elevenM

Australian Digital Health Agency

My Health Record Mobile Apps

Privacy Impact Assessment

Version 1.0

24/01/2022

Contents

Document control

Version	Date	Comments	Author
0.1	10/12/2021	Initial draft	elevenM
1.0	24/01/2022	Final version	elevenM

Context

- In 2021, the Australian Digital Health Agency (the **Agency**) engaged elevenM (**we, us, our**) to deliver a Privacy Impact Assessment (**PIA**) on two initiatives involving the sharing and use of My Health Record (**MHR**) information:
    - the SA DPC proof of concept (**SA DPC POC**) for a home quarantine application process involving the downloading and use of MHR records; and
    - the implementation of the next phase of mobile applications delivering information to consumers via the My Health Record Mobile Gateway (**Mobile apps**), including an app (the **myhealth app**) developed by the Agency itself.
- For each of these initiatives elevenM provided the Agency with a set of preliminary recommendations, to be followed by a comprehensive PIA for each. This document is the comprehensive PIA for the myhealth app and Mobile apps initiative.
- In this document we provide a detailed Privacy Impact Assessment of the Mobile apps initiative. The scope of this assessment is detailed in the *Scope* section of this document (page 14).
- Where we refer to '**the Activities'** we are referring to all Mobile apps inclusive of the myhealth app. When we refer to '**the myhealth app'** we mean only the app currently under development by the Agency in partnership with a vendor (**Chamonix**).

Executive summary

The Agency has engaged elevenM to conduct a PIA in relation to the introduction of new app-based functionalities for consumer users of the My Health Record system, specifically the functionalities of downloading, storing and sharing records via mobile applications (the Activities).

The new functionality will be made available to mobile apps through My Health Record system APIs (**MHR Gateway**). At this point in time the new functionality is being implemented in two contexts that we have been asked to assess:

1. The Australian Digital Health Agency (**the Agency**) is developing a My Health Record (**MHR**) consumer mobile application in partnership with Chamonix IT Solutions. The app, titled 'myhealth', will provide MHR users with a mobile option to complement other access channels to the MHR system, and permit the download, storing and sharing of the user's health information from within the application. The myhealth app will also supply data to the Agency that will be used for reporting purposes, such as data on usage, performance and
2. The Agency is making the functionality to download, store and share a user's health information available as an interaction model to other developers of consumer facing mobile apps provided by app developers who are Registered Portal Operators, such as (but not limited to) Telstra Health.

The Agency intends to continue to develop both its own app and the My Health Record system's capabilities over time with the goal of parity between the web My Health Record data and mobile consumer apps that are authorised to interact with it.

Compliance recommendations

We have identified 7 compliance recommendationss.

The table below sets out the compliance recommendations in the order they appear in the *Privacy analysis* section of this document (page 25).

Where recommendations have changed from the versions shared in the preliminary recommendations or are new, we have indicated this.

We note that while some recommendations are made with reference to the design of the myhealth app, they may also have relevance to the operation of third party apps and should be considered by the Agency in the revision of the PORA and guidelines for third party app developers. These have been identified with a note to this effect.

COMPLIANCE REC. 1 With regard to the feature parity plan, prior to the introduction of the upload features proposed for the mobile apps, the Agency should revise the MHR Privacy Policy to reflect the new types of information that the Agency may collect from users via the apps.

COMPLIANCE REC. 2 In order to be well positioned for the arrival of upload features under the feature parity plan, it is recommended that the Agency adds a privacy notice to the first use sign in experience for new users of the myhealth app (e.g. on the "Before you begin" screen), setting out the matters required under APP 5.2 including the types of personal information collected by the App, the purposes for which the information is collected, and providing a link to the MHR privacy policy.

COMPLIANCE REC. 3 In order to be well positioned for the arrival of upload features under the feature parity plan it is our recommendation that, prior to the roll out of the upload feature, the consent screen be revised to include a separate dot point after '(app name) can access information..' to advise users that by consenting that '(app name) will be able to make changes to their My Health Record'.

Note that this recommendation will be relevant to any third party apps authorised to incorporate this feature.

COMPLIANCE REC. 4 It is recommended that the Agency apply the draft Consent Requirements and Guidelines (**Consent Requirements**)[1] to the myhealth app – presently, the "Connect to My Health Record" consent screen (ONB 9.2) does not include the additional detail described in the Consent Requirements, such as a link which shows the user more detail on how the app interacts with the MHR and links to applicable privacy policies. See in particular req. 007 in the Consent Requirements.

COMPLIANCE REC. 5 It is recommended that the Agency add words to the following effect to the bullet point description on the "Connect to My Health Record" consent screen (ONB 9.2): "you can use myhealth to share data from your My Health Record with others using your mobile device."

Note that this recommendation will be relevant to any third party apps authorised to incorporate this feature.

COMPLIANCE REC. 6 We recommend that cached MHRs remain visible for the following lengths of time (after which access is prevented until the user's device is online and the user's access rights are confirmed):

- for nominated representatives – 24 hours
- for authorised representatives – 72 hours

We further recommend that this timeframe be communicated to users in the myhealth app and through separate materials on the MHR website.

Note that this recommendation will be relevant to any third party apps authorised to incorporate this feature.

COMPLIANCE REC. 7 It is recommended that the Agency reviews the PORA to ensure that portal operators must purge data relating to a user's MHR as soon as reasonably possible if the user revokes consent for the portal operator to access their MHR.

[1] DH_3088_2020_MyHealthRecordFHIRGateway_ConsentRequirementsandGuidelines_v1.1, supplied by the Agency

Best practice recommendations

We have have made 11 best practice recommendations that are not compliance risks to the Agency but are worthy of being outlined in this context.

The table below sets out the observations in the order they appear in the *Privacy analysis* section of this document (page 25).

Where recommendations have changed from the versions shared in the preliminary recommendations or are new, we have indicated this.

We note that while some recommendations are made with reference to the design of the myhealth app, they may also have relevance to the operation of third party apps and should be considered by the Agency in the revision of the PORA and guidelines for third party app developers. These have been identified with a note to this effect.

BEST PRACTICE REC. 1 It is recommended that the Agency updates information published on the MHR website (such as the content set out at https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app) with more details on how the download, store and share functionality works, including details on security arrangements to ensure that third party apps don't view or use data contained in MHRs.

BEST PRACTICE REC. 2 It is recommended that the Agency considers ways to improve the readability score of the existing MHR privacy policy (in line with the OAIC's recommendations for privacy policies). This could include:

- revising and rewriting content in order that it can be understood by people of all ages and education levels
- adopting a layered approach (by creating a summary of the policy which links to detail within the policy)
- reformatting the document to make it easier to navigate.

Note that this recommendation also appears in the comprehensive PIA for the SA DPC POC (see the Context *section for more detail).*

BEST PRACTICE REC. 3 It is recommended that the Agency add additional content to the MHR privacy policy explaining both the Agency's operation of the myhealth app and the new download, store and share functionality available to all authorised third party apps in more detail.

BEST PRACTICE REC. 4 It is recommended that the Agency add additional detail to the MHR privacy policy or related materials on the MHR website describing how to remove third party app access.

BEST PRACTICE REC. 5 It is recommended that, as a matter of Agency policy, the Agency documents and communicates internally the Agency's commitment to adhering to the same standards with regard to the handling of personal information that it has set for third party app developers that are authorised to interact with the MHR system.

BEST PRACTICE REC. 6 It is recommended that Agency procedures for the collection of mobile apps data for reporting and analytics purposes explicitly prohibit the inclusion of identifiers, such as unique device identifiers or any other data types that could reasonably identify an individual.

BEST PRACTICE REC. 7 It is recommended that the Agency add a menu item to the "About the app" view (ACC1.0D and ACC1.1D) titled "App access" (or words to that effect) which contains information about the App's access to the user's MHR, as well as with instructions as to how users can revoke the App's access to the user's MHR. When reasonably possible, add functionality to allow users to revoke access from within the App.

BEST PRACTICE REC. 8 When the App is offline (i.e. unable to connect to a server), it is recommended that the app clearly indicates to users that the app is offline, and that any information they are viewing has not been refreshed and may not be up to date.

BEST PRACTICE REC. 9 If including functionality to allow users to manually refresh a view, it is recommended that the Agency includes text to show when the current view was last refreshed.

