[5]

Accordingly, the Agency has continued to build on its program of work to authorise third-party mobile applications to access My Health Record System Data and is now adding to the functionalities that are available to third-party mobile app developers.

Authorised mobile applications connect to the My Health Record system via the system's Fast Health Interoperability Resources (**FHIR**) standard gateway using two interaction models for consumer-focused applications:

- Interaction Model 1 which is for mobile applications which talk directly to the My Health Record Mobile/FHIR gateway; and
- Interaction Model 4 which allows the mobile application to connect via an intermediary server.

The Agency is currently implementing changes to the arrangements the are in place to enable the third parties to make use of the FHIR gateway as registered portal operators so that they can:

- allow consumers view-only access to their Diagnostic Imaging and Pathology data (Get XML view); and
- allow consumers to share their MHR data using in-app sharing via the device's native capabilities (Share function).

These functionalities will be optional for each vendor to implement in their app, and uptake is not mandatory.

Get XML view (pathology and diagnostic imaging)

This API provides a mechanism for conformant external systems to retrieve a series of predefined views for a consumer's digital health record that can collate data from across documents within record. An XML view is stored as a Base64 string within the FHIR Binary

[4] *Australia's National Digital Health Strategy Framework for Action*, 2018
https://www.digitalhealth.gov.au/sites/default/files/2020-11/Framework_for_Action.pdf
[5] *Australian Digital Health Agency Corporate Plan 2021-2022*
https://www.digitalhealth.gov.au/sites/default/files/documents/adha-corporate-plan-2021-2022.pdf

resource and can be tailored by the requesting application by providing different view types, versions, and date ranges[6].

It will be an optional inclusion for production vendors, in-flight vendors and new vendors in the same way that the Share Function allows registered portal operators a "choice to share".

Share function

RPOs may choose to offer a share function in their apps that would enable users to share their MHR data outside of the app, for example send in an email or share in a messaging app. There is no associated API as this will be an in-app feature utilising the range of sharing options available to the device owner via the native sharing options that are configured for the device user.

About the app vendors

The Agency has confirmed the current app vendors include Telstra, HealthDirect and Chamonix. We are advised that Chamonix will withdraw its app when the my health app gov (**my health**) app is launched (due for launch in late 2022). The Agency has also confirmed previous app vendors, HealthEngine and Tyde have ceased to operate with MHR integration.[7]

Consumer attitudes to mobile health apps

We reviewed a report produced for the Agency by a research agency, ThinkPlace, containing a summary of qualitative and quantitative research into consumer and healthcare provider attitudes towards the design and delivery of a native mobile health application[8]. The research involved a survey of 1064 respondents, and was spread across the following cohorts:

- ages 15-44; 45-64; 65+;
- cities, regional, rural and remote home locations;
- parents and carers;
- people of Aboriginal and Torres Strait Islander origin; and
- culturally and linguistically diverse people.

The report is not dated however it is our understanding that it was conducted as a precursor to the Agency's development of the my health app, which is due to launch in October 2022.

The research identified a number of themes, including these that are relevant to the activities that are the subject of this PIA:

- **Solve for medical rather than health experience:** Consumers see a legitimate, important role for Government to play in the medical space (the information and experience relating to medical appointments), but decidedly not in the personal

[6] *DH_3559_2021__My Health Record FHIR Gateway - API Specification v2.3.0*, supplied.
[7] Emailed advice from the Agency, 17 August 2022
[8] *mHealth App Consumer Insights* report, supplied.

health space (the data collection and monitoring relating to personal health and wellbeing), which is being filled by consumer technology from the private sector.

- **Enable the full functionality of mobile:** Consumers are discouraged by a perception of duplication across the health system, feeling forced to manage personal health information in a way that can be unreliable, scrappy and disempowering. Mobile is often used to support this through live notetaking, audio recording or ad hoc photo capture.
- **Consider native mobile data security concerns:** Native mobile health apps have popularised the idea of tracking certain types of data without justification to consumers, whereas storing more sensitive data related to mental health or past procedures may require justification.

The research also found that:

- 64% of respondents had used their mobile to access, share and manage their health information. Respondents indicated that these uses were for calendar reminders, Medicare claims, booking appointments and for taking photos of and storing health information.
- The survey revealed that the features which seem to be most important to consumers are ones that relate to quick, secure access and ones that relate to storage of secure health information (i.e. 'digital wallet', emergency contacts, test results)
- A majority of consumer respondents reported feeling reserved about the idea of storing sensitive personal health information on their phone, but also recognized that there are a range of probable situations in which they would do so if it was advised by a clinician and/or in the interest of their personal health. Such examples might be that the clinician requests specific details about trauma or a past surgery.
- Some consumers reported wanting to control what information is shared with whom and at what times (especially mental health information and past procedures, such as abortion), for fear of discrimination, unfair treatment or misuse of that data.

About this PIA

This PIA report focusses on the privacy impacts resulting from the expansion of certain MHR functionalities to be available to mobile app vendors. This document represents a holistic consideration of the practical privacy impacts and is not legal advice.

In scope

In this document, we have assessed the privacy impacts associated with the Agency permitting third-party vendors of mobile apps that are Registered Portal Operators (**RPO**s) to offer app users new MHR functionalities, specifically:

- allowing consumers view-only access to their Diagnostic Imaging and Pathology data (Get XML View); and
- allowing consumers to share their MHR data outside the app via the device's native capabilities (Share function).

Where we refer to '**the Activities**' in this PIA, we mean the two new MHR functionalities that are being made available to the mobile app vendors. We note these are optional features that app vendors may choose to implement or not.

We commenced this PIA also reviewing the ability for consumers to add their Covid-19 Certificate (CDC) to Apple Wallet or Google Pay. This was later removed from our scope on advice from the Agency.[9]

Specifically, we have focussed on:

- describing and mapping personal information flows associated with the Activities,
- identifying privacy risks and impacts of the Activities, including risks of non-compliance with the *Privacy Act 1988* (Cth) (**Privacy Act**), *My Health Records Act 2012* (Cth) (**MHR Act**), and *Healthcare Identifiers Act 2010* (Cth) (**HI Act**); and
- recommending strategies to reduce the likelihood and mitigate the impact of identified privacy risks.

