AUSTRALIAN DIGITAL HEALTH AGENCY

My Health Record System Mobile Applications Project

Privacy Impact Assessment

15 April 2020

CLAYTON UTZ

www.claytonutz.com

1. Contents

2. Executive Summary

This Privacy Impact Assessment (**PIA**) considers the effect on a person's privacy of a proposal to give people access to their My Health Record via their mobile devices.

My Health Record is the Australian Government's online summary of a Consumer's key health information. A Consumer's My Health Record is stored in the My Health Record system which is operated by the Australian Digital Health Agency (**Agency**) in its capacity as System Operator. Access to the My Health Record system is controlled by the Mobile Gateway and the Application Programming Interfaces (**APIs**).

Under a new Project, the Agency proposes to give access to the My Health Record system to more Mobile Application Developers who build Mobile Applications used by Consumers, and their Authorised Representatives and Nominated Representatives, to access their My Health Record from their mobile device. In order to do so, the Agency proposes to re-open and operate the Mobile Gateway with Mobile Application Developers who are Registered Portal Operators under the *My Health Records Act 2012* (**MHR Act**). Mobile Application Developers will be able to design their Mobile Applications in accordance with two models that offer different functions to Consumers, and their Authorised Representatives and Nominated Representatives, and affect the way in which their personal information is handled (**Interaction Models 1 and 4**).

2.1 Information flows

The way in which the Project operates is illustrated below for each of the two Interaction Models. The Project is described in more detail in paragraphs 5 and 8.

Figure 1: Interaction Model 1

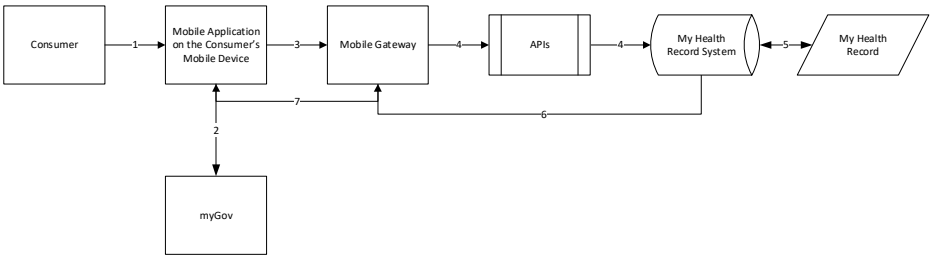
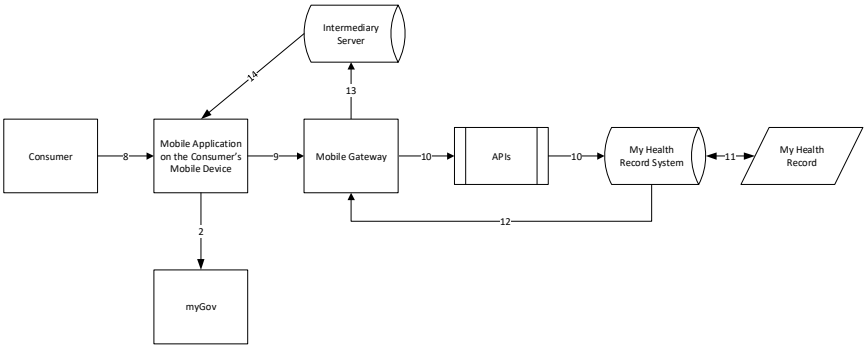


Figure 2: Interaction Model 4



The only relevant difference between the two Interaction Models is that Model 4 uses an Intermediary Server, whereas Model 1 does not.

2.2 Assumptions

This PIA makes the following assumptions as to the nature of the Mobile Applications.

- *First,* the Project contemplates the development of Mobile Applications that have been designed in accordance with Interaction Models 1 and 4.

- *Second*, Mobile Applications will acquire (but not record), a Consumer's My Health Record from the My Health Record system.
- *Third*, personal information will not be recorded on any electronic or other device, including mobile devices controlled by the Consumer (or their Authorised or Nominated Representative).
- *Fourth*, the Consumer (or their Authorised or Nominated Representative) will only be able to view personal information about the Consumer.
- *Fifth*, Mobile Applications designed in accordance with Interaction Models 1 and 4, will not disclose a Consumer's My Health Record to a third party.
- *Sixth*, not all Mobile Application Developers will provide Healthcare.
- *Seventh*, the infrastructure of Mobile Phone Applications will be based wholly within Australia.

These assumptions are described in more detail at paragraph 5.4.

2.3 Compliance with the APPs and risk

Overall, the PIA concludes that the Project is privacy positive and generally compliant with the Australian Privacy Principles (**APPs**). Nevertheless, there is a reasonable risk that the Agency will be held responsible, by the community, for the mishandling or inappropriate use of a Consumer's personal information by a Mobile Application Developer. The privacy risks that flow from this could manifest in the ways set out below.

First, it is technically possible that, rather than simply acquiring a Consumer's personal information, a Mobile Application Developer may also collect, whether deliberately or adventitiously, a Consumer's personal information.[1] **We do not consider that contractual measures to prevent a Registered Portal Operator from collecting personal information about Consumers are, on their own, a sufficient control for this risk.**

Second, in the event a Mobile Application Developer collects personal information of a Consumer, it is possible that a Mobile Application Developer's retention of a Consumer's personal information collected from the My Health Record system could be accessed by unauthorised users.

An unauthorised collection, use or disclosure by a Mobile Application Developer could expose the Agency to:

- criticism as to the perceived loss of control over a Consumer's personal information and a failure to protect personal information
- a loss of credibility as to its ability to manage the My Health Record
- criticism of the Project, and
- the necessity to redesign or retrofit the system, if the breach could not be resolved by simply cancelling or suspending the registration of the Registered Portal Operator.[2]

These risks are explained in more detail at part 9. Our recommendations, which are summarised in part 3, seek to mitigate these risks.

[1] For the purposes of APP 3, regarding the collection of personal information that is solicited, an APP entity collects personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication' (section 6(1)). This means, an APP entity does not collect personal information where that information is acquired but not included in a record or generally available publication.

[2] For example, under s 51(2)(c) of the MHR Act, a Registered Portal Operator's registration as a Registered Portal Operator may be cancelled or suspended if the security or integrity of the My Health Record system may be compromised.

3. Summary of Recommendations

Recommendation 1:

The Agency should put in place contractual arrangements with Mobile Application Developers that require:

- the Mobile Application Developer's compliance with the APPs
- the documentation of the Mobile Application Developers' security procedures for the handling of personal information, with special attention given to the way in which the Mobile Application Developer will use (and not record) a Consumer's personal information
- documents showing the technological tools and system design techniques that are being used by Mobile Application Developers to enhance privacy and security, for example encryption
- the production of documentation showing staff have been trained in the requirements for protecting personal information and are aware of policies regarding breaches of security or confidentiality, and
- evidence showing steps taken by the Mobile Application Developer to destroy any personal information that it may have recorded in the course of acquiring a Consumer's personal information (for example, meta data).

Recommendation 2:

The Agency should ensure that an independent audit[3] is conducted of all the security risks and the reasonableness of countermeasures to secure the Mobile Application Developer's system against unauthorised or improper collection, access, modification, use, disclosure and disposal of a Consumer's personal information.

Recommendation 3:

The Agency should put in place audit mechanisms to ensure a Mobile Application Developer handles a Consumer's personal information in accordance with the contractual arrangements. These audit mechanisms should be in place:

- when the Agency is considering a Mobile Application Developer's application to become a Registered Portal Operator
- during the operation of the Mobile Application Developer's Mobile Application, and
- in the course of responding to any unauthorised handling of personal information.

Recommendation 4:

The Agency should update its Privacy Policy to expressly state that the Agency may:

- collect personal information about a Consumer that is new to the Project, being:
    - that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access the Consumer's My Health Record, and
    - that the Consumer (or their Authorised or Nominated Representative) is using a particular type of Mobile Application to access their My Health Record, and

[3] Independent, in this context, means independent from the Mobile Application Developer.

We consider it would be reasonable for the Agency to notify the Consumer (or their Authorised or Nominated Representative) once, for example, when they first use a Mobile Application to access the Consumer's My Health Record.

Recommendation 5:

The Agency should revise its Privacy Policy to clarify the fact that:

- a Consumer's personal information is not being made accessible or visible to the Mobile Application Developer. Rather, it is being passed through (and not disclosed to) the Mobile Application Developer and its Intermediary Server (in relation to Interaction Model 4), and

- the Mobile Application Developer is not permitted to access or view the Consumer's personal information from its Intermediary Server.

Recommendation: 6

The Agency should ensure that all reasonable risk of unauthorised access is mitigated. The means by which this might be achieved are set out in the Office of the Australian Information Commissioner's (**OAIC**) *Guide to Securing Personal Information*.[4] This document provides guidance on the reasonable steps entities are required to take under the *Privacy Act 1988* (**Privacy Act**) to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. It also includes guidance on the reasonable steps entities are required to take to destroy or de-identify personal information that they hold once it is no longer needed (unless an exception applies). This guide is not legally binding. However, the OAIC will refer to this guide when investigating whether an entity has complied with its personal information security obligations (s 40 of the Privacy Act) or when undertaking an assessment (s 33C of the Privacy Act).

