Australian Government
Australian Digital Health Agency

My Health Record FHIR Gateway Consent Requirements and Guidelines

20 February 2023 v1.2

Approved for external use

Document ID: DH-3705:2023

Note

This document must be read in conjunction with the Portal Operator Registration Agreement (PORA)

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements

The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

HL7 International

This document includes excerpts of HL7™ International standards and other HL7 International material. HL7 International is the publisher and holder of copyright in the excerpts. The publication, reproduction and use of such excerpts is governed by the HL7 IP Policy and the HL7 International License Agreement. HL7 and CDA are trademarks of Health Level Seven International and are registered with the United States Patent and Trademark Office.

Disclaimer

The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

OFFICIAL

Document information

Key information

Owner	Product Owner, Mobile	
Contact for enquiries	Australian Digital Health Agency Help Centre	
	Phone	1300 901 001
	Email	help@digitalhealth.gov.au

Product or document version history

Product or document version	Date	Release comments
v1.1	19/03/2020	Final version for release
V1.2	20/02/2023	Updated version for release

Table of contents

1 Introduction

1.1 Purpose

The purpose of this document is to define the consent requirements and guidelines for applications (apps) connecting with the My Health Record system APIs via the HL7™FHIR® standard gateway, using interaction models #1 or #4 (refer to Appendix A for details).

For the purposes of this document:

- Registered portal operators are referred to as "developers"
- The Agency is the System Operator (SO) for the purposes of the *My Health Record Act 2012* (Cth).
- References to "User" may to refer to a Registered Healthcare Recipient, Authorised Representative or Nominated Representative who may use the portal.

1.2 Intended audience

The intended audience for this document is:

- registered portal operators (which includes mobile application developers), and
- the System Operator (which includes the National Infrastructure Operator and the Gateway Operator)

1.3 Scope

These requirements apply to consumer apps connecting with the My Health Record system.

This document does not address the My Health Record business-to-business (B2B) web-services. Developers interested in using these services will need to complete a separate process including conformance with a different set of requirements, specifications, and the submission of specific B2B web-services forms.

Information about connecting to the B2B web-services can be obtained by emailing: help@digitalhealth.gov.au.

1.4 Background

Health information contained in a consumer's My Health Record is defined as sensitive information in s.6 of the *Privacy Act 1988* (Cth) (Privacy Act), which means that under the Australian Privacy Principles (APPs), specifically APP 3.3, developers collecting such information must first obtain a user's informed consent and the collection must be reasonably necessary for, or directly related to one or more of the Agency's functions or activities. Consumers must be provided with enough information when giving their consent to releasing information from their My Health Record to an application (app).

When seeking consent, app developers are required by the Privacy Act at or before the time of collection to provide a collection notice under (APP 5), which lists the information that needs to be provided to consumers, including:

- The identity and contact details of the entity collecting their personal information
- Why is their personal information being collected
- Consequences (if any) for the individual if some or all of their personal information is not collected
- Any other person, entity, or body to which the app developer may usually disclose personal information
- The privacy policy of the app developer, including how the individual may access, seek correction of their personal information and how they may make a complaint about the handling of their personal information if they believe an app has been breached.
- Who has access to their personal information, including whether their personal information is likely to be sent overseas and, if so, the countries in which recipients are likely to be located
- The legal authority under which their personal information is being collected, used, and disclosed

The SO has provided requirements to support developers with their consent design. These requirements are not intended to prescribe specific designs which developers must replicate, noting that developers must satisfy themselves that their designs meet the requirements of the Privacy Act. Instead, each requirement supports a design intention which the developer can utilise as a basis for obtaining informed consent. While these design requirements were determined with a specific flow in mind, developers do not need to follow this process step-by- step but should contact the Agency at help@digitalhealth.gov.au for advice.

Each developer must demonstrate that they have implemented the design intent at some point as part of the consent screen flow, while maintaining the consistency necessary for an end-to-end process (i.e. between the My Health Record screens and the developer screens). These requirements are based on a mobile interface. However, the same requirements can be applied to desktop interfaces, as long as the design intent is met, and the informed consent criterion is met to the satisfaction of the Agency.

The consent flow for apps to link to the My Health Record consists of screens that are both hosted by the app and the My Health Record system (utilising the myGov OAuth process). Therefore, it is also important that the screens hosted by the app make sense from a user experience and provide a consistent and comprehensible consent process.

The *Australian Privacy Principles Guidelines* [1] from the Office of the Australian Information Commissioner (OAIC) specifies that the four key elements of consent are as follows:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific
- the individual has the capacity to understand and communicate their consent.

https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts

App developers that are designing screens to capture consent to access a user’s My Health Record need to incorporate the above elements of consent.

1.5 Types of applications

The following types of apps can connect to the My Health Record APIs and are referenced throughout this document:

1 **Mobile applications** are developed to run natively on a specific mobile device or platform (e.g. iOS, Android).