We have also considered general community expectations around the handling of personal information, as well as the Agency's social licence, and have identified any corresponding reputational risks as part of our analysis.

Out of scope

We have assumed that the Agency has existing privacy operations which are compliant with Privacy Act and the HI 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 Activities may impact on them.

Additionally, we have not:

- assessed detailed technical security controls for the new functionalities;

[9] Emailed advice from the Agency, 11 August 2022

- conducted assessments of the third-party mobile app vendors that are Registered Portal Operators; or
- considered compliance requirements arising under legislation not identified as being in scope above.

We have not reviewed CDC to wallet functionalities as this was removed from the scope of works by the Agency.[10]

[10] Emailed advice from the Agency, 11 August 2022

Methodology

Information gathering

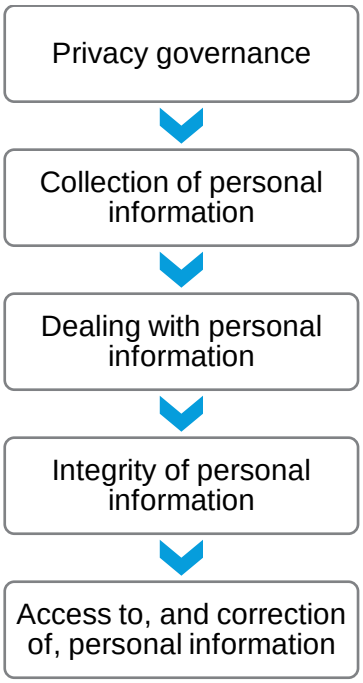
In our analysis, we have relied on information gathered through:

- documentation about the Activities supplied by the Agency;
- notes recorded during remote meetings with the Agency; and
- consideration of publicly available materials.

See Annexure 3 for more information on our 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, the MHR Act and the HI 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. **The list of relevant considerations is a summary only.**

Findings

Each finding in this document is presented as being either related to compliance, best practice, relevant to the management of RPOs or relating to Agency documentation.

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 findings 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.

In this report we have also made a number of recommendations relating to the reputational risks to the Agency that could arise from poor privacy practices by RPOs. These are identified using the prefix '**RPO**' and are included in the Privacy analysis section of this report. We have also made a number of recommendations relating to amendments to the Agency's PORA and associated documents, interoperability guidelines and developer centre materials (see Annexures 1 and 2).

Information Flows

This section describes how personal information will flow between entities participating in the Activities.

An information flow diagram is a visual representation that summarises the movement of personal information between participants in an activity.

Get XML view (pathology and diagnostic imaging)

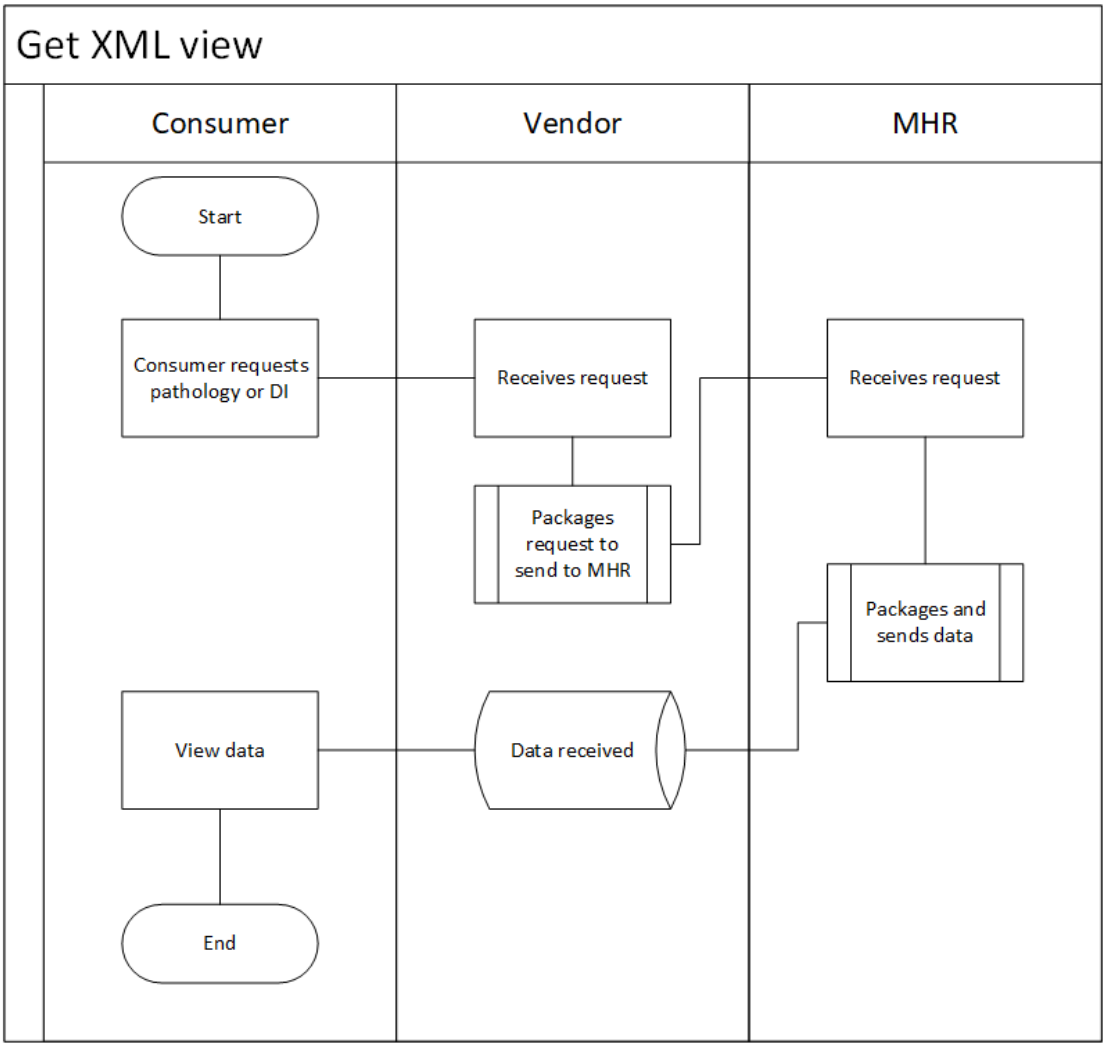
Types of personal information

The table below describes the types of personal information that will be handled in connection with the activity, and the individuals the information will be about.