[4] OAIC *Guide to securing personal information* (5 June 2018) https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/

4. About this PIA

4.1 What is a privacy impact assessment?

A PIA is an examination of a project from a privacy perspective. The primary purposes of a PIA are to:

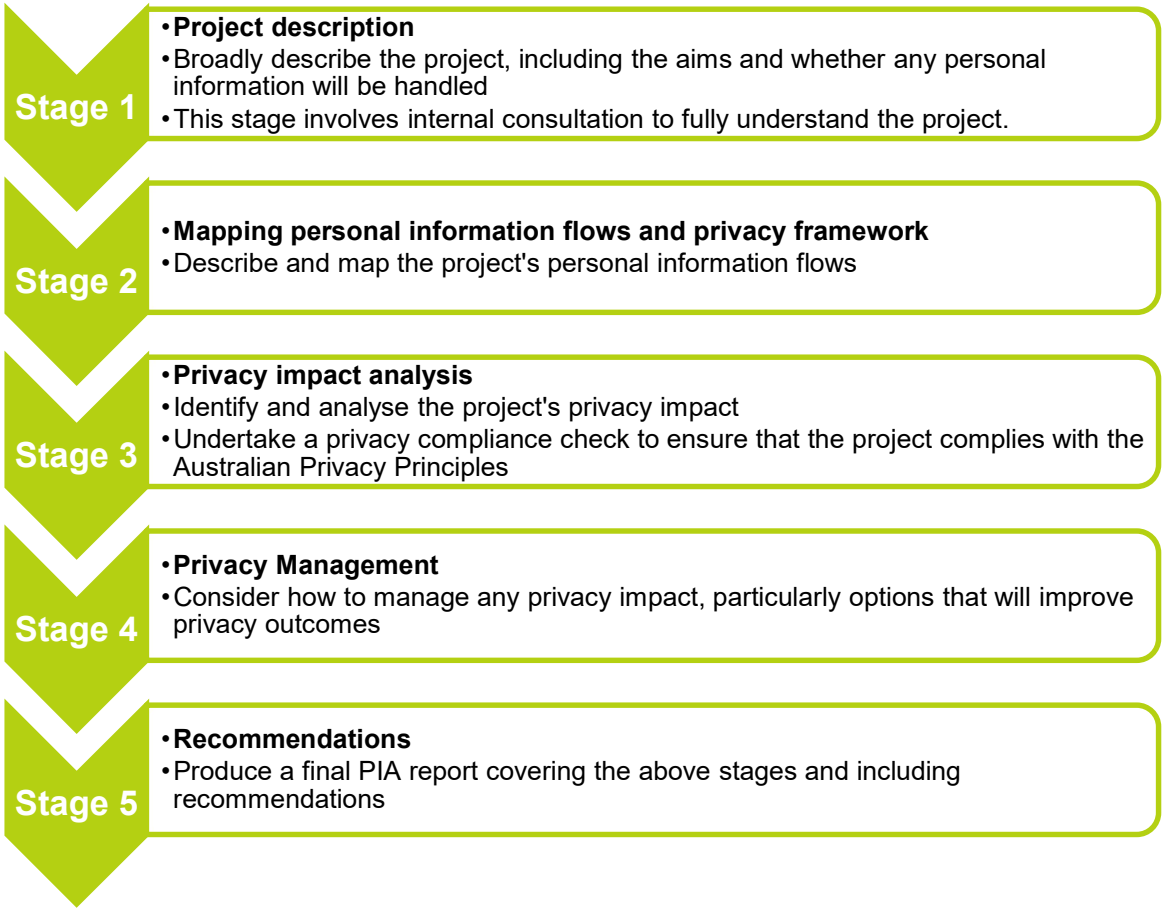
- examine how personal information is collected, used and disclosed by a project
- assess the compliance of a project with privacy laws and analyse its impacts on privacy, and
- identify and recommend options for managing, reducing or removing those impacts.

PIAs are conducted to ensure that privacy issues are fully considered in the design and implementation phase of a project. PIAs help ensure that projects meet privacy requirements in legislation and are also consistent with the expectations of the community.

4.2 The approach of this PIA

This PIA has been prepared broadly in accordance with the OAIC *Guide to undertaking privacy impact assessments*.[5] That guide recommends that PIAs be conducted in ten steps. Some of those steps involve deciding whether or not a PIA is necessary (a threshold assessment) and planning. This PIA was conducted in five key stages, as illustrated below.

Figure 3—PIA stages



[5] OAIC *Guide to undertaking privacy impact assessments* (5 May 2014).

This PIA identifies the effect the Project might have on the privacy of Consumers. The PIA is informed by a 2018 threat and risk assessment that considered the use of the Mobile Gateway by Mobile Applications.[6]

The PIA is set out in the following manner:

- Part 5 of the PIA describes the Project including its objectives as well as its links with the Agency's other programs, namely the National Digital Health Strategy
- Part 6 outlines the components of the My Health Record project and the context in which the Mobile Applications operate
- Part 7 identifies the stakeholders associated with the Project, namely Consumers, the Agency, Healthcare Providers (**HCP**), Mobile Application Developers and Registered Portal Operators
- Part 8 maps the flows of personal information associated with the Project
- Part 9 identifies and critically analyses how the Project impacts upon privacy
- Part 10 considers options for removing, minimising or mitigating any privacy risks identified through the privacy impact analysis. It makes a number of recommendations that identify avoidable impacts or risks and how they can be removed or reduced, and

Sources of information and a Glossary are at Schedule 1 and Schedule 2.

4.3 Applicable legislation

The handling of "personal information" (including "sensitive information") by Australian Commonwealth Government agencies is regulated by the Privacy Act.

The Privacy Act provides that an "APP entity" must not do an act, or engage in a practice, that breaches an APP.[7] As an "agency", the Agency is an APP entity and is therefore bound by the Privacy Act.[8]

The APPs are set out in Schedule 1 to the Privacy Act. The APPs regulate, among other things, the collection, use and disclosure of "personal information" and "sensitive information" by APP entities. This PIA has been prepared having regard to the APPs and other relevant parts of the Privacy Act.

This PIA has also been prepared having regard to the APP Guidelines.[9] The APP Guidelines outline the mandatory requirements of the APPs, how the OAIC interprets the APPs, matters the OAIC may take into account when exercising functions and powers under the Privacy Act, and good privacy practices to supplement minimum compliance with the mandatory requirements in the APPs.[10]

The PIA has also been prepared with regard to the MHR Act and the HI Act.

[6] Shearwater *Threat and Risk Assessment Mobility Gateway* (May 2018). In 2017, the Agency also commissioned a PIA that considered the privacy of Consumers and the development of mobile applications by industry to be used by the Consumers to access their My Health Record from the My Health Record system.

[7] See section 15 of the Privacy Act.

[8] See section 6 of the Privacy Act.

[9] OAIC *Australian Privacy Principles Guidelines* (31 March 2015).

[10] See the Preface to the APP Guidelines.

5. Project description

5.1 Background

My Health Record is the Australian Government's online summary of a Consumer's key health information. When a Consumer has a My Health Record, their health information can be viewed securely online, from anywhere, at any time, from any computer or device that's connected to the internet. HCPs who work with a Registered Healthcare Provider Organisation, registered as a participant in the My Health Record system can also access the Consumer's health information so that the Consumer can get the right treatment. A Consumer's My Health Record is stored in the My Health Record system, which is operated by the Agency.[11]

The Agency aims to increase the adoption of the My Health Record by Consumers (or their Authorised or Nominated Representatives). It is currently doing so by allowing them, to use their mobile devices to download Mobile Applications so that they can view (but not edit or download to their mobile device) the Consumer's My Health Record.

To this is end, the Agency has already:

- invited Mobile Application Developers to connect with the My Health Record system by first undergoing eligibility assessment, and registering with the Agency to become a Registered Portal Operator[12]
- provided technical information and resources to Mobile Application Developers to enable them to connect their Mobile Applications to the My Health Record system via the Mobile Gateway[13]
- connected the My Health Record system to Mobile Applications via the Mobile Gateway and APIs,[14] and
- invited Consumers (or their Authorised or Nominated Representatives) to view the Consumer's My Health Record using a Mobile Application.[15]

Currently, Consumers (or their Authorised or Nominated Representatives) who have a My Health Record and access to the internet can already use Mobile Applications that have been developed by Mobile Application Developers to communicate with the My Health Record system. These Mobile Applications give Consumers (or their Authorised or Nominated Representatives) the ability to view some of the content of the Consumer's My Health Record from their mobile devices. They do not permit any storage of information on their systems. And they are prohibited from using a Consumer's personal information for secondary purposes – such as passing information to a third party.[16]

[11] Australian Digital Health Agency *What is My Health Record?* https://www.myhealthrecord.gov.au/for-you-your-family/what-is-my-health-record (9 January 2020).

[12] Australian Digital Health Agency *FHIR Gateway (Mobile)* (7 January 2020) https://developer.digitalhealth.gov.au/products/fhirr-gateway

[13] Australian Digital Health Agency *FHIR Gateway (Mobile)* (7 January 2020) https://developer.digitalhealth.gov.au/products/fhirr-gateway

[14] Australian Digital Health Agency *FHIR Gateway (Mobile)* (7 January 2020) https://developer.digitalhealth.gov.au/products/fhirr-gateway

[15] Mobile Applications that are currently available to Consumers are HealthEngine by HealthEngine Pty Ltd, Healthi by Chamonix Health Solutions Pty Ltd, Health Now by Telstra Health and Tyde by Tyde Australia Pty Ltd. See https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app

[16] Australian Digital Health Agency *View your record using an app* (7 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app

5.2 Aims and objectives

Under this Project, the Agency now proposes to give access to the My Health Record system to more Mobile Application Developers. In order to do so, the Agency proposes to re-open the Mobile Gateway to Mobile Application Developers who have registered under the MHR Act as Registered Portal Operators.

The objective of the Project is to help improve a Consumer's health and wellbeing by building the Consumer's (or their Authorised or Nominated Representative's) engagement with the Consumer's My Health Record. To this end, Mobile Applications are being developed to give Consumers (or their Authorised or Nominated Representatives) the ability to manage the Consumer's health needs by allowing them to access the Consumer's My Health Record from their smartphones or tablets.

It is envisaged that Consumers (or their Authorised or Nominated Representatives) will be able to read (but not edit or download to their mobile device) the Consumer's My Health Record using their mobile device with a Mobile Application developed by a Registered Portal Operator.

In order to achieve these new objectives, the Project aims to:

- register Mobile Application Developers under the MHR Act to become Registered Portal Operators, and
- give Mobile Applications that have been developed Registered Portal Operators the ability to communicate with the My Health Record system via the Mobile Gateway[17] and the APIs[18].

5.3 Links with existing programs

The Project fits with the Agency's broader objectives to improve health outcomes for Australians through the delivery of digital healthcare systems.

It is linked to the Agency's National Digital Health Strategy which seeks to provide better health for all Australians enabled by digital health services and technologies that provide tools for Consumers (or their Authorised or Nominated Representatives) and HCPs.

The Project is also linked to the Agency's My Health Record system which seeks to deliver better health outcomes for Consumers and their HCPs by allowing Consumers (or their Authorised or Nominated Representatives) to control the Consumer's health information in one place and making it available when and where it's needed, including in an emergency.

5.4 Assumptions

This PIA makes the following assumptions as to the nature of the Mobile Applications.

- *First,* the Project contemplates the development of Mobile Applications that have been designed in accordance with Interaction Models 1 and 4. Interaction Model 1 allows Consumers (or their Authorised or Nominated Representatives) to use a Mobile Application downloaded to their mobile device to access their My Health Record from the My Health Record system via the Mobile Gateway. Interaction Model 4 operates in the same way, with the addition of an Intermediary Server that connects the Consumer's Mobile Application to the Mobile Gateway.
- *Second*, in order to display a Consumer's My Health Record to the Consumer (or their Authorised or Nominated Representative) on their mobile device, Mobile Applications will acquire (but not record), a Consumer's My Health Record from the My Health Record system.

[17] The Mobile Gateway is the software and hardware that allows a Mobile Application to communicate with the My Health Record system.