2 **Web applications** are powered by a web browser (e.g. Chrome, Firefox, Safari) through the internet. Web applications are typically built using HTML, CSS and JavaScript and are served through a mobile or desktop browser. Web applications can be built to look and feel just like a native application but will always runs through a visible browser.

3 **Hybrid applications** are usually coded in HTML, CSS and JavaScript. They are run through an invisible browser which has been packaged into a native application. This enables the application to have the look, feel and functionality of a native application. Hybrid applications allow developers to minimise development time as minimal work is required to target various mobile operating systems. An additional benefit of using a hybrid application framework includes allowing developers to access Native API calls which can be used to enable binary security mechanisms from the device itself. Hybrid applications can also be distributed through native application stores (allowing for additional vetting).

4 **Progressive web applications (PWA)** can appear and behave as native applications on mobile devices but do not require installation of the application on the device.

Developers may choose one app type or a solution that combines multiple app types (e.g. both a web app for web browser use and hybrid app for mobile device app use). The type of app developed, and target consumer audience will determine the model for interacting with the My Health Record system. For example, an app may connect directly to the My Health Record via the FHIR® gateway, or via an intermediary server managed by the app developer. Refer to Appendix A for the interaction model diagrams.

1.6 Requirement keywords

The following normative verbs in these requirements should be read as follows.

SHALL	When appearing in a conformance requirement, the verb **SHALL** indicates a mandatory requirement. Its negative form **SHALL NOT** indicates a prohibition.
SHOULD	When appearing in a conformance requirement, the verb **SHOULD** indicates a recommendation. Its negative form **SHOULD NOT** indicates an option that is recommended against.
MAY	When appearing in a conformance requirement, the verb **MAY** indicates an optional requirement.

2 Consent requirements

As a condition of connecting to the My Health Record system, app developers are required to comply with the Privacy Act regardless of whether or not the app developer is already subject to the Privacy Act. Within the Privacy Act, there are several (APPs) that are particularly relevant to app developers:

- APP 1 requires that app developers have a privacy policy that addresses the requirements of the Privacy Act, informing individuals about how their personal information will be handled.
- APP3 requires that app developer only collect personal information in a lawful manner.

  The app developer may only collect personal information to:
  - undertake the job at hand, **and**
  - the job at hand must be directly related to one or more of the app developer's functions or activities, **and**
  - the collection must be fair and lawful.

  They can only collect personal information that is reasonably necessary [1]for the job at hand; they cannot collect additional personal information because it is interesting or might be useful 'one day'.

- APP 5 requires that app developers provide a collection notice at or before the time they are collecting personal information from users.
- APP6 requires that app developers only use or disclose personal information in a lawful manner.
- APP7 requires that app developers do not use or disclose personal information for the purpose of direct marketing outside of the provisions of this APP.
- APP8 requires that app developer does not disclose personal information to an overseas recipient outside of the provisions of this APP. Note that there are very strict requirements around MHR information not being disclosed in this manner.
- APP9 requires that an app developer not adopt, use, or disclose a government related identifier outside the provisions of this APP
- APP 11 requires that app developers take reasonable steps to protect the security of the personal information they collect.
- APP 12 requires that the app developer must, on request, provide an individual with access to any personal information they hold about that individual.
- APP13 requires that the app developer must be satisfied any personal information they hold about an individual is not inaccurate, out of date, incomplete, irrelevant, or misleading. Additionally, the app developer must, on request, take any reasonable step to correct personal information they hold about an individual.

[1] The Australian Privacy Commissioner considers the term 'reasonably necessary' as requiring a 'consideration of whether or not it is clearly appropriate and relevant to the functions or activities of the organisation'.

Guidelines on the APPs are published by the OAIC and are available online.[2]

The following requirements are provided to support app developers in designing the process for informing users about information handling and consent-collection. The Australian Digital Health Agency (referred to in this document as “the Agency”) has conducted user testing to determine the relative effectiveness of various models of consent collection.

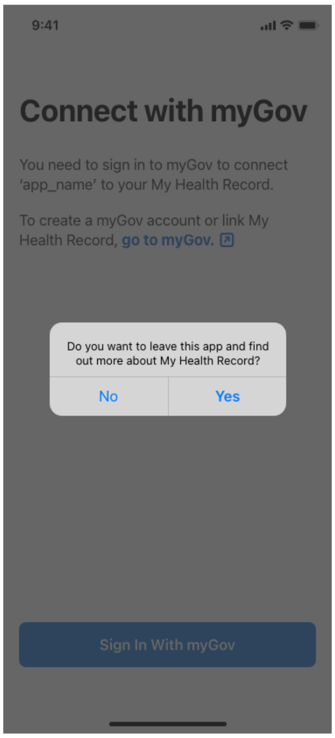
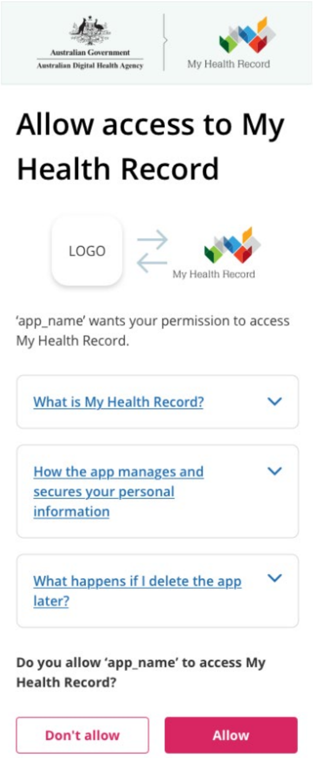
Most requirements are supported by an example design approach. See Appendix B for an end-to-end example of the consent flow that has been user tested.