	Type of individual	Personal information handled
Personal information	Mobile app user[11]	First name Last name Date of birth Gender Individual Healthcare Identifier (IHI)
	Healthcare provider	First name Last name Role Healthcare Provider Identifier – Individual HPI-I Healthcare Provider Identifier – Organisation HPI-O Referring Healthcare Provider Identifier – Individual HPI-I Referring Healthcare Provider Identifier – Organisation HPI-O
Health information	Mobile app user	Pathology reports Diagnostic imaging Health information request type (e.g., pathology) Report type Date of visitation or collection Test results Date the test results or report are issued Anatomical region of testing Examination type

[11] For the Activities we are assessing, a 'mobile app user' means a Healthcare Recipient or their Representative, as designated in the MHR system.

Information flow diagrams



Share function

Types of personal information

The table below describes the types of personal information that will be handled in connection with the activity, and the individuals the information will be about.

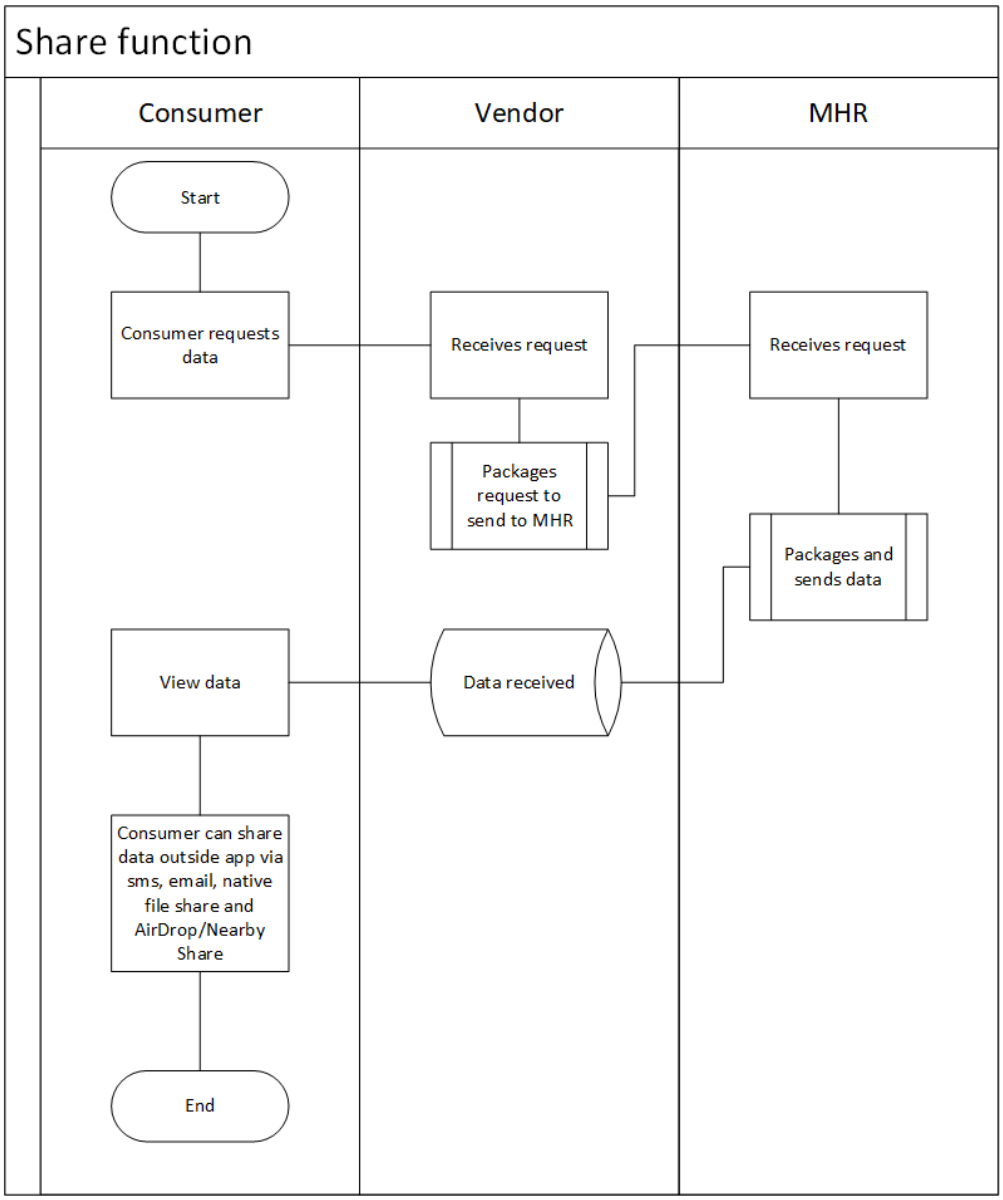
	Type of individual	Personal information handled
Personal information	Mobile app user	First name Last name Date of birth Gender Indigenous status Veteran/ADF status Phone number

	Type of individual	Personal information handled
		Work phone number Email address Address Workplace Emergency contact Organ donor status Height Weight Head circumference OAuth Token Unique user identifier
	Healthcare provider (individual)	First name Last name Role Address Phone number Email address Healthcare Provider Identifier – Individual HPI-I Healthcare Provider Identifier – Organisation HPI-O
Health information	Mobile app user	Individual Healthcare Identifier (IHI) We are advised[12] that all CDA documents and Immunisation History statement can be shared or stored natively, inclusive of the records listed below. Shared Health Summary e-Referral Specialist Letter Discharge Summary Event Summary Diagnostic Imaging Report Pathology Report Prescription Record Dispense Record Pharmacist Shared Medicines List Advance Care planning Document Goals of Care Document Australian Organ Donor Register Immunisation History Statement PBS and MBS Diagnosis of health issues Dates and details of diagnosis Dates and details of onset of symptoms

[12] Emailed advice from the Agency,

Type of individual	Personal information handled
	Dates and details of remissions and recoveries Advanced care directives

Information flow diagrams



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 implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code.
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

Privacy policy oversight

We have assumed that the Agency has existing privacy practices, procedures and systems which meet the governance requirements of the Privacy Act and will make use of those capabilities to develop, deploy, operate, and maintain the Activities.