[18] The API is the set of instructions or commands given by a Consumer from their Mobile Application to the My Health Record system to access their My Health Record.

Personal information will not be saved to an electronic database or cache, including (in the case of Interaction Model 4) the Intermediary Server.

- *Third*, personal information will not be recorded on any electronic or other device, including mobile devices controlled by the Consumer (or their Authorised or Nominated Representative).

- *Fourth*, under this Project the Consumer (or their Authorised or Nominated Representative) will only be able to read personal information about the Consumer. They will not be able to consent to the disclosure of the Consumer's personal information, to a third party, via the Mobile Application.

- *Fifth*, Mobile Applications designed in accordance with Interaction Models 1 and 4, will not disclose a Consumer's My Health Record to a third party. Mobile Applications will make a Consumer's My Health Record visible to that Consumer (or their Authorised or Nominated Representative).

- *Sixth*, not all Mobile Application Developers will provide healthcare.

- *Seventh*, the infrastructure of Mobile Phone Applications will be based wholly within Australia. In this regard, we note that, under s 48(c) of the MHR Act, to be eligible for registration as a Registered Portal Operator, the central management and control of the Mobile Application Developer must be located in Australia at all times. In addition, s 77 of the MHR Act requires My Health Records not be held or taken outside Australia. These requirements are also set out in the Agency's Portal Operator Registration Agreement (My Health Record System View only access).

6. Components of the Project

Part 7 of the PIA outlines the components of the Project. It describes how a Consumer (or their Authorised or Nominated Representatives) uses myGov and a Mobile Application downloaded to their mobile device to verify their identity and access the Consumer's My Health Record. It shows how access to the My Health Record system is controlled via the Mobile Gateway and the API. It also shows how the design of the Mobile Application (being one of two Interaction Models) affects the way in which a Consumer's personal information may be collected, used and disclosed, including via an Intermediary Server.

The components of the Project are:

- myGov
- Mobile Applications
- Mobile Gateway
- API
- My Health Record system
- My Health Record
- Interaction Models 1 and 4, and
- Intermediary Server.

These components are explained in more detail below.

6.1 myGov

To access their My Health Record from the My Health Record system, Consumers (or their Authorised or Nominated Representatives) will first need to have a myGov account linked to the Consumer's My Health Record. The Agency will need to verify the Consumer's (or their Authorised or Nominated Representative's) identity before the Consumer's myGov account can be linked to the Consumer's My Health Record. MyGov is the Australian government's portal for online services, such as Medicare, Centrelink and My Health Record. It is run by Services Australia on behalf of the Australian Government and can be accessed at https://my.gov.au/. The information flows associated with myGov are not the subject of this PIA.

6.2 Mobile Applications

After verifying their identity with myGov, Consumers (or their Authorised or Nominated Representatives) use a Mobile Application to view the Consumer's My Health Record from the My Health Record system. Currently, Consumers (or their Authorised or Nominated Representatives) can use a limited number of commercially available Mobile Applications to view the Consumer's My Health Record.[19]

It is envisaged that, under this Project, Consumers (or their Authorised or Nominated Representatives) would be able to use more Mobile Applications on their mobile devices to view the Consumer's My Health Record. These Mobile Applications would be developed by Mobile Application Providers who have registered with the Agency to become a Registered Portal Operator under the MHR Act.

[19] Australian Digital Health Agency *View your record using an app* (7 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app

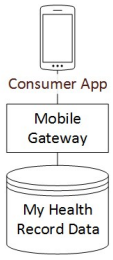
The development of Mobile Applications by Mobile Application Providers was the subject of a draft PIA by Ashurst in March 2017.[20]

Under the Project, Mobile Applications will be designed in accordance with two Interaction Models: 1 and 4.

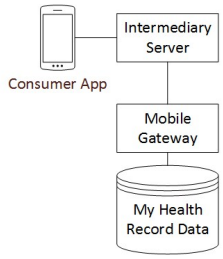
6.3 Interaction Models

Mobile Application Developers will develop Mobile Application based on one of two Interaction Models, each of which offer different functions and affect the way in which a Consumer's personal information will be acquired (but not collected).

Interaction Model 1 allows Consumers (or their Authorised or Nominated Representatives) to use a Mobile Application to access the Consumer's My Health Record via the Mobile Gateway and without intermediate infrastructure (such as an Intermediary Server) handling their personal information. Interaction Model 1 is illustrated below: [21]



Interaction Model 4 allows Consumers (or their Authorised or Nominated Representatives) to access the Consumer's My Health Record via an Intermediary Server. The Intermediary Server may be managed by the Mobile Application Developer to improve the functionality of the Mobile Application without the Consumer having to download updates to the Mobile Application. Interaction Model 4 is illustrated below: [22]



6.4 Intermediary Server

Under Interaction Model 4, a Mobile Application uses an Intermediary Server to connect with the Mobile Gateway and, thus, the My Health Record system. The Intermediary Server is managed by a Mobile Application Developer who is a Registered Portal Operator.

Intermediary Servers also collect an access token from the Agency which may be used to verify a Consumer's authority (or the authority of their Authorised or Nominated Representatives) to access their My Health Record in order to access a Consumer's My Health Record from the My Health Record system

[20] Ashurst *My Health Record – Mobile Apps: Models 1, 2 and 4 (Healthcare Recipient Apps) Privacy Impact Assessment* (24 March 2017).

[21] Shearwater *Threat and Risk Assessment Mobility Gateway* (May 2018) 4.

[22] Shearwater *Threat and Risk Assessment Mobility Gateway* (May 2018) 4.

via the Mobile Gateway. This means a Consumer does not need to verify their authority to access their My Health Record with myGov each time they wish to view their record.[23]

Under Interaction Model 1, the Mobile Application will connect with the My Health Record system via the Mobile Gateway. Conversely, under Interaction Model 4, the Mobile Application will connect with the My Health Record system via communications between the Mobile Gateway and the Intermediary Server.

6.5 Mobile Gateway

The Mobile Gateway is a mechanism by which Mobile Applications can securely integrate and interact with the My Health Record system and give Consumers, and their Authorised Representatives and Nominated Representatives, access to their My Health Record. It separates the My Health Record system from the Internet by allowing only Mobile Applications that have the consent of Consumers (or their Authorised or Nominated Representatives) who have verified their identity via myGov, to communicate with the My Health Record system.

The Mobile Gateway was the subject of a threat and risk assessment which was completed by Shearwater in May 2018.[24] This assessment considered the risks associated with the use of the Mobile Gateway by Mobile Applications. The information flows associated with the operation of the Mobile Gateway are the subject of this PIA. The Mobile Gateway allows Mobile Applications to communicate with the My Health Record system using the API.

6.6 Application Programming Interface (API)

The API is a set of instructions or commands, for example "GET" (to read or search, for example) "DELETE" (to delete) and "POST" (to update or transact). In order to access a Consumer's My Health Record, a Mobile Application uses the API to communicate with My Health Record system.

6.7 My Health Record system

The My Health Record system is the Australian Government's digital health record system that holds a Consumer's My Health Records.[25] It comprises the infrastructure, standards and specifications necessary to enable secure access to a Consumer's health information. It draws this personal information from multiple sources, such as general practices, specialists, hospitals, pharmacies, and pathology and imagery laboratories. The My Health Record system is managed and operated by the Agency. Once a Consumer is able to communicate with the My Health Record system via a Mobile Application that has been developed by a Registered Portal Operator, they are able to access their My Health Record. The My Health Record system was the subject of two PIAs completed in 2011[26] and 2015.[27]

6.8 My Health Record

My Health Record is the Australian Government's online summary of a Consumer's key health information. It is defined in the MHR Act to be the record of information that is created and maintained by the System Operator (being the Agency) in relation to the healthcare recipient (being the Consumer), and information that can be obtained by means of that record, including the following:

- information included in the entry in the Register that relates to the healthcare recipient

[23] Shearwater *Threat and Risk Assessment Mobility Gateway* (May 2018) 9.

[24] Shearwater *Threat and Risk Assessment Mobility Gateway* (May 2018).

[25] The My Health Record system is defined in s 5 of the MHR Act. See also Schedule 2.

[26] Minter Ellison *Privacy Impact Assessment Report Personally Controlled Electronic Health Record (PCEHR) Prepared for the Commonwealth Department of Health and Ageing* (15 November 2011) https://www.myhealthrecord.gov.au/about/privacy-policy/privacy-impact-assessments.

[27] Minter Ellison *Privacy Impact Assessment Report Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model Prepared for the Department of Health* (20 May 2015) https://www.myhealthrecord.gov.au/about/privacy-policy/privacy-impact-assessments.

- health information connected in the My Health Record system to the healthcare recipient (including information included in a record accessible through the index service)
- other information connected in the My Health Record system to the healthcare recipient, such as information relating to auditing access to the record, and
- back-up records of such information.[28]

It can include details of a person's medical conditions and treatments, medicine details, allergies, and test or scan results.[29] HCPs like doctors, specialists and hospital staff may be able to see a person's My Health Record when they need to, including in an accident or emergency, if they work for a Healthcare Provider Organisation who is registered by the System Operator as a participant in the My Health Record system. A Consumer and their Authorised Representatives and Nominated Representatives can also access the Consumer's My Health Record online. To access their My Health Record online, Consumers need to have a myGov account and to link it to their My Health Record.[30] Authorised and Nominated Representatives will need to link the Consumer's My Health Record to their own myGov account.

[28] MHR Act, s 5.

[29] Australian Digital Health Agency *What is My Health Record?* (9 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/what-is-my-health-record

[30] Australian Digital Health Agency *What is My Health Record?* (9 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/what-is-my-health-record

7. Stakeholders

Part 7 of the PIA identifies and describes the stakeholders involved in this Project.

The stakeholders are:

- Consumers
- the Agency, and
- Mobile Application Developers (who must become Registered Portal Operators).

7.1 Consumers

Consumers are people who have a My Health Record and use a Mobile Application to view their My Health Record. All Australians now have a My Health Record, unless they have chosen to opt out.

Consumers access the My Health Record online by:

- creating a myGov account
- downloading a Mobile Application to their smartphone or tablet
- logging in to their myGov account
- verifying their identity with myGov, and
- giving their consent to Mobile Application Developers to access the My Health Record via the Mobile Application.

At this stage, Consumers are able to view (but not edit or download to their mobile device) their My Health Record.

7.2 Australian Digital Health Agency

The Agency is responsible for operating and managing the My Health Record system. The Agency has been prescribed as the System Operator by regulation 2.1.1 of the *My Health Records Regulation 2012*, pursuant to section 14(1)(b) of the MHR Act.