BEST PRACTICE REC. 10 Ensure that the App includes a warning to users before they use the share functionality that:

- there are security and privacy risks associated with sharing their MHR
- that by sharing, the data will leave the Agency's control and the user will not be able to control what the recipient does with the information that is being shared
- it is important to confirm the details of the receipient(s) before sharing.

BEST PRACTICE REC. 11 We recommend that functionality to allow users to change permissions for nominated representatives using the app rather than having to go to the website is prioritised in the feature parity plan. In the meantime we recommend:

- a prominent notice to users to indicate that their records are shared with nominated or authorised reps, where applicable
- for users with nominated representatives, clear instructions in the app on how to change permissions via the national portal.

BEST PRACTICE REC. 12 We recommend that the proposed method for enabling a nominated or authorised representative to use the MyHealth app without having a MHR account is reviewed to avoid reliance on the sharing of MyGov user authentication details.

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 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.

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.

Mobile apps for consumers of My Health Record healthcare information

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"[3]. 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 developing its own consumer-facing mobile app, myhealth.

Third party mobile applications

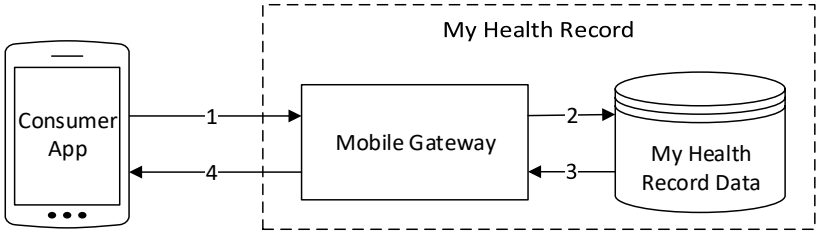
Authorised mobile applications connect to the My Health Record system via the system's Fast Health Interoperability Resources (**FHIR**) standard gateway which supports two interaction models for consumer-focused applications:

[3] Australian Digital Health Agency, *Corporate Plan 2021 – 2022* https://www.digitalhealth.gov.au/sites/default/files/documents/adha-corporate-plan-2021-2022.pdf

- 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.

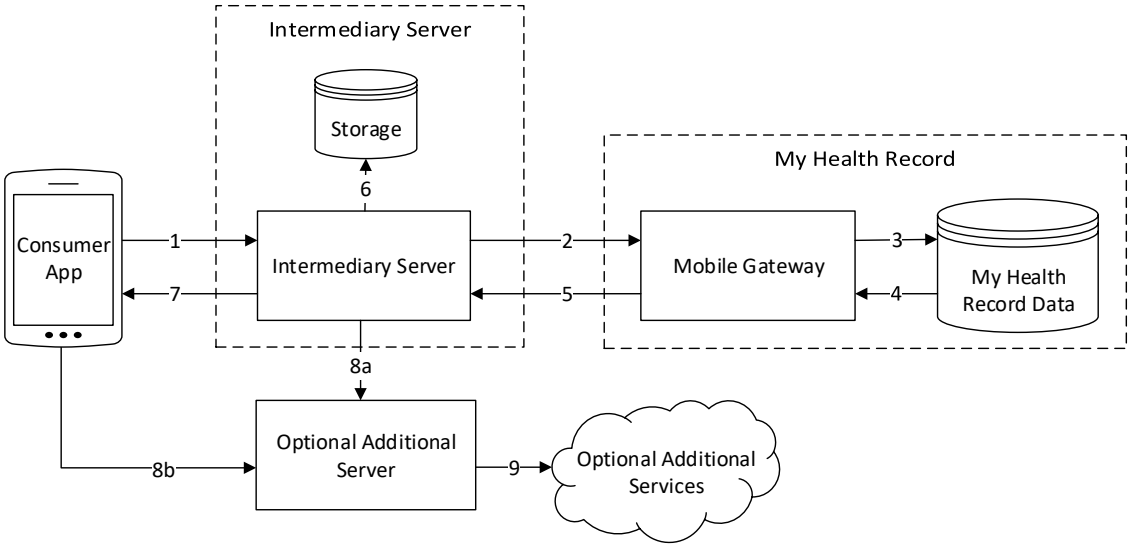
These interaction models are described in more detail below.[4]

Interaction Model #1 – Consumer / Self-Care



Step #	Description
1	Consumer App sends a request for data to the Mobile Gateway.
2	Mobile Gateway forwards the request for data to the My Health Record system.
3	My Health Record system sends the data to the Mobile Gateway.
4	Mobile Gateway pushes the data to the Consumer App.

Interaction Model #4 – Consumer Connection via Platform



[4] Mobile Enablement Interaction Models Data Flows (document supplied by the Agency)

Step #	Description
1	Consumer App may send a request for data to the Intermediary Server.
2	Intermediary Server pushes the request for data to the Mobile Gateway.
3	Mobile Gateway forwards the request for data to the My Health Record system.
4	My Health Record system sends the data to the Mobile Gateway.
5	Mobile Gateway pushes the data to the Intermediary Server.
6	Intermediary Server may store the data.
7	Intermediary Server pushes the data to the Consumer App (e.g. data processing).
8a	Optionally, Intermediary Server may push the data to an additional server. This may be internal within the vendor's infrastructure or external (e.g. third party).
8b	Optionally, the Consumer App may push data directly to an additional server. This may be internal within the vendor's infrastructure or external (e.g. third party).
9	Optionally, the additional server may utilise the data for additional services (e.g. secondary use).

Myhealth

The Agency is developing mobile channel which will complement other digital health channels connected to the My Health Record system. Mobile applications for iOS, iPad OS and Android.

The successful tenderer for the development of the apps was Chamonix. The project is taking an existing app that has been operated by Chamonix (Healthi) and will be making design changes, inclusive of rebranding as 'myhealth', different ways of presenting information and some changes required for COVID management.

We have been advised by the Agency[5] that:

> "The contract for the provision of a Digital Health Mobile Channel with Chamonix IT Management Consulting (SA) sees Government (the Agency) owning all the Intellectual Property (IP) for the current Healthi App from which Agency can then build enhancements. As part of the contracted engagement, Chamonix will build user experience and functionality enhancements to the product before release. The contract also includes 12 months support, with two 12-month options to extend as the Agency transitions IP and aligns our functional structures to support mobile channel."

[5] Email to elevenM from Murray Woodford, ADHA, 26/11/2021

The Agency is planning for internal release of the app on February 4, 2022, and a limited public release on 18 February 2022.

Use of mobile app data for reporting

The RFT for the project to develop the myhealth app for the Agency[6] includes a set of requirements relating to Reporting. These indicate the data that is proposed for routine collection and analysis by the Agency for the purposes of reporting to stakeholders including the Government.

Annexure 1 describes the types of data that are to be collected for reporting purposes in detail and the sources of the data, including the mobile app. Broadly speaking the data falls into the categories of:

- user activity (number of users, downloads, views for example),
- sentiment (user surveys, likes) and
- performance (crashes, complaints).

Where the data comes from an individual's use of the app, it is stored both in the app and the intermediary server. We have not seen any indication in the information provided that the data collected for reporting purposes contains identifiers for individuals. However, we have included a Best practice recommendation in the 'Privacy Analysis' section of this document relating to the collection and use of mobile app data that is designed to manage any risk of improper handling or use of personal information as part of the proposed collection and use of this data (see 2. Collection of personal information).

[6] Consumer Mobile App v0.04, supplied by the Agency

Scope

This PIA report focusses on the privacy impacts that the introduction of the myhealth mobile app and the download and store features will have on individual privacy, including compliance and other privacy issues affecting the Agency, and recommends steps to mitigate negative impacts. This document represents a holistic consideration of the practical privacy impacts of the apps and is not legal advice.

Any differences between the design of the apps 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 assessed the privacy impacts associated with:

- third party mobile apps operated by Registered Portal Operators taking up new download and store features;
- the Agency's own mobile app, myhealth, currently under development, including the proposed uptake of the download and store features; and
- the collection and use of mobile app data for reporting purposes.

As noted in the 'Context' section of this document (page 4) Where we refer to '**the Activities'** we are referring to all Mobile apps inclusive of the myhealth app. When we refer to '**the myhealth app'** we mean only the app currently under development by the Agency in partnership with a vendor (**Chamonix**).

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**);
- requirements to carry out a PIA under the Privacy Code;
- 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 Activities;
- considered compliance requirements arising under legislation not identified as being in scope above.