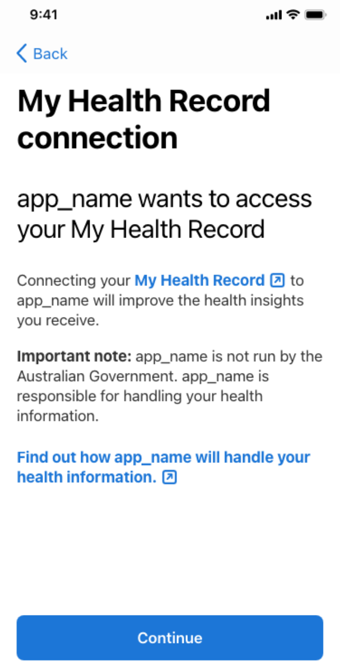
The SO may defer or reject a developer’s access to the production environment if it considers that an app's design does not satisfy the requirements stated in this document. The developer is responsible for understanding its privacy obligations and ensuring the information provided to users is accurate and up to date.

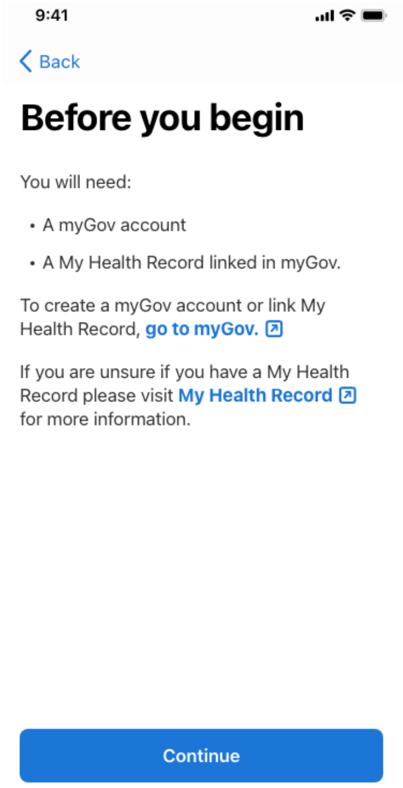
Req. C001	**Gathering express and informed consent.**
Description	Apps **SHALL** adequately inform users about information collection and use before requesting consent to access the user’s My Health Record in line with the requirements of the Privacy Act and APPs.
Additional information	Refer to the OAIC’s Australian Privacy Principles Guidelines and Appendix C for further information on consent.

Req. C002	**Provide evidence that the flow achieves express and informed consent.**
Description	Apps **SHALL** demonstrate to the System Operator that users are: • adequately informed about how their information accessed from the user’s My Health Record is collected, used, and disclosed; and • requested to consent to the collection, use and disclosure of their information. At a minimum this **SHOULD** include screenshots which demonstrate all aspects of the flow (see Appendix B for an example), including links from the main flow to further information. However, the Agency encourages developers to provide other evidence including prototypes, access to test apps, and supporting research or user testing.
Additional information	The evidence provided will be used by the System Operator as part of an overall risk assessment conducted prior to granting access to the production environment. Apps that are deemed to have inadequate consent collection processes, or do not meet all criteria for the provision of informed consent, will have their access to the production environment deferred or rejected.

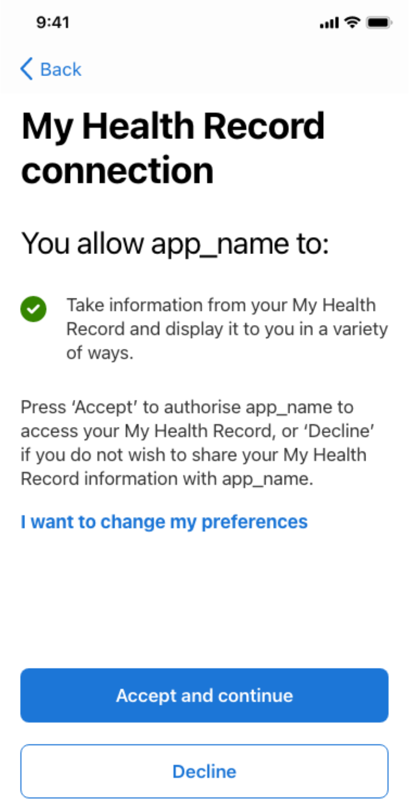
[2] Office of the Australian Information Commissioner, “Australian Privacy Principles Guidelines - Privacy Act 1988,” 31 March 2015. [Online]. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines.