The Agency aims to increase the adoption and use of the My Health Record by Consumers (or their Authorised or Nominated Representatives). It is currently doing so by allowing them to use their mobile devices to download Mobile Applications so that they can view (but not edit or download to their mobile device) the Consumer's My Health Record. To this end, it is supporting more Mobile Application Developers to register as Registered Portal Operators and develop Mobile Applications.

7.3 Mobile Application Developers and Registered Portal Operators

Mobile Application Developers are third parties that develop software for mobile devices that may be used by Consumers (or their Authorised or Nominated Representatives) to access the Consumer's My Health Record.

There are currently four Mobile Application Developers who are Registered Portal Operators:

- HealthEngine Pty Ltd
- Chamonix Health Solutions Pty Ltd
- Telstra Health, and

- Tyde Australia Pty Ltd.[31]

In order to participate in the Project and access the My Health Record system, Mobile Application Developers must first register with the Agency to become a Registered Portal Operator under the MHR Act.

Only Mobile Applications that have been developed by Registered Portal Operators can be used by Consumers, and their Authorised Representatives and Nominated Representatives, to communicate with the My Health Record system and access the Consumer's My Health Record, via the Mobile Gateway.

Registration is granted on the basis that, as Registered Portal Operators, Mobile Application Developers:

- satisfy of all the requirements of the MHR Act for registration as a Registered Portal Operator;[32] and
- meet the eligibility requirements as set out in the Agency's Portal Operator Registration Agreement (My Health Record System View only access), including:[33]
    - provide an electronic interface that facilitates access to the My Health Record system by Consumers, and their Authorised Representatives and Nominated Representatives, and does not copy, record or store that data[34]
    - agree to be bound by the Privacy Act[35] and to comply with the APPs,[36] and
    - ensure their central management, control and portal are located in Australia; and My Health Record System information is not handled outside Australia.[37]

[31] Australian Digital Health Agency *View your record using an app* (7 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app

[32] Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View only access* (22 November 2018) [3.1(a)] and s 47, 48, and 49 of the MHR Act.

[33] Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View only access* (22 November 2018) [3.1(a)].

[34] Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View only access* (22 November 2018) [3.4].

[35] Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View only access* (22 November 2018) [5.1].

[36] Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View only access* (22 November 2018) [5.4].

[37] Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View only access* (22 November 2018) [5.9].

8. Map of information flows

Part 8 of the PIA describes and maps the personal information flows in the Project. It details what information will be used by the Agency (but not collected) and disclosed by the Agency to Mobile Applications via the Mobile Gateway.

Under the Project, personal information will be collected, used and disclosed when Consumers (or their Authorised or Nominated Representative) use a Mobile Application developed by a Mobile Application Developer who is a Registered Portal Operator to view (but not edit or download to their mobile device) the Consumer's My Health Record

This map of information flows assumes the Consumer (or their Authorised or Nominated Representative) has already:

- created a myGov account, online[38]
- registered for (or not opted out of) a My Health Record[39]
- linked the Consumer's My Health Record to their myGov account, and
- downloaded a Mobile Application to their mobile device (from the Apple iTunes Store or Google Play, for example).[40]

8.1 Identity verification

Under the Project, it will first be necessary for the Consumer (or their Authorised or Nominated Representative) to verify their identity in order to access the Consumer's personal information.

In order to do so, the Consumer (or their Authorised or Nominated Representative) will first attempt to log into the My Health Record system. To verify their identity, the My Health Record system uses MyGov to authenticate the Consumer's (or their Authorised or Nominated Representative's) credentials and secret information. Once this information has been validated, they are authenticated to interact with the My Health Record system. During this process, a Consumer's (or their Authorised or Nominated Representative's) myGov credentials and answer to a secret question will be used by the Agency, but otherwise their personal information will not be collected, used or disclosed by the Agency. Nor will it be collected, used or disclosed by the Mobile Application.

8.2 What personal information will be collected, used and disclosed

Having verified their identity, it is envisaged that the Agency will then collect, use and disclose personal information about a Consumer that it already holds in its My Health Record system, in order to give the Consumer (or their Authorised or Nominated Representative) access to the personal information contained in the Consumer's My Health Record.

Under the Project, the Agency will collect one new piece of personal information about a Consumer (or their Authorised or Nominated Representative) who uses a Mobile Application. That information is that the Consumer (or their Authorised or Nominated Representative) is using a particular Mobile Application. This information is needed to provide access to the Consumer (or their Authorised or Nominated Representatives), via the Mobile Gateway, to the Consumer's My Health Record.

Under the Project, the Agency will use and disclose personal information that is sensitive information, being the Consumer's health information. These terms are discussed in detail below.

---

[38] myGov *Welcome, please sign in* (8 January 2020) https://my.gov.au/LoginServices/main/login?execution=e3s1

[39] Australian Digital Health Agency *Register for a My Health Record* (8 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/howtos/register-for-my-health-record

[40] Australian Digital Health Agency *View your record using an app* (8 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app

Personal information

'Personal information' is defined in the Privacy Act as any 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not' (s 6(1)).

It is envisaged that the Project will handle the following personal information about a Consumer:

- first name
- last name
- date of birth
- address, and
- phone number.

The Agency already has this personal information, which will be exchanged between the Agency and the Mobile Application Developer in order to verify a Consumer's (or their Authorised or Nominated Representative's) identity.

Sensitive information

The Project will also use and disclose sensitive health information about a Consumer. 'Sensitive information' is a subset of personal information and is defined in section 6 of the Privacy Act to mean:

- information or an opinion about an individual's:
    - racial or ethnic origin
    - political opinions
    - membership of a political association
    - religious beliefs or affiliations
    - philosophical beliefs
    - membership of a professional or trade association
    - membership of a trade union
    - sexual orientation or practices, or
    - criminal record
- health information about an individual, or
- genetic information about an individual that is not otherwise health information
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or

- biometric templates.[41]

Health information

The definition of 'sensitive information' includes health information of an individual. 'Health information' is defined in section 6FA of the Privacy Act to mean:

- information or an opinion, that is also personal information, about:
    - the health or a disability (at any time) of an individual, or
    - an individual's expressed wishes about the future provision of Health Services to him or her, or
    - a health service provided, or to be provided, to an individual, or
- other personal information collected to provide, or in providing, a Health Service, or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

It is proposed that the following health information about a Consumer may be handled by the Project:

- medical conditions and treatments
- allergies
- test or scan results
- an overview of a person's health uploaded by their doctor (called a shared health summary)
- hospital discharge summaries
- medications prescribed
- referral letters from doctors
- Medicare and Pharmaceutical Benefits Scheme information held by Services Australia
- Medicare and Repatriation Schedule of Pharmaceutical Benefits information stored by the Department of Veterans' Affairs
- organ donation decisions
- immunisations that are included in the Australian Immunisation Register, including childhood immunisations and other immunisations received
- contact numbers and emergency contact details
- allergy information and any previous allergic reactions
- Indigenous status

[41] Privacy Act, s 6(1).

- Veterans' or Australian Defence Force status, and
- advance care plan or contact details of the Consumer's custodian.[42]

The personal information listed above is collected separately by the Agency as System Operator in order to make the My Health Record. It is then disclosed to the Consumer (or their Authorised or Nominated Representative) via the Mobile Application.

In addition, the Agency will handle personal information about a Consumer (or their Authorised or Nominated Representatives) that is new to the Project, being:

- that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access their My Health Record, and
- that the Consumer (or their Authorised or Nominated Representative) is using a particular type of Mobile Application to access their My Health Record.

We consider this to be personal information about a Consumer (or their Authorised or Nominated Representative) because:

- it is information about the Consumer's (or their Authorised or Nominated Representative's) tastes, preferences and practices,
- it is technically possible to identify a Consumer (or their Authorised or Nominated Representative) from the personal information because the Mobile Application is linked to their mobile device (which may itself be linked to their email address and phone number) when it is first downloaded and subsequently used.

8.3 Collection, use and disclosure of personal information

The table below sets out how a Consumer's (or their Authorised or Nominated Representative's) personal information will be collected, used and disclosed by the Agency during the Project.

Table 1: Collection, use and disclosure of personal information

Collection	Under the Project, the Agency will collect personal information about the Consumer that: • the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access their My Health Record, and • the Consumer (or their Authorised or Nominated Representative) is using a particular type of Mobile Application to access their My Health Record. This information is necessary to provide access to the Consumer (or their Authorised or Nominated Representatives), via the Mobile Gateway, to the Consumer's My Health Record.
Use	The ways in which a Consumer's personal information may be used by the Agency are described below: • the Agency searching the My Health Record system for the Consumer's My Health Record, and • the Agency passing that personal information from the My Health Record system to the Mobile Gateway.
Disclosure	The only relevant disclosure of personal information is:

[42] Australian Digital Health Agency *What's in a My Health Record?* https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record

	• a Consumer's own information from their My Health Record to themselves (or their Authorised or Nominated Representative), and • if applicable, information that a Consumer does not have a My Health Record, or has a My Health Record that has been suspended, to the Registered Portal Operator via an error message that reads, for example "404 Not Found".[43] Although, in the case of Interaction Model 4, the Consumer's personal information is passed through the Mobile Application Developer's Intermediary Server, the information is not disclosed to the Mobile Application Developer. This is discussed in more detail in paragraph 9.7.

8.4 Information flows for Interaction Model 1

The figure and table below illustrate and describe the way in which a Consumer's (or their Authorised or Nominated Representative's) Mobile Application first verifies their identity, then connects with the Mobile Gateway and then, via the APIs, communicates with the My Health Record System to obtain the Consumer's personal information. It shows how the Consumer's personal information flows from the My Health Record system to the Consumer (or their Authorised or Nominated Representative), via the Mobile Gateway and a Mobile Application on their Mobile Device.