Methodology

Information gathering

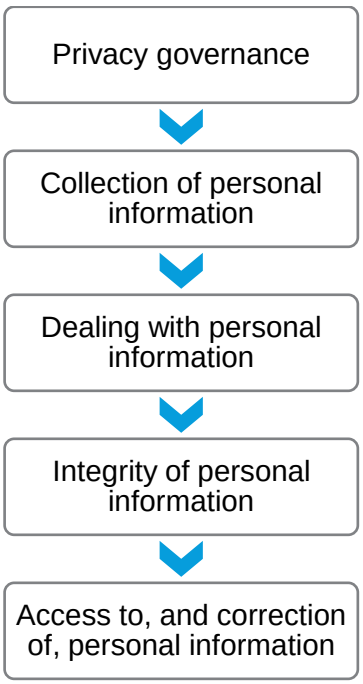
In our analysis, we have relied on information gathered through:

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

See *References and key terms* 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, 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 ‘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 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.

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.

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 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.

Types of personal information

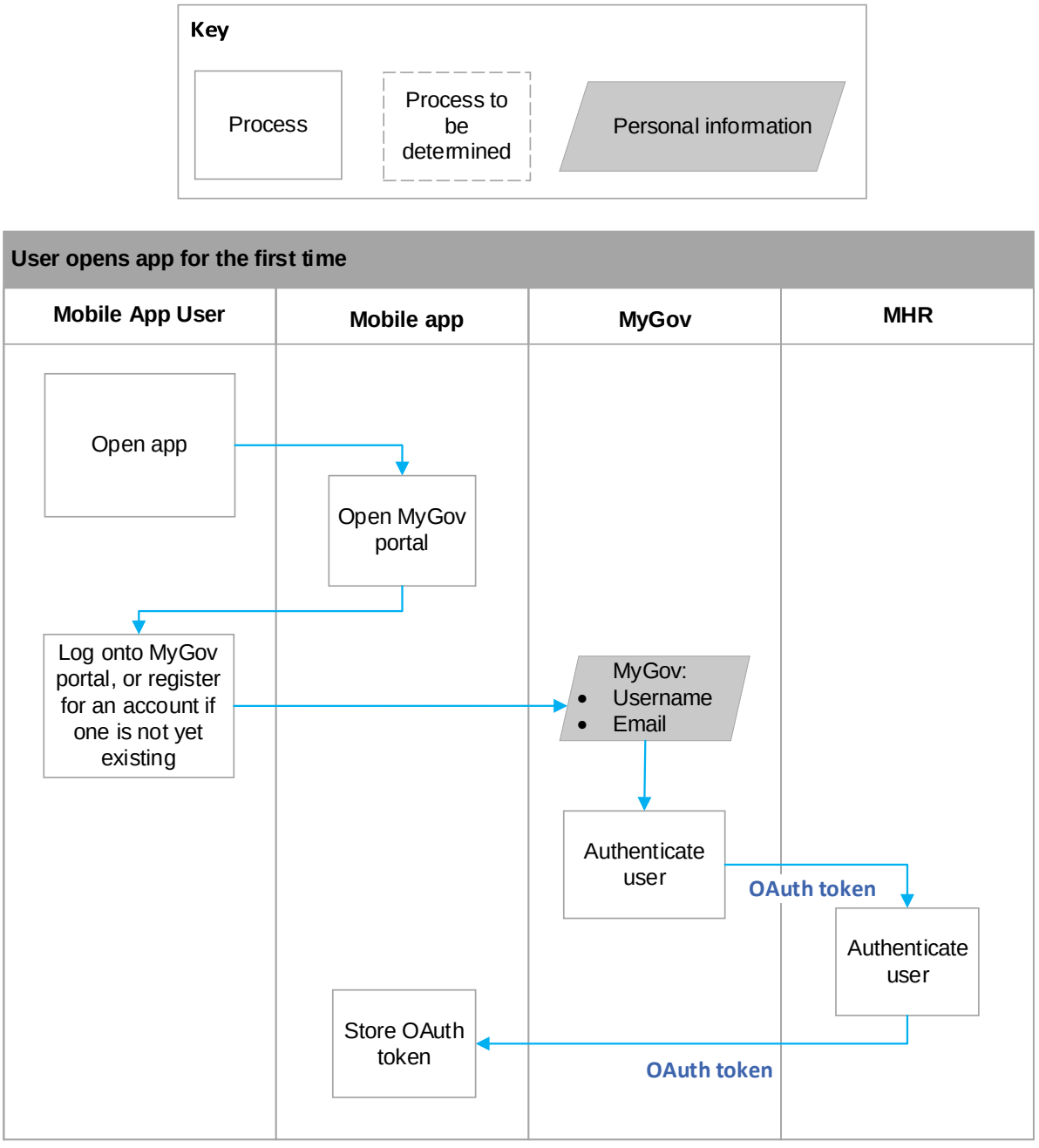
The table below describes the types of personal information that will be handled in connection with the Activities, and the individuals the information will be about.

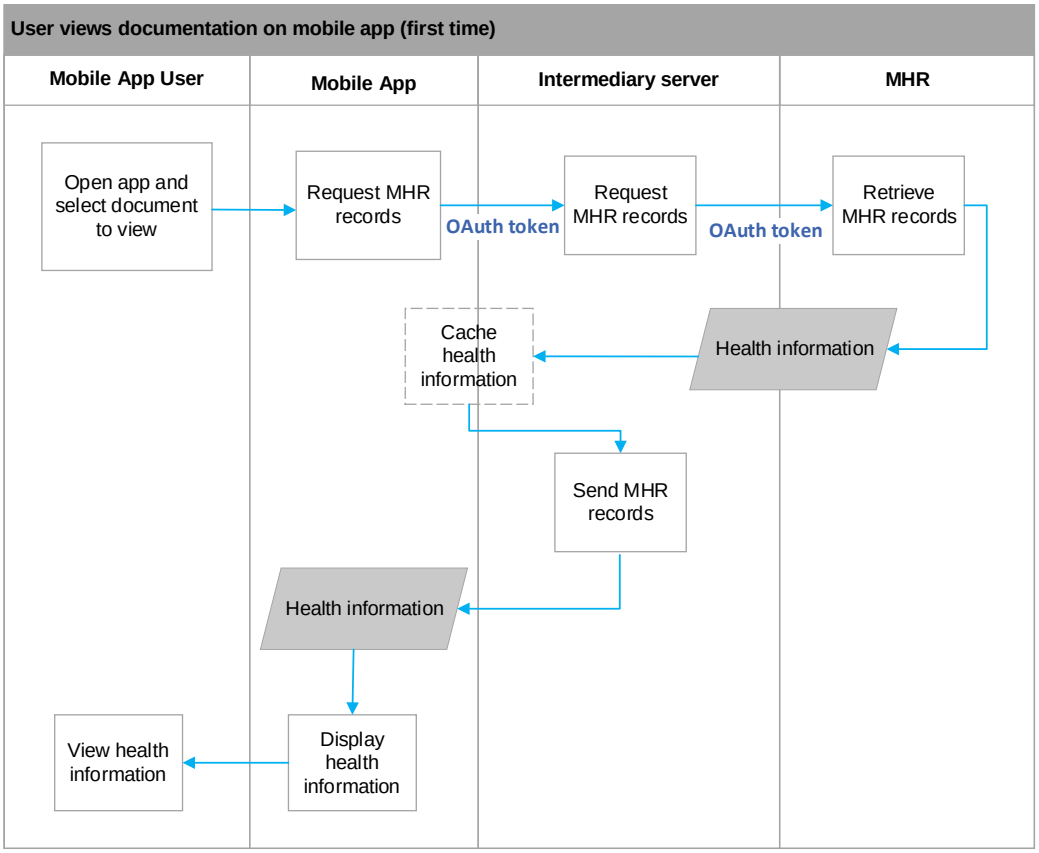
The PI below is both collected from individuals as part of the processes described and via automated processes such as the transfer of IHIs from MyGov into the MHR environment via the app as part of the OAuth token used to identify the correct records for display and download to the app.