The Agency has a publicly available privacy policy on its website (Agency Privacy Policy) which sets out how it handles personal information. The separate My Health Record Privacy Policy (MHR Privacy Policy) explains how the Agency, as System Operator under the MHR Act, collects, uses and discloses personal information to operate and manage the MHR system.

We note this PIA is primarily focused on the Agency's own obligations, however we consider it important to extend the analysis to the standards which the Agency is setting for RPOs given the Agency has the ability to incentivise alignment of the RPOs with privacy obligations and best practice.

As System Operator the Agency has the ability to ensure best practice in privacy policies and notices of third-party apps because of its power to grant or refuse registration. As these are crucial consumer protections, the Agency should adopt a hands-on approach in overseeing and approving app privacy policies.

Information about apps required in MHR Privacy Policy

There is no information on the disclosure of MHR data to RPOs currently in the MHR Privacy Policy we have accessed via https://www.digitalhealth.gov.au/about-us/policies-privacy-and-reporting/privacy-policy[13], except for mention that registered portal operators and registered RPOs must comply with security obligations outlined in the MHR Act and the My Health Record Rule 2016 to maintain eligibility for registration.

The MHR Privacy Policy requires updating to provide high level explanation of the fact of MHR data being accessed by the Agency's app and third-party app providers if individuals choose to use them and give consent. The MHR Privacy Policy should mention the features being made available to users – i.e. to download, store and share their MHR data and receive diagnostic and pathology images. We also suggest these revisions provide additional information on the ability to remove third-party app access, inclusive of the Agency's my health app.

Data retention

Under the PORA, RPOs are required to delete or destroy any information or data that may be accessed and used by the Portal Operator, including any information or data in or from a My Health Record (**System Data**), within 28 days of the data being obtained by the RPO from the System. While we were advised that RPOs would not be storing MHRs in order to implement the new functionalities, metadata relating to the handling of MHRs should not be over retained. It is our experience that explicit requirements to delete or destroy such as this can often by poorly implemented and, in our view, a risk of over retention of such data exists that without the application of additional controls by the Agency.

Findings

We have identified 1 compliance and 3 RPO recommendations in relation to open and transparent management of personal information.

Recommendations
COMPLIANCE REC. 1 We recommend a mobile app section be inserted into the MHR Privacy Policy including high-level plain English explanation of what RPOs offer (view, store, share, view images) and how RPOs will be required to manage MHR information. This would include explaining that RPOs are required to ask for permission for any use,

[13] Accessed in late August 2022

that users can revoke access at any time, and that RPOs are not permitted to keep System Data for longer than 28 days.
RPO REC. 1 Pre-registration point-in-time risk assessments and attestations do not provide ongoing assurance of compliance. The Agency should implement regular post-registration audits where any changes to risks and the data handling practices disclosed in pre-registration are actively sought out and understood by the Agency with a view to ensure continuing compliance with key mandatory requirements and recommended guidelines outlined in the Interoperability Requirements.
RPO REC. 2 The Agency should periodically review the privacy policies and notices of RPOs with respect to their apps to ensure they are in plain English and make necessary disclosures generally. The RPO onboarding documents should specify the Agency's role in monitoring privacy policies.
RPO REC. 3 The Agency should provide RPOs with a recommended list of clauses that should be used in privacy policies applicable to their mobile apps.

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	Any event that compromises security or integrity of health information contained in a healthcare recipient's My Health Record must be handled and notified in accordance with the My Health Record Act.
Notifiable Data Breaches Scheme	The Agency must notify affected individuals and the OAIC if a data breach is likely to result in serious harm to an individual whose personal information is involved.

Impact analysis

The PORA contains a robust set of data breach reporting requirements for RPOs (particularly clauses 5.11-5.16). We have also been provided the Security Requirements and Guidelines document for apps connecting to the MHR system. The document defines an incident and requires an incident management process be established. It contains references to the detailed incident management standards that should be adhered to. These are appropriate requirements.

Findings

We have made no findings on data breach response management.

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

The Activities will not have a material impact on the Agency's compliance with APP2.

Findings

We have made no findings relating to anonymity and pseudonymity.

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

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 15	The Agency is authorised to collect, use and disclose identifying information of a healthcare recipient, and their healthcare identifier for the purposes of the My Health Record system.
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
MHR Act 2012 s 58A	The System Operator may collect, use, and disclose identifying information, including a healthcare identifier, about a healthcare recipient where the collection, use or disclosure is for the purposes of the My Health Record system.
MHR Act 2012 s 58A	A Registered Portal Operator may collect, use, or disclose to a participant in the MHR System the healthcare identifier of a healthcare recipient where the collection, use or disclosure is for the purposes of the MHR system.

Impact analysis

The Activities in scope do not alter the nature of the Agency's collection of personal information. The collection by RPOs of personal information is limited to the provision of their app service and appropriately constrained by the requirements to comply with the Privacy Act (i.e. provide collection notices) and the security requirements in the PORA for deletion of System Data within 28 days.

We note the analysis and recommendations of the *MyHealth Record Mobile Apps* PIA we conducted in 2021 remain relevant. We have made a recommendation in section 1.1 above regarding enhancing the MHR privacy policy to provide important consumer information about MHR use by third-party apps.

Findings

We have made no findings in relation to collection.

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

We don't anticipate that the Activity will have a material impact on the volume or nature of unsolicited personal information that the Agency receives.

Findings

We have not identified any new risks 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.

Impact analysis

Notification will be the responsibility of the RPOs where relevant. We note this PIA is primarily focused on the Agency's own obligations, however we consider it important to extend the analysis to the standards which the Agency is setting for RPOs given the Agency has the ability to incentivise alignment of the RPOs with privacy obligations and best practice.

Notification matters are addressed in the use/disclosure section below.

Findings

We have not made any findings in relation to notification.

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 15	The Agency is authorised to collect, use and disclose identifying information of a healthcare recipient, and their healthcare identifier for the purposes of the My Health Record system.
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 2012 s 58A	The System Operator may collect, use, and disclose identifying information, including a healthcare identifier, about a healthcare recipient where the collection, use or disclosure is for the purposes of the My Health Record system.