Req. C003	**Initiating the process of linking an app to the My Health Record.**
Description	Apps **SHALL** have a process in place to initiate the linking of the app to the My Health Record. Suggested text is below: *"Allow [app name] to access your My Health Record"* The app **SHOULD** also include the My Health Record and app information exchange picture (i.e. the two logos with two arrows between them) at the initiation stage.
Additional information	The inclusion of the My Health Record and app information exchange picture at the initiation stage helps users establish that the consent process involves two entities; the app developer and the My Health Record system.
Reference screen	 9:41 Connect with myGov You need to sign in to myGov to connect 'app_name' to your My Health Record. To create a myGov account or link My Health Record, go to myGov. Do you want to leave this app and find out more about My Health Record? No Yes Sign In With myGov  Australian Government Australian Digital Health Agency My Health Record Allow access to My Health Record LOGO My Health Record 'app_name' wants your permission to access My Health Record. What is My Health Record? How the app manages and secures your personal information What happens if I delete the app later? Do you allow 'app_name' to access My Health Record? Don't allow Allow

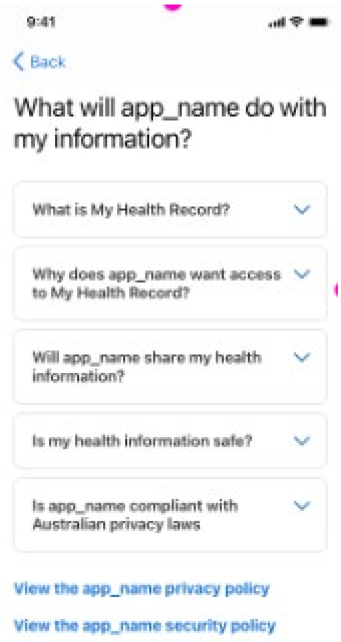
Req. C004	**Introduce the My Health Record.**
Description	Early in the consent flow the developer **SHALL** include the following statement: *Important note: [app name] is not run by the Australian Government. [app name] is responsible for handling your health information. Find out how [app name] will handle your health information.* Applications **SHOULD** provide a brief introduction to the My Health Record (see Req C007). Apps **SHALL** explain why they want access to a user's My Health Record and provide a link to the app's privacy policy where the user can find more information.
Additional information	The intent of this requirement is to recommend that the app explain why a user would want to undertake the linking process and to explain that the app is a separate entity from the My Health Record system. Users may not be familiar with My Health Record and will need guidance to learn more. They may also not understand the benefit of linking their My Health Record to the app. User testing indicated that users may believe the app they are using is owned or endorsed by the Australian Government. This requirement establishes from the outset that the app is a separate entity from the Australian Government. The inclusion of the important note at this stage ensures that the users understand the separation between the app and the My Health Record prior to giving consent to the use of their health information.
Reference screen	 **My Health Record connection** app_name wants to access your My Health Record Connecting your **My Health Record** to app_name will improve the health insights you receive. **Important note:** app_name is not run by the Australian Government. app_name is responsible for handling your health information. **Find out how app_name will handle your health information.**

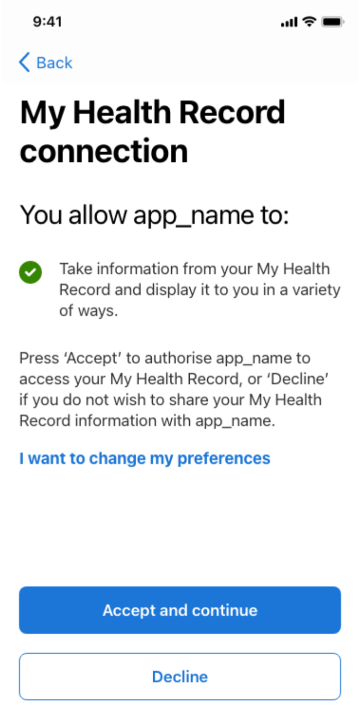
Req. C005	**Prerequisites to linking to a My Health Record.**
Description	Apps **SHALL** inform users that they will need a myGov account and a My Health Record that is linked to their myGov account. The users **SHALL** be provided with a link to the following URL in order to find out more about getting a myGov account or My Health Record. Suggested text: To access My Health Record, you need a myGov account. Find out how to set up a My Health Record [Set up your record online | Australian Digital Health Agency] If a user clicks the link on this page the app **SHOULD** display a pop up indicating that they are going to be navigated outside the app to find out more about the My Health Record system.
Additional information	If a user is not informed of the prerequisites for linking to a My Health Record, they may undertake the consent flow and make it halfway before they realise what is required to complete the process resulting in a poor user experience. Some users will not have a myGov account or linked My Health Record account and will require additional information up-front about the registration process.
Reference screens	 **Before you begin** You will need: • A myGov account • A My Health Record linked in myGov. To create a myGov account or link My Health Record, **go to myGov.** If you are unsure if you have a My Health Record please visit **My Health Record** for more information.