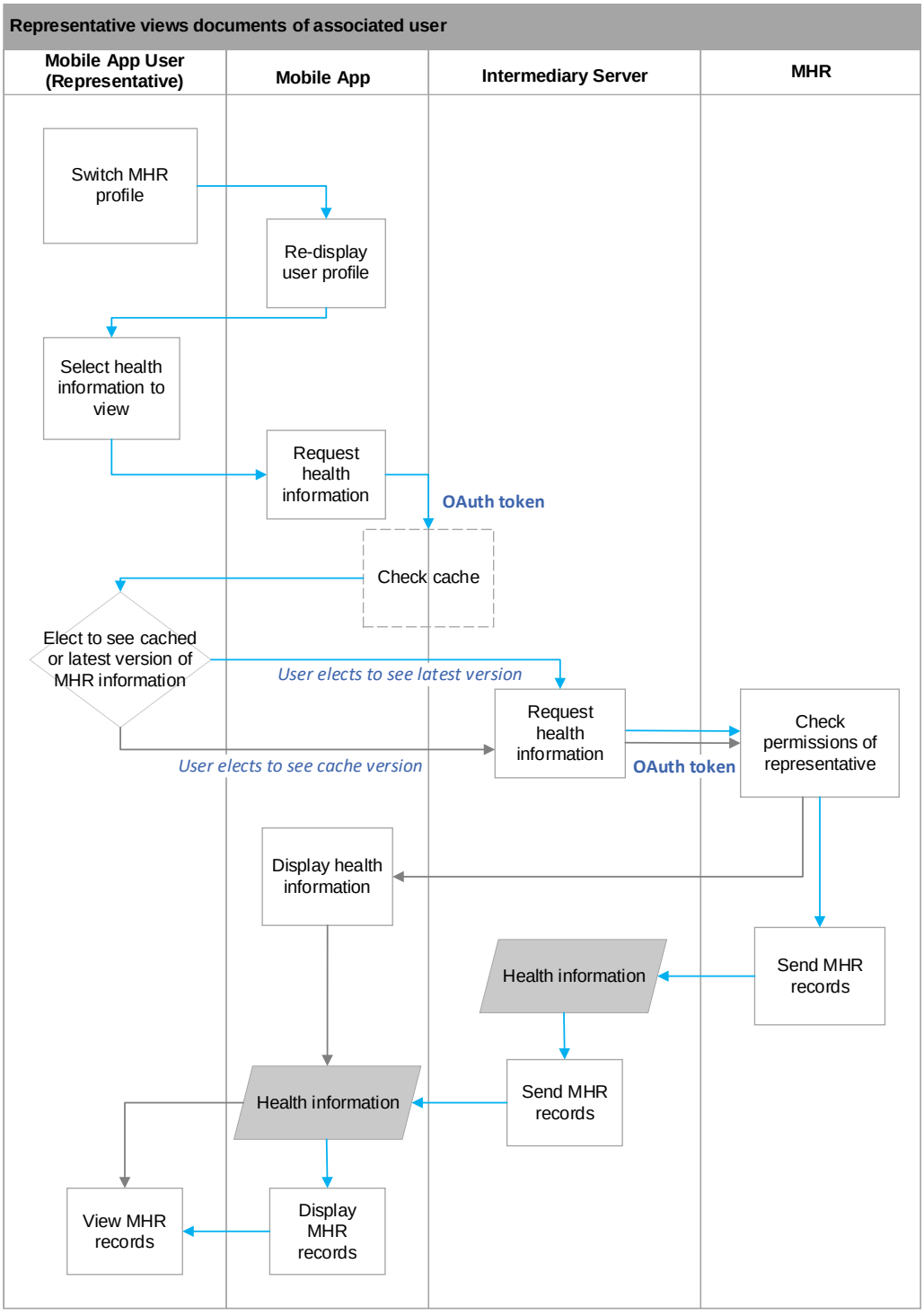
	Type of individual	Personal information handled
MyGov information	MHR user	• Username • Email • Individual Healthcare Identifier
Health information	Mobile app user	*Medical information including clinical documents, medicines, allergy and immunisation information, i.e.:* • Australian Immunisation Record • Covid-19 digital certificate • Diagnostic Imaging Reports • Pathology Reports • Specialist Letters • Discharge Summaries • Personal Health Summary • Shared Health Summary • Event Summaries • eHealth Prescription records • eHealth Dispense Records • Pharmaceutical Benefits Reports • Advance Care Plans • Australian Organ Donor Register status *The following are planned for phase 2 implementation of the mobile app, MyHealth:* • E-referrals • Personal Health Notes

Type of individual	Personal information handled
	• Childhood Development Information including Health Check Assessments • Medicare Services History