Figure 4: Information Flows

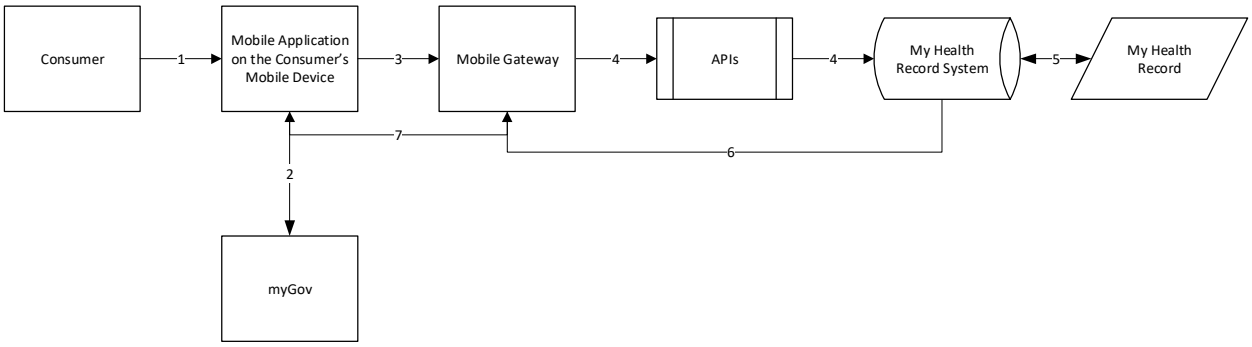


Table 2: Information Flows - Interaction Model 1

Flow	Description
1.	To establish a Consumer's (or their Authorised or Nominated Representative's) authority to access the Consumer's My Health Record: • the Consumer, or their Authorised Representatives and Nominated Representatives, opens the Mobile Application, and • requests access to the Consumer's My Health Record. In doing so, the Agency will handle personal information about a Consumer that it already possesses as well as collect new personal information, namely: • that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access the Consumer's My Health Record, and • that the Consumer (or their Authorised or Nominated Representative) is using a particular type of Mobile Application to access the Consumer's My Health Record.
2.	To establish a Consumer's (or their Authorised or Nominated Representative's) authority to access their My Health Record:

[43] Instructions received on 12 February 2020.

	• the Mobile Application directs the Consumer (or their Authorised or Nominated Representative) to myGov • they verify their identity by signing into myGov using their username (or email address) and password (**myGov Credentials**)[44] • myGov notifies the Mobile Application that their identity has been verified • the Mobile Application collects an access token from myGov which may be used to verify the Customer's (or their Authorised or Nominated Representative's) authority to access their My Health Record. This means they do not need to verify their authority to access their My Health Record with myGov each time they wish to view their record, • the Agency collects information that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access their My Health Record.
3.	For the Mobile Application to obtain access to the My Health Record System, the Mobile Application contacts the Mobile Gateway and notifies it that: • a Consumer (or their Authorised or Nominated Representative) wants to use their mobile device to access the Consumer's My Health Record • their identity has been verified by myGov or with an access token, and • the Mobile Application needs to communicate with the My Health Record system via the Mobile Gateway. The Mobile Gateway does not collect any personal information about the Consumer from the Mobile Application for this purpose.
4.	The Mobile Application then uses the APIs to communicate with the My Health Record system, and requests the My Health Record system give it access to the Consumer's My Health Record. The Mobile Health Record system does not collect any personal information about the Consumer from the Mobile Application for this purpose.
5.	The My Health Record system then searches its records for the Consumer's My Health Record.
6.	The My Health Record system then passes the Consumer's personal information to the Mobile Gateway. If applicable, information that a Consumer does not have a My Health Record, or has a My Health Record that has been suspended, is disclosed by the API to the Registered Portal Operator via an error message that reads, for example "404 Not Found".[45]
7.	The Mobile Gateway then discloses the Consumer's personal information to the Consumer (or their Authorised or Nominated Representative) via their Mobile Application.

[44] myGov *Welcome, please sign in* (9 January 2020) https://my.gov.au/LoginServices/main/login?execution=e2s1

[45] Instructions received on 12 February 2020.

8.5 Information flows for Interaction Model 4

The figure and table below illustrate and describe the way in which a Mobile Application first verifies the identity of the Consumer (or their Authorised or Nominated Representative) via myGov, then connects with the Mobile Gateway and then, via the APIs, communicates with the My Health Record System to obtain the Consumer's personal information from their My Health Record. It then shows how the Consumer's personal information flows from the My Health Record system to the Consumer (or their Authorised or Nominated Representative), via the Mobile Gateway, an Intermediary Server, and a Mobile Application on their Mobile Device.

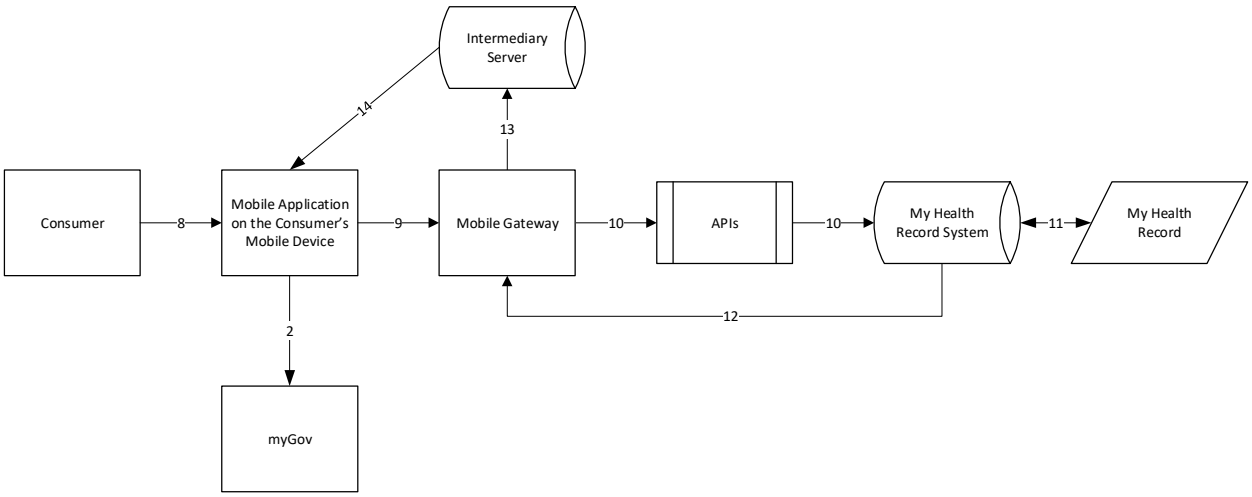


Table 3: Information Flows - Interaction Model 4

Flow	Description
8.	To establish a Consumer's (or their Authorised or Nominated Representative's) authority to access the Consumer's My Health Record: • the Consumer (or their Authorised or Nominated Representative) opens the Mobile Application, and • requests access to their My Health Record. In doing so, the Agency will handle personal information about a Consumer that it already possesses as well as collect new personal information about the Consumer, namely: • that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access the Consumer's My Health Record, and • that the Consumer (or their Authorised or Nominated Representative) is using a particular type of Mobile Application to access the Consumer's My Health Record.
9.	To establish a Consumer's (or their Authorised or Nominated Representative's) authority to access the Consumer's My Health Record: • the Mobile Application directs the Consumer (or their Authorised or Nominated Representative) to myGov • the Consumer (or their Authorised or Nominated Representative) verifies their identity by signing into myGov using their myGov Credentials[46] • myGov notifies the Mobile Application that their identity has been verified

[46] myGov *Welcome, please sign in* (9 January 2020) https://my.gov.au/LoginServices/main/login?execution=e2s1

	• the Mobile Application collects an access token from myGov which may be used to verify the Customer's (or their Authorised or Nominated Representative's) authority to access their My Health Record. This means they do not need to verify their authority to access their My Health Record with myGov each time they wish to view their record, and • the Agency collects information that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access their My Health Record.
10.	For the Mobile Application to obtain access to the My Health Record System, the Mobile Application contacts the Mobile Gateway and notifies it that: • a Consumer (or their Authorised or Nominated Representative) wants to use their mobile device to access the Consumer's My Health Record • their identity has been verified by myGov or with an access token, and • the Mobile Application needs to communicate with the My Health Record system via the Mobile Gateway. The Mobile Gateway does not collect any personal information about the Consumer from the Mobile Application for this purpose.
11.	The Mobile Application then uses the APIs to communicate with the My Health Record system, and requests the My Health Record system give it access to the Consumer's My Health Record. The Mobile Health Record system does not collect any personal information about the Consumer from the Mobile Application for this purpose.
12.	The My Health Record system then searches its records for the Consumer's My Health Record. If applicable, information that a Consumer does not have a My Health Record, or has a My Health Record that has been suspended, is disclosed by the API to the Registered Portal Operator via an error message that reads, for example "404 Not Found".[47]
13.	The My Health Record system then passes the Consumer's personal information to the Mobile Gateway.
14.	The Mobile Gateway discloses the Consumer's personal information to the Consumer (or their Authorised or Nominated Representative) by passing it through an Intermediary Server associated with the Consumer's (or their Authorised or Nominated Representative's) Mobile Application.

[47] Instructions received on 12 February 2020.

9. Privacy impact analysis and compliance check

Part 9 of the PIA identifies and critically analyses how the Project impacts upon privacy, both positively and negatively.

Overall, and for the reasons set out below, the Project is privacy positive.

- *First*, the Project will change the way Consumers (or their Authorised or Nominated Representatives) access the Consumer's personal information in a positive way by making it more readily available to them, via their mobile device.

- *Second*, the Project does not necessitate the Agency collecting any personal information about the Consumer, apart from information that the Consumer (or their Authorised or Nominated Representative) is using a type of Mobile Application to access the Consumer's My Health Record. Rather, it simply uses the personal information already held by the Agency about a Consumer for the purposes of giving the Consumer (or their Authorised or Nominated Representative) access to that personal information.

- *Third*, the Consumer has control over the circumstances in which their personal information is disclosed. In this regard, a Consumer's personal information is only disclosed to them (or their Authorised or Nominated Representative) after they have actively chosen to access the Consumer's personal information on their mobile device, actively downloaded a Mobile Application to their mobile device and actively instructed the Mobile Device to use (but not collect) the Consumer's personal information from the Consumer's My Health Record. To this end, Agency's *My Health Record FHIR Gateway Consent Requirements and Guidelines* informs Mobile Application Developers (who are, or seek to become, Registered Portal Operators) how to obtain a Consumer's (or their Authorised or Nominated Representative's) consent to handle (but not collect) the Consumer's personal information so that it can be viewed by the Consumer (or their Authorised or Nominated Representative) on their mobile device.[48]

  Where an Authorised Representative or Nominated Representative has access to a Consumer's My Health Record, they are required to make reasonable efforts to ascertain the recipient's will and preferences (or likely will and preferences) in relation to the recipient's My Health Record, including by referring to the agreement appointing the Nominated Representative or from people who may be aware of the Consumer's will and preferences (see s 7A of the MHR Act).

- *Fourth*, the implementation of the Project does not require the Agency to make any significant decisions that affect the types of government services and benefits available to Consumers (such as their eligibility to receive Medicare benefits and the amount payable). The Project simply makes decisions about what Mobile Applications (each with their various features and design elements) may be available to Consumers (or their Authorised or Nominated Representatives) to view their My Health Record.

- *Fifth*, the Project is broadly compliant with the APPs. This is discussed in detail from paragraph 10.2.

In our view, the main risk to the privacy of a Consumer through implementation of the Project emerges in the case of Intermediary Model 4, following the flow of a Consumer's My Health Record information through an Intermediary Server, operated by a Mobile Application Developer that is a Registered Portal Operator. This is considered below.