MHR Act 2012 s 58A	A Registered Portal Operator may collect, use, or disclose to a participant in the MHR System the healthcare identifier of a healthcare recipient where the collection, use or disclosure is for the purposes of the MHR system.

Impact analysis

We note this PIA is primarily focused on the Agency's own obligations, however we consider it important to extend the analysis to the standards which the Agency is setting for RPOs given the Agency has the ability to drive alignment of the RPOs with privacy obligations and best practice.

Continuing checks

In determining whether to grant registration to an app developer, the Agency seeks information and attestations through a number of documents including the CCD Risk Assessment questionnaire, the PEAR form and the Conformance Vendor Declaration form. These enable decision-making on whether the applicant conforms to key mandatory requirements and recommended guidelines outlined in the Interoperability Requirements. However once onboarded and in operation, sophisticated apps are dynamic and subject to ongoing iteration such that data handling practices are likely to deviate over time from the disclosure made before registration. We have made recommendations for ongoing post-registration checks.

Oversight of consent practices

We consider the consent provisions of the PORA to be a core consumer protection. In particular:

> *5.24 Subject to the terms of this Agreement, you must only Use System Data in accordance with the informed consent provided by the relevant Registered Healthcare Recipient or their Representative, in accordance with the requirements of the My Health Records Act.*
>
> *5.25 You must ensure that, at or before the time that you seek consent from a Registered Healthcare Recipient or their Representative you explain each of your acts and practices that do or may fall within the scope of that consent (including that you may provide a copy of the consent to us), to ensure that the consent provided is explicit and informed.*
>
> *5.26 To the extent practicable you must ensure that consents are current and specific. You must minimise any use of any bundled or general consents.*

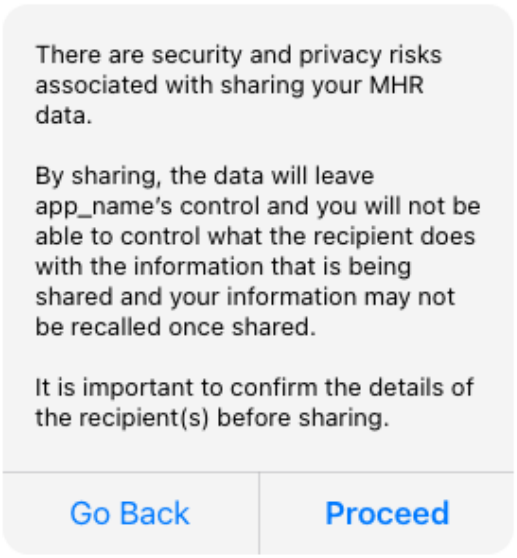


Figure 2 Warning to consumers required under the My Health Record FHIR Gateway Consent Requirements and Guidelines, Rec C012

As these clauses are essential for protection of users, it is important for the Agency to be prepared and equipped to address the tendency of sophisticated app operators to 'nudge' users into choices through use of shrewd wording or design features. In the case of MHR-integrated apps, there is a risk users will be nudged into agreeing to uses of data that are convenient for the RPO but where the implications are not fully understood by the user.

There is a growing literature on these 'dark patterns' in websites, apps and other digital interfaces.[14] Some of these practices may be easily categorised as deceptive, but there is a spectrum of more subtle influencing features that fall short of any legal definition of deceptive conduct. We have made a recommendation to explicitly prohibit this and for the Agency to request applicants provide their app's proposed consent requests, including design and presentation, to enable the Agency to prevent manipulative practices.

It also follows that in the event of an app presenting users with choices in a manner which the Agency considers in its discretion to be breaches of the PORA, the Agency should have the ability to achieve a rapid rectification. The Agency should be able to direct an RPO to cease a particular practice or to change a particular feature of their consent request or the wording of a disclosure to users. The direction should be backed by the sanction of de-registration.

Inadvertent disclosure of personal information in xml view

We are aware of the potential for medical professionals to have personal address and other contact details in pathology reports. We are aware of a recommended rendering process that would ensure these details are hidden when the image is rendered for the recipient.

Requirements for apps to warn about external sharing

[14] https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy; https://www.natlawreview.com/article/trends-data-privacy-regulation-dark-patterns

In-app notices may need to address how the data will also likely be subject to the handling practices of third parties as MHR-derived data is stored locally on individuals' devices or shared to other apps.

Rapid pass through of access permission changes

We note that both Nominated and Authorised Representatives (see 'References and Key Terms') will be able make use of the new functionalities to the extent that these are permitted line with the specific access permissions that are assigned to them in the MHR system. Potential harms could arise from the sharing of personal information by estranged family or friends or in cases of domestic violence. It is our view that such risks are more likely to arise in the case of Nominated Representatives, these being the category of representative likely to be a partner. We see the risk of reckless sharing of information by an Authorised Representative as significantly lower and note that these representatives are subject to more stringent controls in their appointment.

Therefore we have made a Best Practice recommendation seeking rapid pass through of any changes to Nominated Representatives' access permissions to RPOs. We have also recommended that advice to the public[15] regarding what Nominated and Authorised Representatives may be able to do (depending, in the case of Nominated Representatives, on their access level) with regard to MHR information sharing is updated to accurately reflect the new Share feature.

Findings

We have identified 1 compliance recommendations, 2 best practice and 4 RPO recommendations in relation to use and disclosure of personal information.

Recommendations
COMPLIANCE REC. 2 The Agency should require that RPOs implement a rendering process that would ensure unnecessary personal information of third parties such as an individual doctor's home address is not rendered in xml view images.
BEST PRACTICE REC. 1 The Agency should take steps to ensure that changes to access permissions granted by an individual to a Nominated Representative are passed through to RPOs as rapidly as technically possible to mitigate risk where there is potential harm from either continuing access or lack of access.
BEST PRACTICE REC. 2 The Agency should ensure that public facing advice regarding what Nominated and Authorised Representatives may be able to do (depending, in the case of Nominated Representatives, on their access level) with regard to MHR information sharing is updated to accurately reflect the new Share feature.