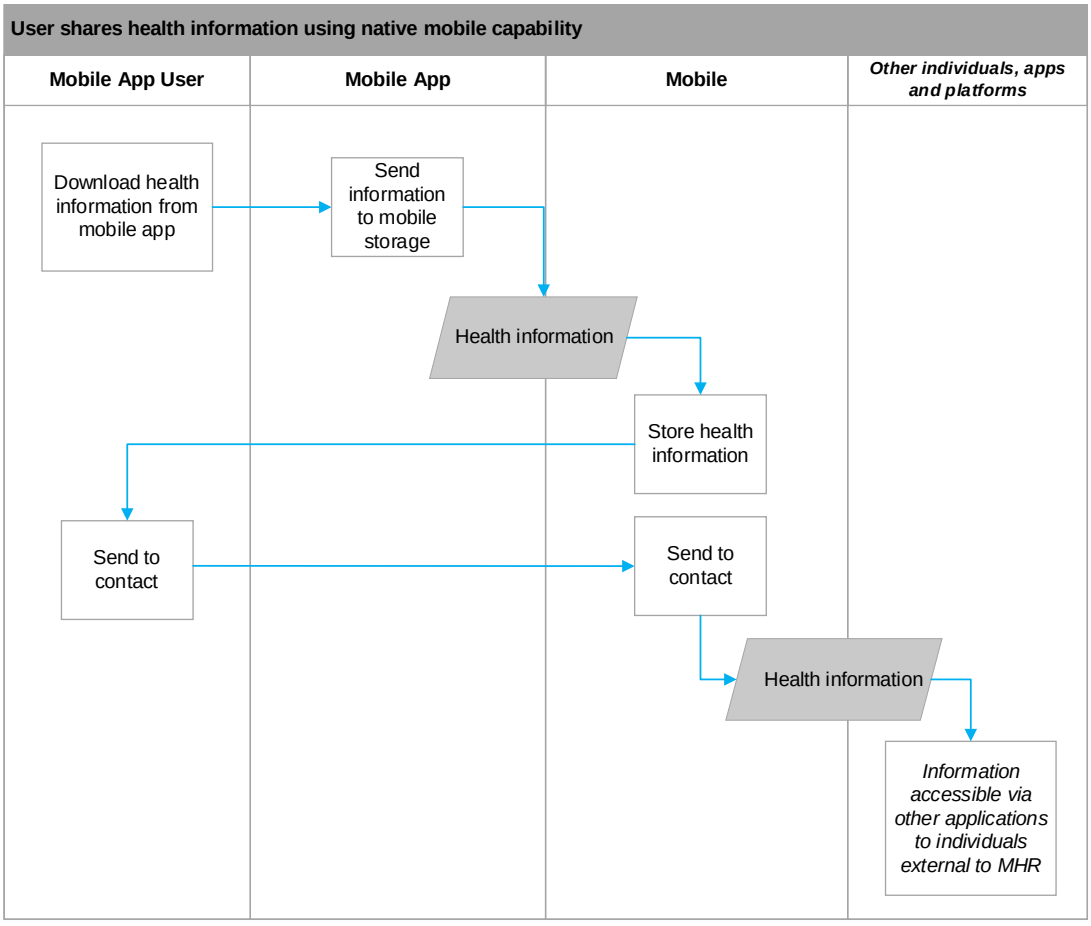
Information flow diagrams

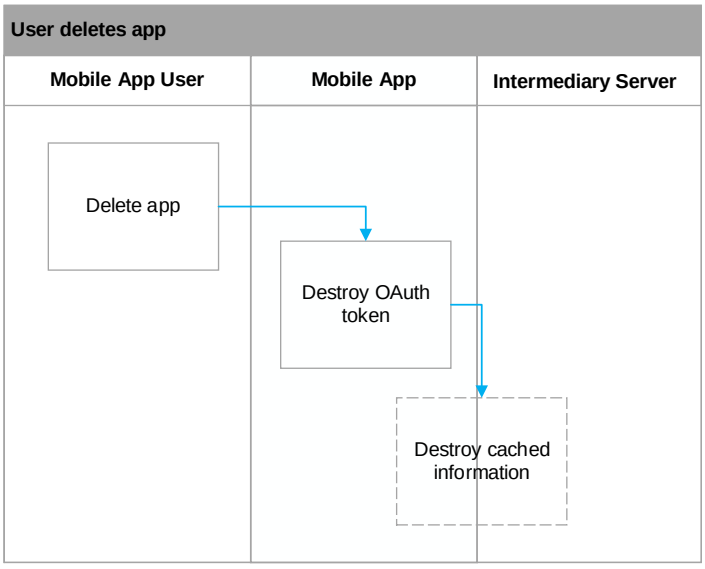


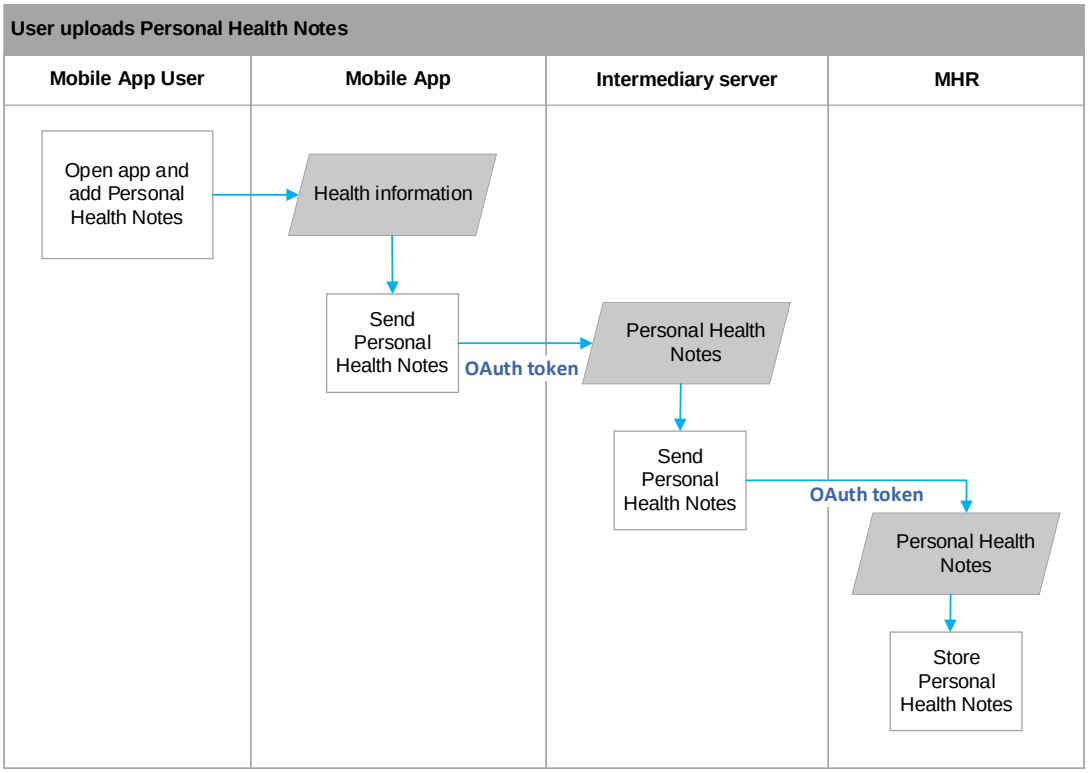

User views documentation on mobile app (first time)
Mobile App User
Mobile App
Intermediary server
MHR
Open app and select document to view
Request MHR records
OAuth token
Request MHR records
OAuth token
Retrieve MHR records
Cache health information
Health information
Send MHR records
Health information
View health information
Display health information



Note: This diagram assumes that the Nominated or Authorised Representative has their own myHealth app account and MHR. See our analysis regarding representatives who do not have an MHR in section 4.2, Security.


User shares health information using native mobile capability
Mobile App User
Mobile App
Mobile
Other individuals, apps and platforms
Download health information from mobile app
Send information to mobile storage
Health information
Store health information
Send to contact
Send to contact
Health information
Information accessible via other applications to individuals external to MHR

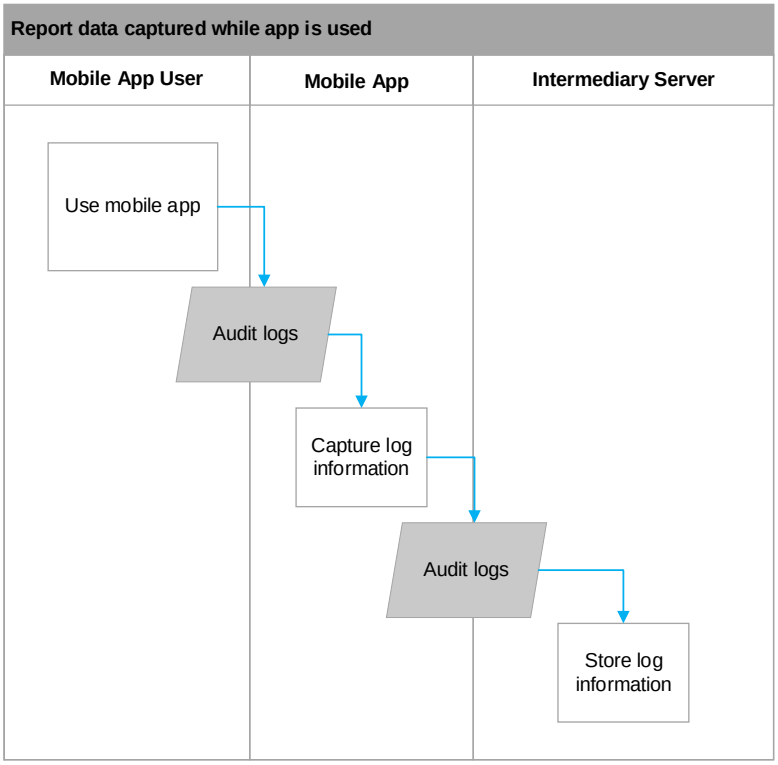

User deletes app
Mobile App User
Mobile App
Intermediary Server
Delete app
Destroy OAuth token
Destroy cached information



Use of aggregate data for reporting

	Type of individual	Personal information handled
Audit logs	Mobile app user	• User activity data • Performance data • Sentiment data

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 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

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**)[7] that sets out how it handles personal information. Ths policy explains how the Agency handles personal information. The separate My Health Record Privacy Policy (**MHR Privacy Policy**)[8] explains how the Agency, as System Operator under the *My Health Records Act*

[7] https://www.digitalhealth.gov.au/privacy
[8] https://www.myhealthrecord.gov.au/about/privacy-policy

2012 (Cth), collects, uses and discloses personal information to operate and manage the My Health Record system.

The MHR policy includes information on individuals and organisations that, as System Operator, the Agency may disclose personal information to. This includes disclosures that are required under the MHR Act and collections, uses and disclosures that are authorised under the Act.

The policy states that users of the MHR system's personal information is authorised to be disclosed when it is: "to you (including your authorised representatives and nominated representatives)" and also "with your consent", amongst a number of additional authorised types of disclosures.

The section in the MHR Privacy Policy on 'Mobile applications' describes what Registered Portal Operators are permitted to do when interacting with the My Health Record Mobile Gateway. This section requires updating to reflect the new features being made available to users, to download, store and (natively) share MHR information, in addition to viewing. We also suggest that these revisions provide additional information on how to remove third party app access, inclusive of the Agency's myhealth app.

This section in the MHR Privacy Policy does not make reference to the Agency's delivery and operation of the myhealth app. We anticipate that the myhealth app will generate media and public interests and that the Agency should prepare additional content explaining the app and the new functionality in more detail.

With regard to openness and transparency with regard to the management of personal information and taking reasonable steps to comply with the APPs in the Agency should commit to ensuring that the design, deployment and operation of the myhealth app conforms where applicable to the standards it has set for other app developers who have been authorised to interact with the My Health Record system.

With regard to APP1.2(b) we have assumed that assumed that the Agency, as the System Operator, has existing practices, procedures and systems in place to handle complaints and inquiries.

The MHR Privacy Policy has a Flesch Kincaid Reading Ease of 33.1 which means it should be easily understood by 20 to 21 year olds.[9] To an average reader the policy may appear overly complicated and is long to read. Some sections may also appear to be contradictory because an ordinary reader may not understand the technical differences between terms such as "access" and "view". We therefore recommend revising the policy to make its content more concise, and reformatting and 'layering'[10] to make the document easier to navigate.