[48] Australian Digital Health Agency *My Health Record FHIR Gateway Consent Requirements and Guidelines (v 2.0)*. See especially the example consent flow at Appendix B which requires Consumers to actively choose to move through about five screens in the course of giving their consent to the Mobile Application taking personal information from the Consumer's My Health Record so that the Consumer may view it.

9.1 Alignment with community expectations

Under the Privacy Act and the APPs, the Agency is not responsible for the handling of a Consumer's personal information after it leaves the Agency's effective control. In addition, the Agency assesses the connection of the API to the My Health Record to ensure the Mobile Application is not configured to capture personal information.[49]

Nevertheless, there is a reasonable risk that the Agency will be held responsible, by the community, for the mishandling or inappropriate use of a Consumer's personal information by a Mobile Application Developer. It may be that Consumers (or their Authorised or Nominated Representatives) do not distinguish between the Agency and a Mobile Application Developer and will consider the Agency to be ultimately responsible for the handling of their information. The privacy risks that flow from this could manifest in the ways set out below.

First, it is technically possible that, rather than simply acquiring personal information, a Mobile Application Developer may also collect, whether deliberately or adventitiously, personal information.[50] **We do not consider that contractual measures to prevent a Registered Portal Operator from collecting personal information about Consumers are, on their own, a sufficient control for this risk.**

Second, it is possible that a Mobile Application Developer's retention of personal information collected from the My Health Record system could be accessed by unauthorised users.

In these circumstances, it is likely that Consumers (or their Authorised or Nominated Representatives) would expect the Agency to have in place audit and oversight mechanisms in case a Mobile Application Developer mishandles personal information. Consumers (or their Authorised or Nominated Representatives) will likely direct any complaints they have about the handling of their personal information by Mobile Application Developers to the Agency.

An unauthorised collection, use or disclosure by a Mobile Application Developer could expose the Agency to:

- criticism as to the perceived loss of control over personal information and a failure to protect personal information
- a loss of credibility as to its ability to manage the My Health Record
- criticism of the Project, and
- the necessity to redesign or retrofit the system, if the breach could not be resolved by simply cancelling or suspending the registration of the Registered Portal Operator.[51]

9.2 Ensuring compliance with the APPs

The following paragraphs consider whether the Project complies with each of the APPs and identifies any risks to compliance.

First, we consider that, for the reasons set out below, APPs 2 and 9 do not apply to this Project.

- **APP 2**, regarding anonymity and pseudonymity, does not apply to the Project. We consider it to be impracticable for the Agency to give Consumers (or their Authorised or Nominated

[49] Instructions received on 6 February 2020.

[50] For the purposes of APP 3, regarding the collection of personal information that is solicited, an APP entity collects personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication' (section 6(1)). This means, an APP entity does not collect personal information where that information is acquired but not included in a record or generally available publication.

[51] For example, under s 51(2)(c) of the MHR Act, a Registered Portal Operator's registration as a Registered Portal Operator maybe cancelled or suspended if the security or integrity of the My Health Record system may be compromised.

Representatives) the option of not identifying themselves, or of using a pseudonym. It is necessary for Consumers (or their Authorised or Nominated Representatives) to verify their identity before they can be given access to the Consumer's personal information.

- **APP 9**, regarding the adoption use or disclosure of government related identifiers by an organisation because the Agency is an 'agency' and not an 'organisation' for the purposes of the Privacy Act (see section 6(1)).

Second, we consider the Project to be compliant with APPs 7 and 12, for the reasons set out below.

- **APP 7**, regarding direct marketing, is satisfied because the Project will not disclose a Consumer's personal information for the purpose of direct marketing.

- **APP 12**, regarding access to personal information, is satisfied because the Project's objective is to give Consumer's (or their Authorised or Nominated Representatives) easy access to the Consumer's My Health Record via their mobile devices.

Third, and for the reasons set out in the paragraphs below, we consider the Project to be broadly compliant with APPs 1, 3, 5, 6, 8, 9, 11 and 13.

9.3 APP 1 — Open and transparent management of personal information

APP 1 provides that the APP entity must have ongoing practices and policies in place to ensure that it manages personal information in an open and transparent way.

Subject to the implementation of our recommendations at paragraph 10.2, and for the reasons set out below, we consider the Project to be generally compliant with APP 1.

- First, the Agency has an APP Privacy Policy about how it manages a Consumer's personal information. This may be accessed, free of charge online at https://www.myhealthrecord.gov.au/about/privacy-policy.

  The Privacy Policy describes the personal information that may be collected for the purposes of creating a Consumer's My Health Record. It also notifies Consumers (or their Authorised or Nominated Representatives) of the potential for the disclosure of personal information to a Registered Portal Operator via a Mobile Application:

  > "*We may also disclose your personal information contained in a clinical document that has been uploaded to a My Health Record to a registered portal operator through the registered portal operator's interface with the My Health Record System, where a healthcare recipient, or their representative, consents to the disclosure of their My Health Record information to that portal operator's app or portal operator.*"

- Second, steps have been taken to ensure the Project complies with the APPs and any binding registered APP code. This includes the Agency's commissioning of this PIA, as well as an earlier PIA into the My Health Record system in 2011[52] and the Department of Health's commissioning of a PIA of the opt-out model in 2015.[53]

[52] Minter Ellison Lawyers and Salinger *Privacy Impact Assessment Report Personally Controlled Electronic Health Record (PCEHR)* (15 November 2011) https://www.myhealthrecord.gov.au/about/privacy-policy/privacy-impact-assessments and

[53] Minter Ellison Lawyers *Privacy Impact Assessment Report Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model* (20 May 2015) https://www.myhealthrecord.gov.au/about/privacy-policy/privacy-impact-assessments

9.4 APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect solicited personal information. Higher standards apply to the collection of sensitive information.

We consider the Project to be generally compliant with APP 3 because it is necessary to collect personal information that the Consumer (or their Authorised or Nominated Representative):

- is using a Mobile Application to access their My Health Record, and
- is using a particular type of Mobile Application to access their My Health Record.

In this way, the collection of personal information is for the purpose of making health information about the Consumer available to them.

9.5 APP 5 — Notification of the collection of personal information

APP 5 provides that an APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.

We consider APP 5 will be satisfied, subject to the Agency notifying Consumers that it will:

- collect information that the Consumer (or their Authorised or Nominated Representative) is using a particular Mobile Application, and
- if applicable, disclose information that a Consumer does not have a My Health Record, or has a My Health Record that has been suspended, to the Registered Portal Operator via an error message that reads, for example "404 Not Found".[54]

9.6 APP 6 — Use of personal information

APP 6 provides that an APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. Use and disclosure are dealt with separately, below.

For the reasons set out below, we consider the Project to be generally compliant with APP 6 for the use of personal information.

APP 6

APP 6 outlines the circumstances in which an APP entity may use personal information that it holds. An APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information. Generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control.

Use

The term 'use' is not defined in the Privacy Act. Under the APP Guidelines, an APP entity 'uses' information where it handles or undertakes an activity with the information, within the entity's effective control.[55] Under the Project, the Agency proposes to use a Consumer's personal information when it searches the My Health Record system for the Consumer's My Health Record and then passes the records in that My Health Record to the Mobile Gateway so that they can then be made visible to a Consumer via a Mobile Application.

[54] Instructions received on 12 February 2020.

[55] OAIC *APP Guidelines* (22 July 2019).

Primary Purpose

An APP entity can only use personal information for the particular purpose for which it was collected (known as the 'primary purpose'). This is the specific function or activity for which the entity collects the personal information.

In this case, the Consumer's personal information, was collected for the primary purpose of making up a Consumer's My Health Record under the MHR Act.[56]

The Agency collected a Consumer's personal information when:

- it automatically created a My Health Record for the Consumer (unless the Consumer opted out) under the MHR Act
- when the Consumer asked to register for a My Health Record.[57]

My Health Record of a healthcare recipient means the record of information that is created and maintained by the System Operator in relation to the healthcare recipient, and information that can be obtained by means of that record, including the following:

- information included in the entry in the Register that relates to the healthcare recipient
- health information connected in the My Health Record system to the healthcare recipient (including information included in a record accessible through the index service)
- other information connected in the My Health Record system to the healthcare recipient, such as information relating to auditing access to the record, and
- back-up records of such information.[58]

The Agency collected this personal information in its capacity as System Operator of the My Health Record system under the MHR Act.[59] As System Operator, it is a function of the Agency to facilitate the retrieval of information from the My Health Record system when required, and to ensure that Consumers and their Authorised Representatives and Nominated Representatives are able to do so readily.[60] The ways in which the Agency handles a Consumer's personal information to operate and manage the My Health Record system is set out in the Agency's My Health Record Privacy Policy.[61]

For these reasons, we consider the Project to be compliant with APP 6 for the use of this personal information. The Agency is using the Consumer's personal information for the purpose for which it was collected. By undertaking activities to first search for and then pass a Consumer's personal information from the My Health Record system to the Mobile Gateway [which in turn allows a Consumer (or their Authorised or Nominated Representative) to access their personal information], the Agency is using the personal information for the primary purpose of making a person's My Health Record readily available to the Consumer.

---

[56] MHR Act, s 4.

[57] Australian Digital Health Agency *My Health Record Privacy Policy* (17 January 2020) https://www.myhealthrecord.gov.au/about/privacy-policy

[58] MHR Act, s 5.

[59] The Agency has been prescribed as the System Operator by regulation 2.1.1 of the My Health Records Regulation 2012, pursuant to section 14(1)(b) of the MHR Act.

[60] MHR Act, s 15(a)(ii).

[61] Australian Digital Health Agency *My Health Record Privacy Policy* (17 January 2020) https://www.myhealthrecord.gov.au/about/privacy-policy

9.7 APP 6 — Disclosure of personal information

For the reasons set out below, we consider the Project to be generally compliant with APP 6, for the disclosure of personal information.

APP 6

APP 6 also outlines the circumstances in which an APP entity may disclose personal information that it holds. An APP entity can only disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information.

Disclosure

Disclosure is not defined in the Privacy Act. Under the APP Guidelines, an APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.[62]

In this case, a Consumer's personal information is not being made accessible or visible to the Mobile Application Developer. Rather, it is being passed through (and not disclosed to) the Mobile Application Developer's Intermediary Server. Furthermore, the Mobile Application Developer is not permitted to access and view the Consumer's personal information from its Intermediary Server.

Thus, the only relevant disclosure of personal information is a Consumer's own information from their My Health Record to themselves (or their Authorised or Nominated Representative). Although, in the case of Interaction Model 4, the Consumer's information is passed through the Mobile Application Developer's Intermediary Server, the information is not disclosed to the Mobile Application Developer.