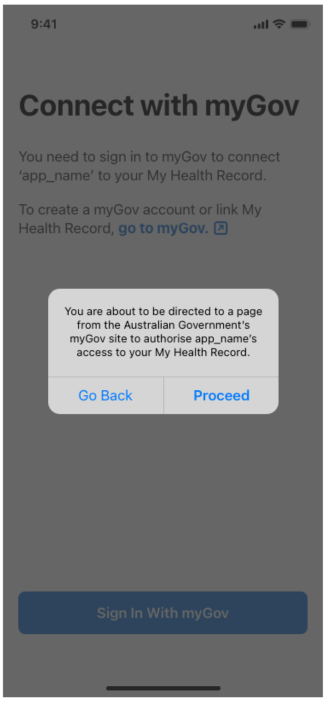
Req. C006	**Gaining express and informed consent for the app to access a user's My Health Record.**
Description	When seeking consent for an app to gain access to a user's My Health Record, apps **SHALL** clearly state: • what information the app will access from the My Health Record • the specific intended uses of the user's My Health Record information • any other information as required by the Privacy Act and APP 5. Users **SHALL NOT** need to read the app's full privacy policy or FAQs, or navigate to screens external to the app, to understand how their information will be handled (although a privacy policy must still be provided – see **Req. C007** below). If apps ask the user a series of questions to gather consent, the app **SHOULD** introduce the user to the process (see screen 5 in Appendix B) and **SHOULD** provide a progress indicator for the process. Users **SHOULD** also be able to go back and forth between steps to reconsider their choices and understand what they have done.
Additional information	Each developer will need to determine the key points that a user needs to be informed of when it comes to the use of the user's information. This includes reviewing the requirements of APP 5 and developing a collection notice that addresses these obligations. Developers should also consider the OAIC's guidance on bundled consent [1], including providing guidance on what it means to withhold consent for specific uses of information. The intent behind this requirement is that users are made aware of how their information will be handled (at a summary level), without needing to read large privacy policies or terms and conditions. If users are not provided adequate information, and are asked to consent to specific uses of information that they do not understand, then our user testing suggests a high likelihood that users will delete the app. Our user testing found that an effective method to ensure that users understand what they are consenting to is to pose a series of targeted questions to the users across a number of screens. This breaks up the complexity and forces a user to think about each question before they answer. This method also enables the user to consent to one particular intended use of their My Health Record information, but not consent to a different intended use of their health information.

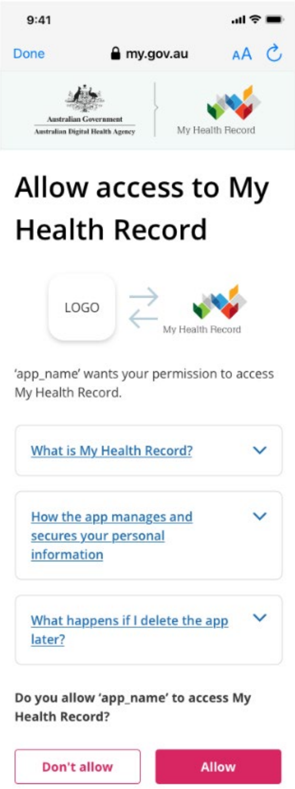
Req. C006	**Gaining express and informed consent for the app to access a user's My Health Record.**
Reference screens	 My Health Record connection You allow app_name to: ✓ Take information from your My Health Record and display it to you in a variety of ways. Press 'Accept' to authorise app_name to access your My Health Record, or 'Decline' if you do not wish to share your My Health Record information with app_name. I want to change my preferences Accept and continue Decline **NOTE:** See Appendix B Example consent flow for an expanded set of the above screens.