[15] For example, the advice that is provided on the Agency's website at https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record/getting-started/authorised-representatives and https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record/manage-your-record/privacy-and-access/nominated-representatives

RPO REC. 4 The Agency should insert a clause in the customer communications section of the PORA prohibiting the use of deceptive or manipulative practices including factual omissions, visual design features and any other factors relevant to app user decision-making.

RPO REC. 5 In pre-registration application documents including the PEAR and the CCD Risk Questionnaire, in the user stories sections, the Agency should require applicants to provide examples of the design and visual features surrounding the presentation of user decision points such as the decision to share an MHR.

RPO REC. 6 The Agency should provide RPOs with a recommended list of plain English alerts that should be displayed prior to common scenarios of user sharing. We recommend a prominent 'Before you share or save' header on these alerts. The alerts should be, for example, 'your data will be stored on your device/sent to your email address. MHR won't be protecting the data once you've downloaded it. Are you ok with this? Ok or go back'.

RPO REC. 7 The Agency should require as a condition of registration that that RPO privacy policies applicable to their apps alert or remind users that after MHR data is saved on their device it is subject to any automated cloud backup or other data handling enabled or agreed to by users for their devices with Apple iOS and Google Android operating systems.

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, and note also that the PORA explicitly prohibits direct marketing uses of MHR data.

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.
MHR Act s.77	The System Operator, a registered repository operator, a registered portal operator or a registered contracted service provider that holds records for the purposes of the My Health Record system must not hold, process or handle the records outside Australia.

Impact analysis

We do not consider the new Activities materially alter either the likelihood or the risks of cross-border disclosure.

Findings

We have not made any findings in relation to cross-border disclosure.

3.4. Government related identifiers

Relevant considerations

Individual Healthcare Identifiers (IHIs) are disclosed to RPOs for use in their apps and these identifiers are likely to fall within the scope of APP 9 as government-related identifiers. 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 9.2 relevantly provides that an organisation may use or disclose a government related identifier of an individual where:

a) reasonably necessary to verify the identity of the individual; or
b) if the use or disclosure is reasonably necessary for the organisation to fulfil its obligations to an agency (such as ADHA); or
c) as required or authorised by or under an Australian law.[16]

The HI Act also outlines the limited circumstances where IHIs and other healthcare identifiers may be used. We are not aware of specific provisions in this Act authorising RPOs to use healthcare identifiers although we note a number of provisions in Part 3 of the Act that may have the effect of permitting the use of identifiers by RPOs. In particular we note that

[16] OAIC, *Australian Privacy Principles Guidelines, Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers* https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers

Section 15 of the HI Act, and Section 58 of the MHR Act both permit the disclosure of the IHI for "the purposes of the My Health Record system". Section 3 of the MHR Act states that the object of the Act is: "to enable the establishment and operation of a voluntary national system for the provision of access to health information relating to recipients of healthcare, to:

(a) help overcome the fragmentation of health information; and

(b) improve the availability and quality of health information; and

(c) reduce the occurrence of adverse medical events and the duplication of treatment; and

(d) improve the coordination and quality of healthcare provided to healthcare recipients by different healthcare providers."[17]

Our analysis is that it is likely the RPOs' use of government related identifiers would come within the exception in APP 9.2 (b), this being the exception that refers to what is reasonably necessary for an organisation to fulfill obligations to an Agency – i.e. the proper functioning of apps is necessary for the fulfillment of the RPO's obligation to ADHA under the PORA.

With regard to IHIs, it is our view that the disclosure of IHIs to RPOs occurring under the proposed Activities falls under the purposes of the My Health Record system as described in the MHR Act, and so is permitted under section 58 of the IHI Act.

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 under the Activities is accurate, up-to-date and complete and relevant and not misleading.

Impact analysis

We do not consider the new Activities materially alter either the likelihood or the risks of data quality issues arising for the Agency. However, there is a risk of data that is low quality

[17] *My Health Records Act* 2012 (C'wealth), Section 3 'Object of Act'

accumulating externally due to sharing of MHR data outside of the Agency's control. This is addressed in security and use sections.

Findings

We have not made any findings in relation to quality of personal information.

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

Highlighting prohibition on retention

We are aware of academic research involving large-scale analysis of 20,000 mobile health apps. The research shows these apps are on average better aligned with security best practices than non-health apps. However, the same research also finds a significant proportion of health apps falling short on important security practices.[18]

We note clause 5.3 of the draft PORA provided to us requires Registered Portal Operators (RPOs) to delete or destroy the System Data they have either downloaded or copied within 28 days. System data is defined as including MHR data. We have also been informed there is no technical control available that could prevent retention by RPOs, with the Agency relying on contractual obligations, threat of penalties imposed by MHR legislation and audits by the Agency.

Our view is the retention of MHR data by RPOs, either deliberate or inadvertent, remains a key risk and have made recommendations to mitigate this to the extent possible including plain English communications for RPOs that would highlight the prohibition on retaining data and emphasise user consent cannot be sought for retention.

Risks of data leakage

[18] Gioacchino Tangari et al *Analyzing security issues of android mobile health and medical applications*, Journal of the American Medical Informatics Association : JAMIA, 28: 10, Oct 2021

Our interviews with the Agency's information security professionals demonstrated their awareness that the app ecosystem is a dynamic and commercially driven space where there is likely to be use of advanced tracking and analytics designed to measure app performance and the use of mobile app advertising networks that bring with them privacy and security risks to consumers, including tracking. We have been made aware that apps are often developed with software development kits (SDKs) from social media and digital advertising firms and these entail security vulnerabilities.[19]

The Agency has made efforts to reduce the risk of misuse of MHR data by strict contractual controls and robust self-attestations backed by criminal penalties. In view of these requirements there is a view that there is already a filter for firms with more mature governance. A decision has been made not to require regular penetration testing on the basis the cost would potentially limit the number of firms able to participate in the MHR services. However, there may be a limited effect if the RPO participants are already filtered for only more established firms with financial resources. There is a possibility for other forms of technical audit to also be considered. In the absence of ongoing audits and technical oversight such as penetration testing which monitors 'under the hood' of the third-party apps, there is some risk that is being accepted.

Findings

We have identified 3 RPO recommendations in relation to the security of personal information.