It is also possible that the Agency may accidentally disclose personal information if it provides personal information to an unintended recipient, for example, another Mobile Application and another Consumer. However, we understand that the architecture would not support the provision of user personal information to an unintended recipient.[63]

Primary Purpose

An APP entity can only disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'). As discussed above, the Consumer's personal information, was collected for the primary purpose of making up a Consumer's My Health Record under the MHR Act.[64]

Accordingly, we consider the Project to be compliant with APP 6 for the disclosure of personal information. The Agency is disclosing the Consumer's personal information to the Consumer (or their Authorised or Nominated Representative) for the purpose of for which it was collected

By undertaking activities to give a Consumer (or their Authorised or Nominated Representative) the ability to view their My Health Record, the Agency is using the personal information for the primary purpose of making a person's My Health Record readily available to the Consumer (or their Authorised or Nominated Representative).

9.8 APP 8 — Cross-border disclosure of personal information

APP 8 provides for the cross-border disclosure of personal information. It generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.

---

[62] OAIC *APP Guidelines* (22 July 2019) B.63-B.64.

[63] Instructions received on 6 February 2020.

[64] MHR Act, s 4.

In this case, APP 8, is satisfied because the cross-border disclosure of personal information is not intended. To this end, we note the following arrangements that are in place to ensure personal information is not disclosed outside Australia.

First, it is not proposed that the Agency will engage Mobile Application Developers located overseas to provide Mobile Applications to Consumers (or their Authorised or Nominated Representative). Rather, there is a legal prohibition imposed on the Agency and Mobile Application Developers that prevents Registered Portal Operators from holding or taking My Health Records outside Australia (see 77(1) of the MHR Act). A person commits an offence if this prohibition is contravened. The penalty is 5 years or 300 penalty units or both (s 77(2)(a)).

Second, there is a contractual obligation imposed on Registered Portal Operators that requires they ensure that:

- their central management and control, and the portal they operate, will be located in Australia
- they will not hold, take, process or handle My Health Records, or related information, outside Australia, and
- they will not cause or permit another person to hold, take, process or handle My Health Records, or related information, outside Australia.[65]

Third, the Agency can cancel or suspend a Mobile Application Developer's registration as a Registered Portal Operator if the Mobile Application Developer discloses personal information outside Australia, which would constitute a contravention of the MHR Act and the terms of the Portal Operator Registration Agreement (s 51(3)). It is open to the Agency to cancel or suspend a Mobile Application Developer's registration quickly, in urgent circumstances (s 53(4) and (5)).

Fourth, the Agency has proposed to take steps to monitor compliance with the MHR Act and the terms of the Portal Operator Registration Agreement, in this regard.[66]

When considered together, and subject to the implementation of a rigorous compliance monitoring program, we consider these arrangements to be reasonable steps to ensure a Registered Portal Operator does not disclose a Consumer's personal information overseas.

9.9 APP 9 — Adoption, use or disclosure of government related identifiers

Individual healthcare identifier (IHI)

The Project does not envisage the Agency collecting, using or disclosing of a Consumer's individual healthcare identifier (**IHI**), a type of government related identifier. However, the Agency may disclose healthcare identifiers of the Consumer, Authorised Representatives, Nominated Representatives and healthcare providers if it is embedded in records in a Consumer's My Health Record. IHI's do not appear to be used during the identity verification process.

The use and disclosure by the Agency, in its role as system operator of the My Health Record, of healthcare identifiers of the Consumer, Authorised Representatives, Nominated Representatives and healthcare providers is authorised by section 58A of the MHR Act, in particular item 1 of s 58A(1).

Accordingly, the use and disclosure of such healthcare identifiers will comply with the HI Act and Privacy Act as it is authorised under another Commonwealth law, in accordance with subsection 26(3)(b) of the HI Act and with APP 6.2(b) (disclosure of personal information), respectively.

[65] Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View only access* (22 November 2018).

[66] Instructions received 3 February 2020.

9.10 APP 11 — Security of personal information

For the reasons set out below, we consider the Project to be generally compliant with APP 11.

APP 11 requires that an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

It is beyond the scope of this PIA to undertake a comprehensive threat analysis or evaluate the security and access arrangements for the Agency. That said, from a privacy perspective, it is important that the outcome required by APP 11 is met, namely that reasonable steps are taken by the Agency to protect the information collected. In this regard, we note the Agency has already taken a number of steps to protect a Consumer's personal information. These are set out in My Health Record Privacy Policy.[67]

In order to ensure it is continually meeting the APP 11 requirement, the Agency should carefully review its security and access arrangements to ensure that all reasonable risk (both internal and external) of unauthorised or inappropriate access is mitigated. The OAIC's *Guide to Securing Personal Information* contains further useful guidance on this issue.[68]

9.11 APP 13 — Correction of personal information

For the reasons set out below, we consider the Project to be generally compliant with APP 13.

APP 13 requires that an APP entity must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

A link to the My Health Record Privacy Policy is available online at https://www.myhealthrecord.gov.au/. It currently directs Consumers (or their Authorised or Nominated Representative) to the My Health Record Help Line and a post office box address if they wish to correct their My Health Record.

We consider the Project to be compliant with APP 13 to the extent that, under the existing arrangements for the correction of a Consumer's My Health Record, the Agency also:

- takes reasonable steps to notify other APP entities of a correction
- gives notice to the Consumer (or their Authorised or Nominated Representative), which includes reasons and available complaint mechanisms if correction is refused
- takes reasonable steps to associate a statement with personal information it refuses to correct
- responds to a request for correction or to associate a statement, and
- does not charge a Consumer (or their Authorised or Nominated Representative) for making a request, correcting personal information or associating a statement.

[67] Australian Digital Health Agency *Privacy Policy* (20 January 2020) https://www.myhealthrecord.gov.au/about/privacy-policy

[68] OAIC *Guide to Securing Personal Information* (5 June 2018) https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/.

10. Privacy management — addressing risks

Part 10 of the PIA addresses the risks to privacy in the Project's current design that were identified in Part 10 of the PIA. These risks mainly affect a Consumer's privacy and the Agency's reputation, or both.

Options that may assist the Agency to address the risks to privacy are considered below.

10.1 Alignment with community expectations

It is important that the Agency takes steps to audit the security and information handling practices of Mobile Application Developers so as to mitigate the risk of a compromise of the My Health Record data after it leaves the My Health Record system.

Recommendation 1:

The Agency should put in place contractual arrangements with Mobile Application Developers that require:

- the Mobile Application Developer's compliance with the APPs
- the documentation of the Mobile Application Developers' security procedures for the handling of personal information, with special attention given to the way in which the Mobile Application Developer will use (and not record) a Consumer's personal information
- documents showing the technological tools and system design techniques that are being used by Mobile Application Developers to enhance privacy and security, for example encryption
- the production of documentation showing staff have been trained in the requirements for protecting personal information and are aware of policies regarding breaches of security or confidentiality, and
- evidence showing steps taken by the Mobile Application Developer to destroy any personal information that it may have recorded in the course of acquiring a Consumer's personal information (for example, meta data).

Recommendation 2:

The Agency should ensure that an independent audit[69] is conducted of all the security risks and the reasonableness of countermeasures to secure the Mobile Application Developer's system against unauthorised or improper collection, access, modification, use, disclosure and disposal of a Consumer's personal information.

Recommendation 3:

The Agency should put in place audit mechanisms to ensure a Mobile Application Developer handles a Consumer's personal information in accordance with the contractual arrangements. These audit mechanisms should be in place:

- when the Agency is considering a Mobile Application Developer's application to become a Registered Portal Operator
- during the operation of the Mobile Application Developer's Mobile Application, and
- in the course of responding to any unauthorised handling of personal information.

[69] Independent, in this context, means independent from the Mobile Application Developer.

10.2 APP 1 — Open and transparent management of personal information

It is important that the Agency manages personal information in an open and transparent way, including via a clearly expressed and up-to-date Privacy Policy about how it manages personal information. It is also important that Consumers (or their Authorised or Nominated Representatives) are made aware of the fact that, and circumstances in which, the Agency collects information that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access their My Health Record, once and when the Consumer first uses a Mobile Application to access their My Health Record.

Recommendation 4:

The Agency should update its Privacy Policy to expressly state that the Agency may:

- collect personal information about a Consumer that is new to the Project, being:
    - that the Consumer (or their Authorised or Nominated Representative) is using a Mobile Application to access the Consumer's My Health Record, and
    - that the Consumer (or their Authorised or Nominated Representative) is using a particular type of Mobile Application to access their My Health Record, and

We consider it would be reasonable for the Agency to notify the Consumer (or their Authorised or Nominated Representative) once, for example, when they first use a Mobile Application to access the Consumer's My Health Record.

Recommendation 5:

The Agency should revise its Privacy Policy to clarify the fact that:

- a Consumer's personal information is not being made accessible or visible to the Mobile Application Developer. Rather, it is being passed through (and not disclosed to) the Mobile Application Developer's Intermediary Server, and
- the Mobile Application Developer is not permitted to access and view the Consumer's personal information from its Intermediary Server.

10.3 APP 11 — Security of personal information

It is beyond the scope of this PIA to undertake a comprehensive threat analysis, however, the Agency should, as part of its business-as-usual IT processes, review the information transfer, security and access arrangements for the Mobile Gateway to ensure that all reasonable risks of unauthorised access are mitigated.

Recommendation 6:

The Agency should ensure that all reasonable risk of unauthorised access is mitigated. The means by which this might be achieved are set out in the OAIC's *Guide to Securing Personal Information*.[70] This document provides guidance on the reasonable steps entities are required to take under the Privacy Act to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. It also includes guidance on the reasonable steps entities are required to take to destroy or de-identify personal information that they hold once it is no longer needed (unless an exception applies). This guide is not legally binding. However, the OAIC will refer to this guide when investigating whether an entity has complied with its personal information security obligations (s 40) or when undertaking an assessment (s 33C).