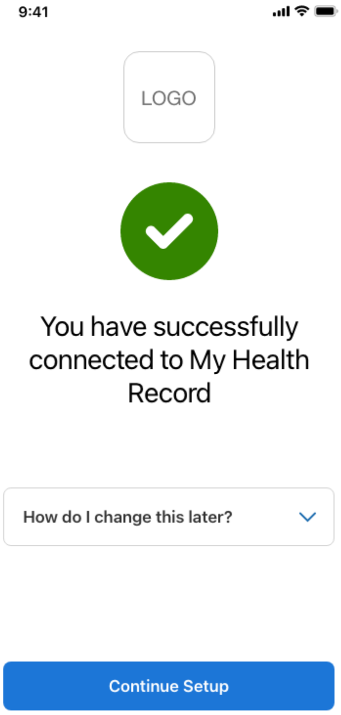
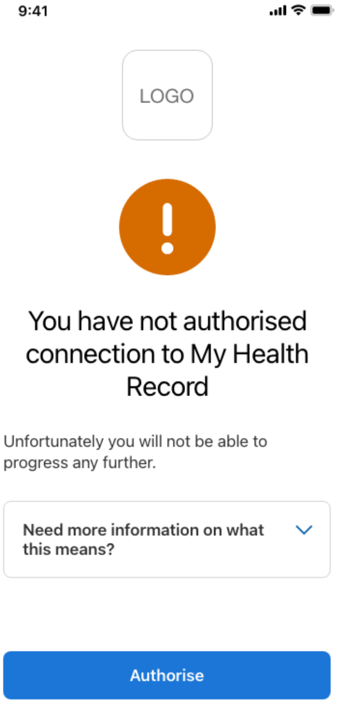
Req. C007	**Detailed consent information.**
Description	The app **SHALL** provide users with the opportunity to read more information about how the app is going to interact with their My Health Record and use the information that it downloads from the My Health Record. • *What is the My Health Record?* [For this first question, apps **SHALL** provide the following answer] *The My Health Record system is a national digital health record system, managed by the Australian Government.* *Having a My Health Record gives you a secure electronic summary of your health information and means you, and any participating doctors, nurses and other healthcare professionals involved in your care will, have access to a summary of your information – including medications, allergies, and immunisations.* *This will contribute to better, safer, and more efficient care for you.* *Information in your My Health Record can include your personal details and important health information such as discharge summaries from hospitals, allergies, medical conditions and treatments, medicine details and test or scan reports.* *If you are unsure if you have a My Health Record, find out more about My Health Record* https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record. • *Why does [app name] want access to My Health Record?* • *What health information will [app name] download from the My Health Record?* • *Will [app name] share my health information?* • *Is my personal information safe?* • *Is [app name] compliant with Australian privacy laws?* The app **SHALL** also display or provide links to their full privacy policy and full security policy. See *My Health Record – Security Requirements and Guidelines* [3] for more details on the security policy.
Additional information	This is the screen where a developer can include detailed information about what they are going to do with a user's information, what their obligations are, link to their own privacy policy etc. More information on having an APP compliant Privacy Policy is available in the OAIC's *Australian Privacy Principles Guidelines* [1].

Req. C007	Detailed consent information.
Reference screens	 9:41 Back What will app_name do with my information? What is My Health Record? Why does app_name want access to My Health Record? Will app_name share my health information? Is my health information safe? Is app_name compliant with Australian privacy laws View the app_name privacy policy View the app_name security policy

Req. C008	**Consent summary.**
Description	Apps **SHOULD** clearly summarise what the user has agreed to when providing consent for an app to access their My Health Record. The user **SHALL** be asked to agree to the use of their My Health Record information after the user has been informed of the specific intended uses of their My Health Record information (see **Req. C006**). The user **SHALL** be provided with the following statement: *Press “I agree” to authorise [app name] to access your My Health Record, or “Cancel” if you do not wish to share your My Health Record information with [app name].* The user **SHOULD** be given the opportunity to edit their preferences on the summary screen after agreeing to share their information with the app, or return to the start of the flow. The user should also be given an option to withdraw their consent at any time and advised on how this may be done
Additional information	The purpose of the summary is to allow users who rapidly click through the consent questions to pause and reflect on what they are agreeing to.
Reference screen	 9:41 Back **My Health Record connection** You allow app_name to: ✓ Take information from your My Health Record and display it to you in a variety of ways. Press ‘Accept’ to authorise app_name to access your My Health Record, or ‘Decline’ if you do not wish to share your My Health Record information with app_name. I want to change my preferences Accept and continue Decline

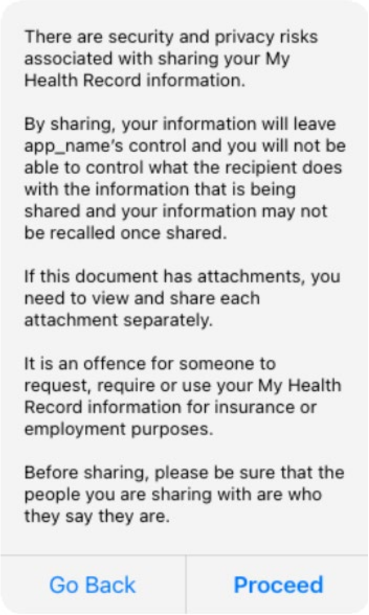
Req. C009	**Prompt users prior to being directed to the myGov site.**
Description	The apps **SHALL** provide a statement that indicates the app will direct the user to the Australian Government's myGov site to authorise the app's access to their My Health Record.
Additional information	User testing has indicated that some users were unaware throughout the consent process whether they were interacting with the My Health Record or the app. This requirement helps to reinforce a clear distinction between the app and the My Health Record.
Reference screen	 Connect with myGov You need to sign in to myGov to connect 'app_name' to your My Health Record. To create a myGov account or link My Health Record, go to myGov. You are about to be directed to a page from the Australian Government's myGov site to authorise app_name's access to your My Health Record.