Recommendations
RPO REC. 8 Create plain English communications, separate from contractual documents, targeted at staff of RPOs, highlighting among other obligations that retention of System Data after 28 days is a blanket prohibition.
RPO REC. 9 Ensure resourcing of Agency audit or conformance functions so that regular reviews of data retention and handling practices of RPOs are maintained over time and RPOs are incentivised to comply with deletion and handling requirements.
RPO REC. 10 Perform periodic technical audits of RPOs to test cyber security measures. Such audits should include penetration testing.

4.3. Retention

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

[19] https://www.techtarget.com/searchsecurity/answer/How-do-SDKs-for-ad-networks-cause-data-leaks

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.
APP 11.2	An APP entity must take reasonable steps to destroy personal information or ensure it is de-identified if it no longer needs the information for any purpose for which it may be used or disclosed under the APPs (APP 11.2)

Impact analysis

We do not consider the new Activities materially alter the risks around retention by the Agency. The risk of retention by RPOs is addressed in the security and use sections.

Findings

We have not made any findings in relation to retention.

4. Access to, and correction of, personal information

4.1. 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 data, 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 do not consider the new Activities materially alter the risks around access and correction for the Agency. The requirements for RPOs to have access and correction measures in place is addressed by the terms in the PORA requiring they comply with the Privacy Act.

Findings

We have not made findings in relation to access and correction.

References and Key Terms

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

Activities, the	means the functionalities that are described as in scope for this PIA in the 'About this PIA' section of this document
Agency	means the 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
Agency rule	Means the *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule 2016* (Cth)
AHPRA	means the Australian Health Practitioner Regulation Agency.
Australian Privacy Principles or **APPs**	means the 13 Australian Privacy Principles set out in Schedule 1 of the Privacy Act.
Authorised representative	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.
CDA	means Clinical Document Architecture, a Health Level 7 (HL7) standard that provides a framework for the encoding, formatting and semantics of electronic documents.
Contracted Service Provider or **CSP**	has the meaning given in the HI Act.
FHIR	means Fast Health Interoperability Resources
Health Information	has the meaning given in subsection 6(1) of the Privacy Act.
Healthcare Identifiers Act or **HI Act**	means the Healthcare Identifiers Act 2010 (Cth).

Healthcare Provider Identifier or **HPI**	means an individual IHI, an HPI-I or an HPI-O.
Healthcare Provider Identifier-Individual or **HPI-I**	has the meaning given in the HI Act.
Healthcare Provider Identifier-Organisation or **HPI-O**	has the meaning given in the HI Act.
HI Service	means the Health Identifier Service operated by the Chief Executive Medicare under the HI Act.
HL7	means Health Level Seven, a standard for exchanging information between medical information systems
IHI	means Individual Healthcare Identifier.
Individual Healthcare Identifier or **IHI**	has the meaning given in the HI Act.
Information Commissioner	means the Australian Information Commissioner.
MHR System	means the My Health Record system operated by the Agency.
my health	means the my health mobile app developed by the Agency
Nominated representative	means a representative who is provided access to a My Health Record by the individual or the individual's authorised representative. A nominated representative can view health information. A nominated representative with read-only access is not required to provide any evidence of identity to the System Operator.
PEAR	means Production Environment Access Request
Personal Information	has the meaning given in section 5 of the Privacy Act.
Portal Operator Registration Agreement or **PORA**	means the agreement between the Agency and entities applying to become Portal Operators. For this PIA we reviewed the version of the PORA as listed in Annexure 3.
Privacy Act	means the *Privacy Act 1988* (Cth).
Privacy Code	means the *Privacy (Australian Government Agencies — Governance) APP Code* 2017 (Cth).
Risk Management Strategy, Framework and Policy or **Risk Framework**	Means the document of the same name and at the time of writing, provided to elevenM by the Agency.
RPO	means Registered Portal Operator

System Data	means any information or data that may be accessed and used by the Portal Operator, including any information or data in or from a My Health Record
TEAR	means Test Environment Access Request

Annexure 1: Interoperability guidelines & developer centre materials review

In this Annexure, we have provided a number of recommendations that relate to the Interoperability Guidelines and Developer Centre materials provided to us by the Agency. In some instances these recommendations relate to or complement our findings in the Privacy analysis section of this report. We have indicated where this is the case. We have numbered the recommendations in this Annexure using an 'IGDC' prefix.

App Vendor Guide to the Connection Process v1.1

This document describes the process involved in developing an application (app) that connects with the My Health Record system. We have made no recommendations relating to the content of this document.

My Health Record Managing Your App in Production v2.8

This document outlines the process for notifying the My Health Record system operator (System Operator) about incidents and other events, such as changes and upgrades to apps that connect to the My Health Record system.

- **IGDC REC. 1** It is recommended that Table 1– Incident types is updated to include 'Privacy' incident scenario examples that describes an incident involving the In-app share function. Such a scenario could involve, for example, a failure to share all documents when multiple attachments exist.
- **IGDC REC. 2** It is recommended that, to highlight the fact of retention beyond 28 days being considered an incident, a separate incident scenario example is inserted in Table 1 – Incident types under 'Privacy' to the effect of: "System Data is retained by a developer's app after 28 days.

My Health Record FHIR Gateway Consent Requirements and Guidelines v1.1

This document defines the consent requirements and guidelines for apps connecting with the My Health Record system APIs via the FHIR standard gateway, using interaction models #1 or #4. We have made no recommendations relating to the content of this document.

My Health Record FHIR Gateway - Security Requirement and Guidelines v1.1

This document defines the mandatory security requirements and recommended security guidelines for apps connecting with the My Health Record system APIs via the FHIR standard gateway, using interaction models #1 or #4.

It is recommended that:

- IGDC REC. 3 S4109 'Access authorised document types only via the GetDocument API' is amended to reflect the ability for app vendors to enable the viewing of pathology and diagnostic imaging reports using the GetXML API.
- IGDC REC. 4 S4116 'Erase information assets from mobile devices following multiple unsuccessful attempts to unlock mobile apps' is amended to include explicit reference to any MHR information stored natively on the user's device.

See also Compliance Recs 6 and 7 in the Privacy analysis section of this report.

My Health Record FHIR Gateway - API Specification v2.3

This document provides an overview of the API specifications required by developers to connect applications (apps) to the My Health Record system.