[9] See https://www.webfx.com/tools/read-able/flesch-kincaid.html
[10] Layering is a method of breaking up privacy policy information into prioritized portions, with the key points presented in short and clear sentences, with the option to seek further information from additional 'layers' See: https://iapp.org/news/a/2012-09-13-best-practices-in-drafting-plain-language-and-layered-privacy/

Findings

We have identified five best practice recommendations in relation to open and transparent management of personal information.

Recommendations
BEST PRACTICE REC. 1 It is recommended that the Agency updates information published on the MHR website (such as the content set out at https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app) with more details on how the download, store and share functionality works, including details on security arrangements to ensure that third party apps don't view or use data contained in MHRs.
BEST PRACTICE REC. 2 It is recommended that the Agency considers ways to improve the readability score of the existing MHR **privacy** policy (in line with the OAIC's recommendations for privacy policies). This could include: • revising and rewriting content in order that it can be understood by people of all ages and education levels • adopting a layered approach (by creating a summary of the policy which links to detail within the policy) • reformatting the document to make it easier to navigate. *Note that this recommendation also appears in the comprehensive PIA for the SA DPC POC (see the* Context *section for more detail).*
BEST PRACTICE REC. 3 It is recommended that the Agency add additional content to the MHR privacy policy explaining both the Agency's operation of the myhealth app and the new download, store and share functionality available to all authorised third party apps in more detail.
BEST PRACTICE REC. 4 It is recommended that the Agency add additional detail to the MHR privacy policy or related materials on the MHR website describing how to remove third party app access.
BEST PRACTICE REC. 5 **[new]** It is recommended that, as a matter of Agency policy, the Agency documents and communicates internally the Agency's commitment to adhering to the same standards with regard to the handling of personal information that it has set for third party app developers that are authorised to interact with the MHR system.

1.2. Data breach response management

Relevant considerations

The My Health Records 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 My Health Record must be handled and notified in accordance with the My Health Record Act.

Impact analysis

We have reviewed the Portal Operator Registration Agreement (PORA) and note that portal operators' data breach obligations are addressed in section 5.10 – 5.15. We assume that these provisions were written with regard to the applicable requirements under the MHR Act.

We have assumed that the Agency has existing practices, procedures, and systems in place for responding to its own data breaches, including detection, containment, assessment, notification, and remediation.

The changed collection and handling of data by the Agency as a result of the myhealth app's operation may increase the likelihood and impact of the Agency's existing data breach risk. The Agency may wish to consider this changed risk profile in the implementation of mitigating strategies for cyber security risks.

Findings

We have made no findings relating 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

In line with rules issued under the MHR Act, it is possible for individuals to apply for a pseudonynm IHI, and with this, obtain a My Health Record user account.

Individuals can use a different name or pseudonym to register for an IHI[11]. An existing IHI is required before a request is made for an IHI in a pseudonym name. Once an individual has an IHI they can set up a user account with the MHR system.

We sought advice from the Agency on whether the MHR system treats pseudonym IHIs any differently from typical IHI records We were advised that the MHR system does not receive

[11] See: https://www.servicesaustralia.gov.au/individuals/services/medicare/individual-healthcare-identifiers/how-get-ihi

any details on whether an IHI is pseudonym nor does it have any specific rules for them, hence there is no impact on the Mobile Gateway or on the interactions with the Gateway by third party apps and the myhealth app.

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. Section 58A of the MHR Act permits the Agency to collect, use and disclose IHIs for the MHR system. 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.
MHR Act s 58A	The Agency may collect, use and disclose the healthcare identifiers of a healthcare receipient for the purposes of the My Health record system.
HI Act s 18B	The Agency may disclose the IHI of a healthcare recipient to the healthcare recipient.
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

We have observed that the proposed onboarding process for a new app user for the myhealth app involved the collection of the following personal information:

- username (user supplied)
- email (user supplied)
- Individual Healthcare Identifier (acquired via the MyGov interaction and collected for the purpose of identifying the user's MHR information).

We note that, as described in the My Health Record Privacy Policy "When you use mobile apps of registered portal operators to access your My Health Record, we will collect:

- data that you are using a mobile app to access your My Health Record, and
- information about the specific mobile app that you are using."

While the upload of information to the MHR system via an app is not yet implemented, we are advised that this feature is due for deployment in 2022, and is on the roadmap for the myhealth app to reach feature parity (**feature parity plan**) with the national portal. With this in mind we have made a Compliance recommendation (below) with regard to the inclusion of details of the types of personal information that will be collected by the app in the MHR Privacy Policy prior to the feature going live.

As described in the 'Background' section of this document, the project to develop the myhealth app for the Agency includes a set of requirements relating to Reporting. These indicate the data that is proposed for routine collection and analysis by the Agency for the purposes of reporting to stakeholders including the Government.

We have not seen any indication in the information provided that the data collected for reporting purposes contains identifiers for individuals. However in the interests of protecting against inadvertent collection and storage or personal information by personnel in the Agency tasked with compiling these reports, it is our recommendation that Agency procedures for the collection of mobile apps data for reporting explicitly prohibit the inclusion of identifiers, such as device identifiers or any other data types that could reasonably identify an individual.

Findings

Recommendations

COMPLIANCE REC. 1	With regard to the feature parity plan, prior to the introduction of the upload features proposed for the mobile apps, the Agency should revise the MHR Privacy Policy to reflect the new types of information that the Agency may collect from users via the app.
BEST PRACTICE REC. 6	It is recommended that Agency procedures for the collection of mobile apps data for reporting and analytics purposes explicitly prohibit the inclusion of identifiers, such as unique device identifiers or any other data types that could reasonably identify an individual.

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

We have reviewed mock ups for the myhealth app sign in experience for new users. As currently configured, we do not believe that the experience provides adequate notification of matters detailed in APP 5.2. Therefore it is recommended that additional information be inserted in these screens, inclusive of links to the MHR Privacy Policy.

We are advised that the upoload and 'write to' functionalities for the apps, for example to add allergies, notes or medication information is planned for 2022. With this mind we are recommending that the consent screen be revised prior to these functionalities being rolled out to include a separate dot point after '(app name) can access information..' to advise users that by consenting that '(app name) will be able to make changes to their My Health Record'.

Findings

We have identified one compliance recommendation in relation to notification of collection of personal information.

Recommendations
COMPLIANCE REC. 2 In order to be well positioned for the arrival of upload features under the feature parity plan, it is recommended that the Agency adds a privacy notice to the first use sign in experience for new users of the myhealth app (e.g. on the "Before you begin" screen), setting out the matters required under APP 5.2 including the types of personal information collected by the App, the purposes for which the information is collected, and providing a link to the MHR privacy policy.
COMPLIANCE REC. 3 In order to be well positioned for the arrival of upload features under the feature parity plan it is our recommendation that, prior to the roll out of the upload feature, the consent screen be revised to include a separate dot point after '(app name) can access information..' to advise users that by consenting that '(app name) will be able to make changes to their My Health Record'. *Note that this recommendation will be relevant to any third party apps authorised to incorporate this feature.*

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. The HI and MHR Act sets out the circumstances in which the Agency may use and disclose healthcare identifiers.

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).
MHR Act s 58A	The Agency may collect, use and disclose the healthcare identifiers of a healthcare recipient for the purpose of the MHR system.
HI Act s 18B	The Agency may disclose the IHI of a healthcare recipient to the healthcare recipient.
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.

Impact analysis

In relation to the use and dislosure of personal information, as a matter of best practice, opting out of the sharing of such information should be as simple as opting in. This is a view that has been expressed by the OAIC in guidelines they have issued on compliance with the Australian Privacy Principles[12].

[12] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines*, combined July 2019, B.40
https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf

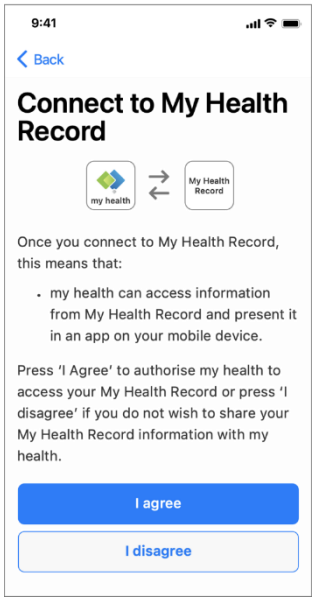
Office of the Australian Information Commissioner research[2] shows that almost half - 47% - of Australians have downloaded an app or signed up to a new digital service due to COVID-19. For young Australians, this figure is 68%[13]. More consumers today are likely to first engage with the MHR service via an app, and continue to interact with MHR primarily via the app.