Req. C010	**Provide content for the My Health Record hosted OAuth screens.**
Description	Developers **SHALL** provide certain information to the System Operator, in order for the System Operator to populate app-specific information on consent screens hosted by the My Health Record system. The System Operator will advise developers as to what information is required to be provided in order to meet this requirement.
Additional information	The System Operator will host a consent screen as part of the OAuth process which contains information specific to the app attempting to access the My Health Record. Input information required from apps includes: 1 the app logo - PNG format and 64 x 64 pixels in colour 2 the exact name of the app as it should be referred to on the consent screen. For content that the My Health Record will include under each of the FAQs see Appendix D.
Reference screen (Note: This screen is hosted by the My Health Record system)	 9:41 Done my.gov.au AA Australian Government Australian Digital Health Agency My Health Record LOGO My Health Record Allow access to My Health Record 'app_name' wants your permission to access My Health Record. What is My Health Record? How the app manages and secures your personal information What happens if I delete the app later? Do you allow 'app_name' to access My Health Record?

Req. C011	**Process completion screen.**
Description	Following the completion of the OAuth process, the app **SHALL** indicate to the user whether the process has been completed successfully or unsuccessfully. If the process is successful the app **SHALL** provide guidance on how these settings can be changed later, either on the app side or on the My Health Record side. If the user has withheld access, then the app **SHALL** provide guidance on the outcomes of withholding consent.
Additional information	Users expect that – after completing this process – they will receive feedback as to whether it has been successful or not.
Reference screens	 9:41 LOGO How do I change this later? Continue Setup You have successfully connected to My Health Record  9:41 LOGO Need more information on what this means? Authorise You have not authorised connection to My Health Record Unfortunately you will not be able to progress any further.

Req. C012	**Consent to Share**
Description	If the apps are providing the ability for consumers to share MHR data, then the apps **SHALL** display the following information and warnings to users before they use the ‘Share’ functionality: • there are security and privacy risks associated with sharing their MHR data • by sharing, the MHR data will leave the apps’ control and the user will not be able to control what the recipient does with the information that is being shared and that their information may not be recalled once shared. • it is an offence for a person to request, require or use information from a My Health Record for insurance or employment purposes. • it is important to confirm the details of the recipient(s) before sharing. • be clear with communication using plain English alerts • ensure any related document attachments are included
Additional information	This is to ensure that the app is providing sufficient alerts to the consumers before they attempt to share their MHR data. This requirement will only be applicable if the app provides ‘Share’ feature. Note the PORA requires retention of consents, refer to Clause 5.27. Consumers shall be made aware of the health information they are about to share, prior to sharing this information to the intended recipient. Some examples of attachments include: - PDF - JPEG - PNG - JPG - GIF - HTML - TXT

Reference screen



There are security and privacy risks associated with sharing your My Health Record information.

By sharing, your information will leave app_name’s control and you will not be able to control what the recipient does with the information that is being shared and your information may not be recalled once shared.

If this document has attachments, you need to view and share each attachment separately.

It is an offence for someone to request, require or use your My Health Record information for insurance or employment purposes.

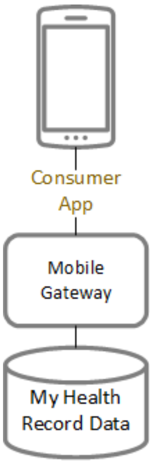
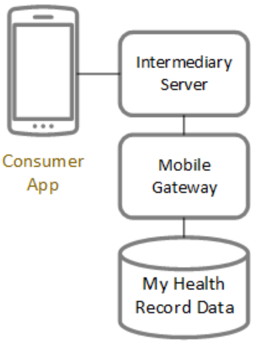
Before sharing, please be sure that the people you are sharing with are who they say they are.

Req. C013	**Prompt consumers that storing data may have automated cloud back up implications.**
Description	The apps **SHALL** provide a statement that reminds consumers that any My Health Record data which is saved to their device is subject to automated cloud backups or any other data handling relating to file locations which has already been agreed to such as Apple Inc and Apple iOS or Google and Android operating systems.
Additional information	This is to ensure that the app is providing sufficient alerts to the consumers before they store their MHR data. This requirement will only be applicable if the app provides the 'Share' feature.