It is recommended that:

- IGDC REC. 5 The recently added section 'Add CDC Wallet' is removed from section 3.4 and from Appendix A.

My Health Record FHIR Gateway - Presentation Requirements and Guidelines v1.1

This document provides developers of applications (apps) accessing the My Health Record system through its FHIR Gateway with guidelines and requirements for the on-screen presentation of structured, non-CDA My Health Record data.

It is recommended that:

- IGDC REC. 6 Requirements are added to 3.1.3 Consumer demographics that require the printing of the record owner's demographic data on every page when the consumer:
    - shares a record using native mobile device sharing capabilities
    - stores a record using native file storage on a mobile device
- IGDC REC. 7 Requirements are added to 3.1.3 Consumer demographics so that when consumer apps are capable of storing records for consumers other than the current user using native file storage on a mobile device the app prints the record owner's demographic data on every page.
- IGDC REC. 8 Requirements are added to 3.1.3 Consumer demographics so that when consumer apps are capable of sharing records for consumers other than the current user using native sharing capabilities on a mobile device the app prints the record owner's demographic data on every page.

See also Best Practice Rec 4. in the Privacy analysis section of this report.

My Health Record FHIR Gateway - Release Note v2.3.0

This document is part of a series of updated to the technical specifications enable developers to connect applications to the My Health Record system via the FHIR® Gateway. We have made no recommendations in relation to the content of this document.

My Health Record FHIR Gateway Operations Requirements and Guidelines v1.1

The purpose of this document is to define the operations requirements and guidelines for applications (apps) connecting with the My Health Record system APIs via the My Health Record FHIR Gateway, using interaction models #1 or #4

It is recommended that:

- IGDC REC. 9 The introductory text to Appendix A is amended to include reference to 'sharing' amongst the ways that apps may be configured to process MHR information.

Annexure 2: Portal Operator Registration Agreement review

We have reviewed the Portal Operator Registration Agreement (PORA) and related documents including the Production Environment Access Request (PEAR) Form, the Portal Operator Registration Form (PORF), the Test Environment Access Request (TEAR) form, the Conformance Vendor Declaration Form and the CCD Risk Based Approach Risk Assessment Questionnaire.

For our recommendations pertaining to the PORA and related documents please refer to the following recommendations in the Privacy analysis section of this report:

- RPO recommendation 4;
- RPO recommendation 5; and
- RPO recommendation 7.

Annexure 3: Interviews conducted and documents reviewed

Interviews

Compliance and Conformance/Data Quality: Friday, 19 August 2022 9:30 AM-10:00 AM

Clinical Safety and Governance: Thursday, 18 August 2022 4:00 PM-5:00 PM

Cyber Security: Monday, 17 August 2022 1:00 PM-2:00 PM

Ops and Implementation: Tuesday, 16 August 2022 4:00 PM-5:00 PM

Policy and Legal: Monday, 15 August 2022 4:00 PM-5:00 PM

Privacy and Product: Tuesday, 9 August 2022 2:30 PM-3:30 PM

Documents supplied by the Agency

Analyzing security issues of android mobile health and medical applications.pdf

Copy of NEHTA_2055_2015-1_eHealth Pathology Report View Data Usage Guide v1.0.xlsx

Current Privacy Policies for Mobile Vendor Onboarding PIA SECOFFICIAL.msg

DH -3555.2021 App Vendor Guide to the Connection Process v1.1.docx

DH -3556.2021 My Health Record_Managing Your App in Production_v2.8.docx

DH_3087_2020_MyHealthRecordFHIRGateway_OperationsRequirementsandGuidelines_v1.1 (1).docx

DH_3088_2020_MyHealthRecordFHIRGateway_ConsentRequirementsandGuidelines_v1.1 reviewed.docx

DH_3089_2020_MyHealthRecordFHIRGateway_SecurityRequirementsandGuidelines_v1.1 (1).docx

DH_3119_2020_My Health Record_Conformance Vendor Declaration Form.docx

DH_3409_2021_MyHealthRecord_FHIRMobileGatewayCCDRiskBasedApproachRiskAssessmentQuestionnaire_v1.0.docx

DH_3557_2021__MyHealthRecordFHIRGateway_ErrorMapping_v2.3.0 dv016.xlsx

DH_3558_2021__MyHealthRecordFHIRGateway_DataMapping_v2.3.0 dv014.xlsx

DH_3559_2021__My Health Record FHIR Gateway - API Specification v2.3.0 dv044.docx

DH_3628_2022_MyHealthRecord_PortalOperatorProductionEnvironmentAccessRequestPEARForm_v3.6 (VK).docx

DH-3090.2020_My Health Record FHIR Gateway - Presentation Requirements and Guidelines v1.1_dv006 recent.docx

DH-34572021 My Health Record - Portal Operator Registration Form (PORF) v5.2 (002).docx

DH_3423_2021_MyHealthRecordB2BGatewayServices_ViewServiceTechnicalServiceSpecification_v2.0

DH-34582021 My Health Record - Test Environment Access Request (TEAR) form v5.1.docx

DH-3668_2022__My Health Record FHIR Gateway - Release Note v2.3.0.docx

Healthcare Privacy Publisher_version_open_access_.pdf

High Level Architecture.pptx

MicrosoftTeams-image (1).png

MicrosoftTeams-image.png

Mobile vendor onboarding PIA July 28 2022.pptx

Mobile health and privacy Cross sectional study.pdf

'my health' app glossary v1.0.docx

My Health Record Mobile Gateway - Portal Operator Monitoring and Audit Framework (Draft)

My Health Record_Portal Operator Registration Agreement (PORA Phase 1) v21122021_DRAFT (002).docx

NEHTA_2055_2015_eHealthPathologyReportView_PresentationGuide_v1.1.pdf

ThinkPlace - ADHA mHealth App Consumer Insights Report v1.0.pdf

elevenM research

Gioacchino Tangari et al, ‘Analyzing security issues of android mobile health and medical applications’, *Journal of the American Medical Informatics Association* : JAMIA, 28: 10, Oct 2021

OAIC, *Australian Privacy Principles Guidelines* https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines

OAIC Submission to the My Health Record Act Review 2020.pdf

OAIC *Australian Community Attitudes to Privacy Survey 2020*