To continue to build trust with the Australian community, it is important that they see how they can change permissions, such as revoking access for a nominated representative easily, and using the interface that they are most familiar with. Accordingly, we recommend implementing key functionality related to user consent and nominating representatives in the App as soon as reasonably possible. In the interim, we recommend adding a link to the portal for users to easily go to the page for opting out, in the app.

We have been provided with the following mock-up screen showing a proposed consent for users to link the my health app with their MHR:

ONB 9.2

Final screen before app opens up oAuth flow in mobile web browser



In our view, the bullet point text in the image above should be expanded to indicate that the App will be able to write to the user's MHR.

We also recommend applying the same standard imposed by the draft Consent Requirements and Guidelines[14] (**Consent Requirements**). For example, a link should be shown at the bottom of the consent screen which take the user to another screen which sets out more detail on how the app interacts with the MHR and links to applicable privacy policies.

[13] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2020* https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

[14] My Health Record FHIR GatewayConsent Requirements and Guidelines19 March 2020 v1.1, supplied by the Agency

Although the Consent Requirements are drafted with third party developers in mind, they serve as a consistent benchmark for how to inform users as to how an app will interact with their MHR, and they should be applied to Government-developed and operated apps to the extent that this is possible Adjustments should be made as needed, for example with an alteration to the wording of the required statement in Req. C004.

Findings

We have identified three compliance recommendations and one best practice recommendation in relation to use and disclosure of personal information.

Recommendations
COMPLIANCE REC. 4 It is recommended that the Agency apply the draft Consent Requirements and Guidelines (**Consent Requirements**)[15] to the myhealth app – presently, the "Connect to My Health Record" consent screen (ONB 9.2) does not include the additional detail described in the Consent Requirements, such as a link which shows the user more detail on how the app interacts with the MHR and links to applicable privacy policies. See in particular req. 007 in the Consent Requirements.
COMPLIANCE REC. 5 It is recommended that the Agency add words to the following effect to the bullet point description on the "Connect to My Health Record" consent screen (ONB 9.2): "you can use myhealth to share data from your My Health Record with others using your mobile device." *Note that this recommendation will be relevant to any third party apps authorised to incorporate this feature.*
BEST PRACTICE REC. 7 It is recommended that the Agency add a menu item to the "About the app" view (ACC1.0D and ACC1.1D) titled "App access" (or words to that effect) which contains information about the App's access to the user's MHR, as well as with instructions as to how users can revoke the App's access to the user's MHR. When reasonably possible, add functionality to allow users to revoke access from within the App.

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.

[15] DH_3088_2020_MyHealthRecordFHIRGateway_ConsentRequirementsandGuidelines_v1.1, supplied by the Agency

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 explicity 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.

Impact analysis

We note that the Agency is likely rejecting the usage of Microsoft App Centre in the myhealth architecture due to it being hosted overseas.

Findings

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

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 apps is accurate, up-to-date and complete and relevant and not misleading.

Impact analysis

The introduction of the download and store interactions brings with it an increased risk to users of viewing MHR information that is not current, for example, viewing a cached or downloaded document as opposed to the most recent version in the MHR system, when their device is offline. We note that the proposed design pattern to address this issue is, at present, to refresh by default and show the user a loading indicator (while still showing the cached/downloaded information). We recommend giving the users the ability to manually force a refresh in addition to this measure may also be desirable.

Findings

We have identified two best practice recommendations in relation to the quality of personal information.

Recommendations
BEST PRACTICE REC. 8 When the App is offline (i.e. unable to connect to a server), it is recommended that the app clearly indicates to users that the app is offline, and that any information they are viewing has not been refreshed and may not be up to date.
BEST PRACTICE REC. 9 If including functionality to allow users to manually refresh a view, it is recommended that the Agency includes text to show when the current view was last refreshed.

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 held in the apps 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

While we have not conducted a detailed security assessment of the Activities, we have reviewed the security guidelines applicable to Registered Portal Operators that are operating mobile apps, and we have reviewed the relevant portion of the MHR Privacy Policy with regard to security controls over the MHR system. We have also seen details of security arrangements for MHR records in transit and at rest at intermediary servers set up by the app developers, which include:

- no data caching in the intermediary servers;
- data in the intermediary servers encrypted at rest (likely using private key cryptography) with all staff who may access the content have the appropriate government clearance (NV1 or higher);
- data in the intermediary encrypted at rest (likely private key cryptography) with the cached data automatically cleared after a short period (likely 10 minutes or less); or
- data in the intermediary encrypted at rest (likely public key cryptography) and encrypted in a manner that can only be decrypted by the user's handset.

Once the MHR record has been downloaded we assume the users device's inbuilt security measure apply to any stored records. However we note that the ability for users to share information using the native sharing features of their device presents a potential risk and therefore we recommend that any mobile apps with the download and store functionalities include a warning to users before they use the share functionality.

The sharing of MHR information is permitted in certain circumstances, for example amongst family members or where an individual is a child under 14, or is incapable of managing their own affairs. See 'References and Key terms' in this document for an explanation of the roles of these 'nominated' or 'authorised' representatives.

In light of the potential harms that can arise from the accessing of personal information by estranged family or friends or in cases of domestic violence, we have examined carefully the ways in which users can manage access to MHR information using the apps.

The user experience when using the app should enable them to see quickly whether other parties have rights of access to their MHR information. Noting our observation about the uptake of mobile apps in favour of other channels in this PIA it is our view that it should be

as easy to change these arrangements as it is for those users who solely use the online portal. This means either making the changes directly in the case of nominated representatives or seeing clear information on how to go about making a request in the case of authorised representatives.

We note that in-app changing of such permissions for nominated representatives is planned for future development of the app. In the interim we recommend that certain information is displayed prominently to app users regarding the sharing of their MHR information and how to go about changing these arrangements.

Where an individual needs to make immediate changes to a nominated representative, such as an estranged partner, we note that these changes will flow through to the app users on the next request for information. That is, every time the user clicks on a link and downloads data relating to a nominated or authorised representative the app is in effect checking if they still have access and the request will be denied if that access has been revoked.

We have considered the scenario in which access for a nominated representative is revoked but that individual continues to be able to view cached MHR information while their device is in offline mode. A balance must be struck here:

- If the proposed time period after which the information is deleted is too short, there could be adverse impacts for proper and necessary uses of MHR. A likely use case for the apps could be, for example, a parent checking their child's medical history while offline owing to lack of coverage in a hospital or a remote location. Automatically preventing access to a cached MHR might also disproportionately disadvantage App users living in regional areas with poor mobile reception.
- On the other hand, if the proposed time period after which the cached information is deleted is too long, then the risk of harm to users from individuals that they have since removed as nominated representatives owing to threatening behaviours increases.

The arguments in favour of allowing a user to view a cached MHR are stronger in the case of authorised representatives, because the relationship is established through separate channels (e.g. family relationships or a legal order) and cannot be granted as easily as in the case of a nominated representative.

Accordingly, we have made some specific recommendations with regard to the lengths of time that cached MHRs should remain visible when a user's device is offline.

The Agency sought advice from us regarding the order in which the features to remove nominated representatives vs healthcare providers should be added to the myhealth app as part of the feature parity plan. Feature parity should be a priority in general, but to the extent that it is necessary to schedule one in front of the other our suggestion is that the ability to change access permissions for nominated representatives should be prioritised in that access by healthcare providers could reasonably be seen as a lower risk to the user.

With regard to the security of access to MHR information by nominated or authorised representatives, we have been advised by the Agency[16] that if you don't have an MHR, you can still create a MyHealth app account, and that if you have their MyGov authentication

[16] Email to elevenM from Murray Woodford, dated 21/01/2022.

details you can link the app account to the MHR records of anyone for whom you are a nominated or authorised representative. We note that under the standard Terms of use for MyGov that accessing another person's MyGov account is prohibited, and that as a general security principle individuals should not share credentials. Therefore we would advise that the proposed method for enabling a nominated or authorised representative to use the MyHealth app without having a MHR account is reviewed to avoid the sharing of MyGov user credentials.