[70] OAIC *Guide to securing personal information* (5 June 2018) https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/

Schedule 1 - Sources

Ashurst *My Health Record – Mobile Apps: Models 1, 2 and 4 (Healthcare Recipient Apps) Privacy Impact Assessment* (24 March 2017).
Australian Digital Health Agency *Australia's National Digital Health Strategy.*
Australian Digital Health Agency *FHIR Gateway (Mobile)* (7 January 2020) https://developer.digitalhealth.gov.au/products/fhirr-gateway
Australian Digital Health Agency *My Health Record FHIR Gateway Consent Requirements and Guidelines (v 2.0)*.
Australian Digital Health Agency *My Health Record FHIR Gateway Security Requirements and Guidelines* (19 December 2016).
Australian Digital Health Agency *My Health Record Privacy Policy* (17 January 2020) https://www.myhealthrecord.gov.au/about/privacy-policy
Australian Digital Health Agency *Portal Operator Registration Agreement My Health Record System View Only Access* (22 November 2018).
Australian Digital Health Agency *Privacy Policy* (20 January 2020) https://www.myhealthrecord.gov.au/about/privacy-policy
Australian Digital Health Agency *View your record using an app* (7 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/howtos/view-your-record-using-app
Australian Digital Health Agency *What's in a My Health Record?* (7 January 2020) https://www.myhealthrecord.gov.au/for-you-your-family/whats-in-my-health-record
Department of Human Services *Individual Healthcare Identifiers* (20 November 2019) https://www.humanservices.gov.au/individuals/services/medicare/individual-healthcare-identifiers
Healthcare Identifiers Act 2010.
Minter Ellison Lawyers and Salinger Privacy *Privacy Impact Assessment Report Personally Controlled Electronic Health Record (PCEHR)* (15 November 2011) https://www.myhealthrecord.gov.au/about/privacy-policy/privacy-impact-assessments
Minter Ellison *Privacy Impact Assessment Report Personally Controlled Electronic Health Record (PCEHR) Prepared for the Commonwealth Department of Health and Ageing* (15 November 2011) https://www.myhealthrecord.gov.au/about/privacy-policy/privacy-impact-assessments.
My Health Records Act 2012.
My Health Records Regulation 2012.
My Health Records Rule 2016.
OAIC *APP Guidelines* (22 July 2019).
OAIC *Chapter 9: APP 9 — Adoption, use or disclosure of government related identifiers* (22 July 2019) 9.1 https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers/
OAIC *Guide to Securing Personal Information* (5 June 2018) https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/.
OAIC *Guide to undertaking privacy impact assessments.*

OAIC *My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016* https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/
Privacy Act 1988.
Privacy Impact Assessment Report *Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model* (20 May 2015) https://www.myhealthrecord.gov.au/about/privacy-policy/privacy-impact-assessments
Shearwater *Threat and Risk Assessment Mobility Gateway* (May 2018).

Schedule 2 - Glossary

Agency	Australian Digital Health Agency
API	Application Programming Interface
Application Programming Interface	The API is a set of instructions or commands, for example "GET" (to read or search, for example) "DELETE" (to delete) and "POST" (to update or transact). In order to access a Consumer's My Health Record, a Mobile Application uses the API to communicate with My Health Record system.
APPs	Australian Privacy Principles
Australian Digital Health Agency	The Agency responsible for national digital health services and systems. It is a statutory authority that reports to State and Territory Health Ministers through the Council of Australian Governments Health Council. The Agency operates and manages the My Health Record system.
Australian Privacy Principles	The Australian Privacy Principles are set out in the clauses of Schedule 1 to the Privacy Act.
Authorised Representative	*For Healthcare Recipients aged under 14* Each person who the System Operator is satisfied has parental responsibility for a Healthcare Recipient aged under 14 is the authorised representative of the Healthcare Recipient. However, a person who has parental responsibility for a Healthcare Recipient aged under 18 is not the authorised representative of the Healthcare Recipient if the System Operator is satisfied that: • under a court order or a law of the Commonwealth or a State or Territory, the person must be supervised while spending time with the Healthcare Recipient; or • the life, health or safety of the Healthcare Recipient or another person would be put at risk if the person were the authorised representative of the Healthcare Recipient. If there is no person who the System Operator is satisfied has parental responsibility for a Healthcare Recipient aged under 14, or the only such persons are covered by subsection (1A), the authorised representative of the Healthcare Recipient is: • a person who the System Operator is satisfied is authorised to act on behalf of the Healthcare Recipient for the purposes of this Act under the law of the Commonwealth or a State or Territory, or a decision of an Australian court or tribunal; or • if there is no such person—a person: • who the System Operator is satisfied is otherwise an appropriate person to be the authorised representative of the Healthcare Recipient; or • who is prescribed by the regulations for the purposes of this paragraph. *For Healthcare Recipients aged between 14 and 17* A person is the authorised representative of a Healthcare Recipient aged between 14 and 17 years if the Healthcare Recipient, by written notice given to the System Operator in the approved form, nominates the person to be his or her authorised representative. *For Healthcare Recipients aged at least 18*

	If the System Operator is satisfied that a Healthcare Recipient aged at least 18 is not capable of making decisions for himself or herself, the authorised representative of the Healthcare Recipient is: • a person who the System Operator is satisfied is authorised to act on behalf of the Healthcare Recipient under the law of the Commonwealth or a State or Territory or a decision of an Australian court or tribunal; or • if there is no such person—a person: • who the System Operator is satisfied is otherwise an appropriate person to be the authorised representative of the Healthcare Recipient; or who is prescribed by the regulations for the purposes of this paragraph.[71]
Consumers	Consumers are Healthcare Recipients who have a My Health Record and use a Mobile Application to view their Record. All Australians now have a My Health Record, unless they have chosen to opt out.
HCP	Healthcare Provider
Healthcare	Healthcare means Health Service within the meaning of subsection 6(1) of the Privacy Act (see s 5 of the MHR Act).

Health Information	The following information is health information
	• information or an opinion about:
	  • the health, including an illness, disability or injury, (at any time) of an individual
	  • an individual's expressed wishes about the future provision of health services to the individual, or
	  • a health service provided, or to be provided, to an individual
	that is also personal information
	• other personal information collected to provide, or in providing, a health service to an individual
	• other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances, or
	• genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.[72]

Health Service	An activity performed in relation to an individual is a health service if the activity is intended or claimed (expressly or otherwise) by the individual or the person performing it: • to assess, maintain or improve the individual's health; or • where the individual's health cannot be maintained or improved—to manage the individual's health; or • to diagnose the individual's illness, disability or injury; or • to treat the individual's illness, disability or injury or suspected illness, disability or injury; or

[71] MHR Act, s 6.

[72] Privacy Act, s 6FA

	• to record the individual's health for the purposes of assessing, maintaining, improving or managing the individual's health. The dispensing on prescription of a drug or medicinal preparation by a pharmacist is a health service.[73]
Healthcare Provider	Healthcare provider means: • an individual healthcare provider (being an individual who has provided, provides, or is to provide, healthcare; or is registered by a registration authority as a member of a particular health profession, or • a healthcare provider organisation (being an entity that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).[74]
Healthcare Provider Organisation	An entity that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).[75]
Healthcare Recipients	Healthcare recipient means an individual who has received, receives, or may receive, healthcare.[76]
HI Act	*Healthcare Identifiers Act 2010*
IHI	Individual Health Care Identifier
Individual Health Care Provider	An individual who as provided, provides, or is to provide, healthcare; or is registered by a registration authority as a member of a particular health profession.[77]
Interaction Model	Interaction Models set the way in which Mobile Applications communicate with the Mobile Gateway and handle a Consumer's personal information. They offer different functions and affect the way in which a Consumer's personal information will be collected, used and disclosed.
MHR Act	*My Health Records Act 2012*
Mobile Application Developers	Mobile Application Developers are third parties that develop software for mobile devices that may be used by Consumers to access their My Health Record.
Mobile Applications	Software for mobile devices that may be used by Consumers to access their My Health Record.
Mobile Gateway	The Mobile Gateway is a mechanism by which Mobile Applications can securely integrate and interact with the My Health Record system and give Consumers, and their Authorised Representatives and Nominated Representatives, access to their My Health Record. It separates the My Health Record system from the Internet by allowing only Mobile Applications that have the consent of Customers who have verified their identity via myGov, to communicate with the My Health Record system.

[73] MHR Act s 5 and Privacy Act s 6 and s 6FB.

[74] MHR Act, s 6.

[75] MHR Act, s 5.

[76] MHR Act, s 6.

[77] HI Act, s 5.

My Health Record	My Health Record of a healthcare recipient means the record of information that is created and maintained by the System Operator in relation to the healthcare recipient, and information that can be obtained by means of that record, including the following: • information included in the entry in the Register that relates to the healthcare recipient • health information connected in the My Health Record system to the healthcare recipient (including information included in a record accessible through the index service) • other information connected in the My Health Record system to the healthcare recipient, such as information relating to auditing access to the record, and • back-up records of such information.[78]
My Health Record system	My Health Record system means a system that is for: • the collection, use and disclosure of information from many sources using telecommunications services and by other means, and the holding of that information, in accordance with the healthcare recipient's wishes or in circumstances specified in the MHR Act; and • the assembly of that information using telecommunications services and by other means so far is it is relevant to a particular healthcare recipient, so that it can be made available, in accordance with the healthcare recipient's wishes or in circumstances specified in the Act, to facilitate the provision of healthcare to the healthcare recipient or for purposes specified in the Act; and that involves the performance of functions under the Act by the System Operator.[79]
myGov Credentials	A Consumer verifies their identity by signing into myGov using their myGov Credentials, being their username (or email address) and password.
Nominated Representative	An individual is the nominated representative of a healthcare recipient if: • an agreement is in force between the individual and the healthcare recipient that the individual is the healthcare recipient's nominated representative for the purposes of this Act; and • the healthcare recipient has notified the System Operator that the individual is his or her nominated representative.[80]
OAIC	Office of the Australian Information Commissioner.
Privacy Act	*Privacy Act 1988*
PIA	Privacy Impact Assessment
Project	The ongoing operation of the Mobile Gateway to allow a Mobile Application to provide My Health Record information to Consumers to view only.[81] The Project proposes to give access to the My Health Record system to Mobile Application Developers who build Mobile Applications used by Consumers to view their My

[78] MHR Act, s 5.

[79] MHR Act, s 5.

[80] MHR Act, s 7.

[81] Instructions received on 3 February 2020.

	Health Record from their mobile devices. In order to do so, the Agency proposes to re-open and operate the Mobile Gateway with Mobile Application Developers who are Registered Portal Operators under the MHR Act.[82]
Registered Healthcare Provider Organisation	Registered healthcare provider organisation means a healthcare provider organisation that is registered under section 44 of the MHR Act.[83]
Registered Portal Operator	A person that: • is the operator of an electronic interface that facilitates access to the My Health Record system; and • is registered as a portal operator under section 49 of the MHR Act.[84]
System Operator	The System Operator is: • the Secretary of the Department; or • if a body established by a law of the Commonwealth is prescribed by the regulations to be the System Operator—that body.[85] The Agency has been prescribed as the System Operator by regulation 2.1.1 of the My Health Records Regulation 2012, pursuant to section 14(1)(b) of the MHR Act.

[82] Instructions received on 3 February 2020.

[83] MHR Act, s 5.

[84] MHR Act, s 5.

[85] MHR Act, s 14.