Findings

We have identified two best practice recommendations and one compliance recommendation in relation to the security of personal information.

Recommendations

BEST PRACTICE REC. 10 Ensure that the App includes a warning to users before they use the share functionality that:

- there are security and privacy risks associated with sharing their MHR
- that by sharing, the data will leave the Agency's control and the user will not be able to control what the recipient does with the information that is being shared
- it is important to confirm the details of the receipient(s) before sharing.

BEST PRACTICE REC. 11 We recommend that functionality to allow users to change permissions for nominated representatives using the app rather than having to go to the website is prioritised in the feature parity plan. In the meantime we recommend:

- a prominent notice to users to indicate that their records are shared with nominated or authorised reps, where applicable
- for users with nominated representatives, clear instructions in the app on how to change permissions via the national portal.

BEST PRACTICE REC. 12 We recommend that the proposed method for enabling a nominated or authorised representative to use the MyHealth app without having a MHR account is reviewed to avoid reliance on the sharing of MyGov user authentication details.

COMPLIANCE REC. 6 We recommend that cached MHRs remain visible for the following lengths of time (after which access is prevented until the user's device is online and the user's access rights are confirmed):

- for nominated representatives – 24 hours
- for authorised representatives – 72 hours

We further recommend that this timeframe be communicated to users in the App and through separate materials on the MHR website.

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

With regard to healthcare recipients' records in the MHR system, retention is governed by the MHR Act, which applies retention periods of 30 years after the death if the healthcare recipient, or 130 years after the recipient's birth if date of death is not known.

With regard to other information created or received in the course of its business, we note that "almost all personal information, whether unsolicited or actively collected in the course of business, is considered a 'Commonwealth record'."[17] The APPs do not apply to the retention, destruction, and alteration of Commonwealth records because these actions are governed by the Archives Act 1983 (Cth) (**Archives Act**).

We note that the download and store model introduces a risk of over retention of personal information by app developers who are portal operators. In this regard our recommendation is for the revision of the Portal Operator Registration Agreement to include an explicit obligation on portal operators to delete all user data as soon as reasonably possible if the user revokes consent for the portal operator to access their MHR. In addition, a clause should be included in the PORA requiring the deletion or return of all MHR data to the Agency on conclusion of the contract with the provider.

We note that the 'Consequences of expiry or termination' section (s 11.4)[18] of the PORA requires the return or deletion of all copies of MHR information at the conclusion of the contract when the provider ceases to be a Registered Portal Operator.

Findings

We have identified one compliance recommendation in relation to the retention of personal information.

Recommendations

COMPLIANCE REC. 7 It is recommended that the Agency reviews the PORA to ensure that portal operators must purge data relating to a user's MHR as soon as reasonably possible if the user revokes consent for the portal operator to access their MHR.

[17] http://www.naa.gov.au/information-management/information-governance/legislation-standards/records-privacy/index.aspx
[18] Version we viewed: My Health Record_Portal Operator Registration Agreement Policy input 271021, supplied by the Agency

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

Access to MHR information is provided to healthcare recipients who sign up to use the system as a core functionality. We note that the Agency's website contains instructions for users of the MHR system on how to correct information uploaded to the MHR system[19].

It is worth noting here that the *Privacy Act 1988* is under review, with enhanced data subject rights under consideration. For this reason is would be prudent for the Agency to ensure it has awareness of possible future rights and ensure that planned system architecture, procedures and arrangements with portal operators are designed with enough flexibility to accommodate such anticipated changes.

Findings

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

[19] https://www.myhealthrecord.gov.au/for-you-your-family/howtos/incorrect-or-missing-information

References and key terms

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

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
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.
Privacy Code	means the *Privacy (Australian Government Agencies — Governance) APP Code* 2017 (Cth).
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.
IHI	means Individual Healthcare Identifier.
MHR System	means the My Health Record system operated 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.
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.
Privacy Act	means the *Privacy Act 1988* (Cth).

Annexure 1: Reporting requirements data collection

Appendix C - Reporting Requirements

Version 1.0

ID	Category	Report Name	Audience	Goal	Data Source	Frequency	Date	Measurements
1	Strategic	Organizational (ADHA) benefits (phase I)	• Research and Insights • Product	To track qualitative organisational benefits identified for Phase I	• Survey data • Mobile App	Monthly	First report due one month after go-live	• Minutes saved in consumer time • Pathology reports views • Pathology reports downloads
2	Strategic	Project benefits (phase I)	• Research and Insights • Product • Mobile App project • Communications	To track project benefits and the Mobile App uptake	• Mobile App • FHIR API • B2B API	Monthly	First report due one month after go-live	• % Consumers viewing clinical content on the app vs. other channels (e.g., NCP)/other apps such as Healthi or HealthNow • Net rate of uptake (installs and linked to MHR, less uninstalls) • Repeated / return use of the app and their delta over time (increase/decrease) • Source of invite to download the app • Type and frequency changes in support requests

ID	Category	Report Name	Audience	Goal	Data Source	Frequency	Date	Measurements
								• Viewed vs downloaded documents
3	Strategic	App Market Share	• Product • Communications • Experience Design	To track the importance of the app over time compared to other options	• Mobile App • FHIR API • B2B API	Quarterly	First report due one month after go-live (March 2021	• % App usage (no. of transactions*) compared to other apps available such as Healthi or HealthNow • Break down by demographic (IHI) * Adding information or sharing a document to outside the my health app is considered a transaction.

ID	Category	Report Name	Audience	Goal	Data Source	Frequency	Date	Measurements
4	Operational	Registration and Usage	• Product • Experience Design • Communications	To provide stats on the rate of adoption and volumes (who is doing what and how much of it)	• Mobile App • FHIR API • B2B API	Weekly	Promptly following the go-live or first report due one month after go-live (March 2021)	• Downloads • Installations* • Uninstalls • Screen views • Ratio app downloads vs. app installations • Active users • Session length • Session depth • Pages per visit • Session interval ** • Volume and proportion of new vs return users • Proportion of app usage to a) overall usage MHR, b) other mobile mobile app usage such as Healthi or HealthNow * User must have opened the my health mobile app. ** Time between 1st and 2nd session, and time between subsequent sessions.
5	Operational	Performance	• IT Operations • Incident Management		• Mobile App	Daily	Promptly following the go-live	• API latency • Time to load page • Resource usage (memory, CPU)

ID	Category	Report Name	Audience	Goal	Data Source	Frequency	Date	Measurements
			• Communications					• Type, Frequency, and volume of crashes
6	Operational	Feature Adoption	• Communications • Experience Design • Product	To track the use of app features that improve user experience (e.g., notifications) to track usage and prioritise changes/fixes	• Mobile App	Monthly	Promptly following the go-live or first report due one month after go-live (March 2021)	• Security/privacy settings enabled (future phases) • Permissions allowed (future phases) • Notifications enabled • Use of the document or credential vault
7	Operational	User Experience	• Experience Design • Product • Communications	To monitor the user behaviour and change in Mobile App, including comparison with NCP	• Mobile App	Quarterly	Promptly following the go-live or first report due one month after go-live (March 2021)	• OS types • Features like filtering options on the timeline • Device types • Screen resolution • User flow (Sankey diagram) • Time on Page • Event tracking (goals) • Page exits • Modals triggered (e.g.: details view of meds or docs) • User screengrabs • Share activity; Including document type, category, share channel, etc

ID	Category	Report Name	Audience	Goal	Data Source	Frequency	Date	Measurements
8	Operational	Contact Centre	• Contact Centre • Communications	To track the volume and types of support calls received for the app to identify trends and manage resources	• Datacom telephony solution • Vendor IT Support	Weekly	Promptly following the go-live or first report due one month after go-live (March 2021)	• Call volume • Call category • Call type • Call length • Call abandoned Rate • Time to resolve call • % Within SLA (time to answer, time to resolve) • % Escalations
9	Operational	Customer Satisfaction	Communications	To track user sentiment towards to app to tailor campaigns	• Survey Data • Mobile App store (Google/Apple)	Monthly	First report due one month after go-live (March 2021	• App rating • User feedback text (how often is X word used?) • User polling e.g., NPS (likelihood to recommend) • User sentiments e.g., 4 scale Likert • User surveys (positive and negative experiences – ratio) • Ability to break down by demographics