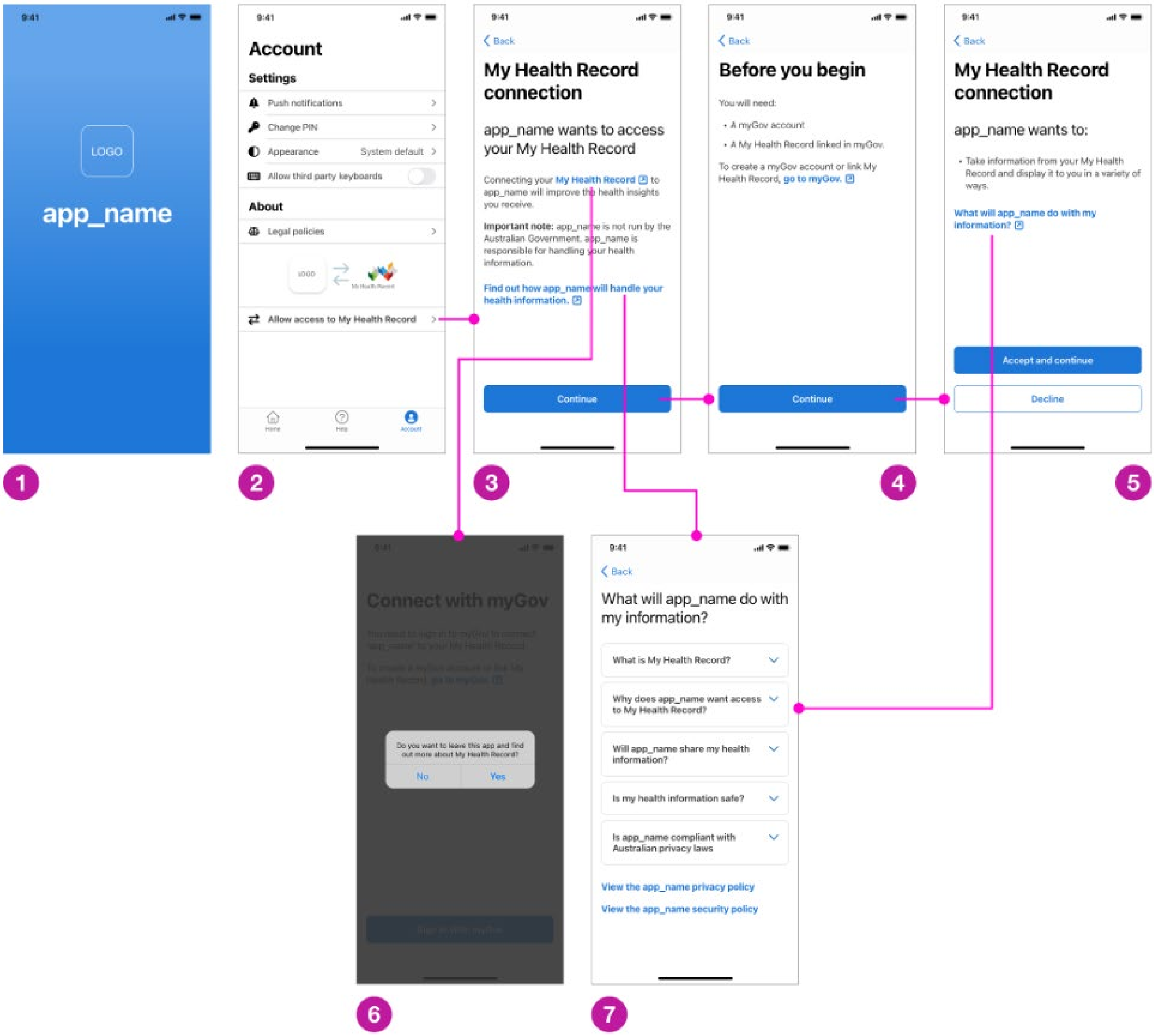
Appendix A Interaction models

The following table describes the two currently available interaction models for an application to connect with the Health Record system, and they vary based on the type of app, app end-users, and intended plans for accessing, using, and storing My Health Record data.

Current interaction models

Interaction model	Description
#1 Consumer / Self-Care  	Consumer mobile app connects with the My Health Record system via the FHIR® gateway.
 Intermediary Server Consumer App Mobile Gateway My Health Record Data #4 Consumer Connection via Platform	Consumer mobile app connects with the My Health Record system via an intermediary server (managed by the Mobile Application Developer), which orchestrates the flow of data between the mobile app, FHIR® gateway, or an end server (either managed by the Mobile Application Developer or third party). **Note:** It is possible that the data accessed via the intermediary server may be presented to the end user in a web app (e.g. portal accessible via a web browser).

Appendix B Example consent flow



1

2

3

My Health Record connection

app_name wants to access your My Health Record

Connecting your My Health Record to app_name will improve the health insights you receive.

Important note: app_name is not run by the Australian Government. app_name is responsible for handling your health information.

Find out how app_name will handle your health information.

4

Before you begin

You will need:

- A myGov account
- A My Health Record linked in myGov.

To create a myGov account or link My Health Record, go to myGov.

5

My Health Record connection

app_name wants to:

- Take information from your My Health Record and display it to you in a variety of ways.

What will app_name do with my information?

6

Connect with myGov

You need to sign in to myGov to connect app_name to your My Health Record.

To create a myGov account or link My Health Record, go to myGov.

Do you want to leave this app and find out more about My Health Record?

7

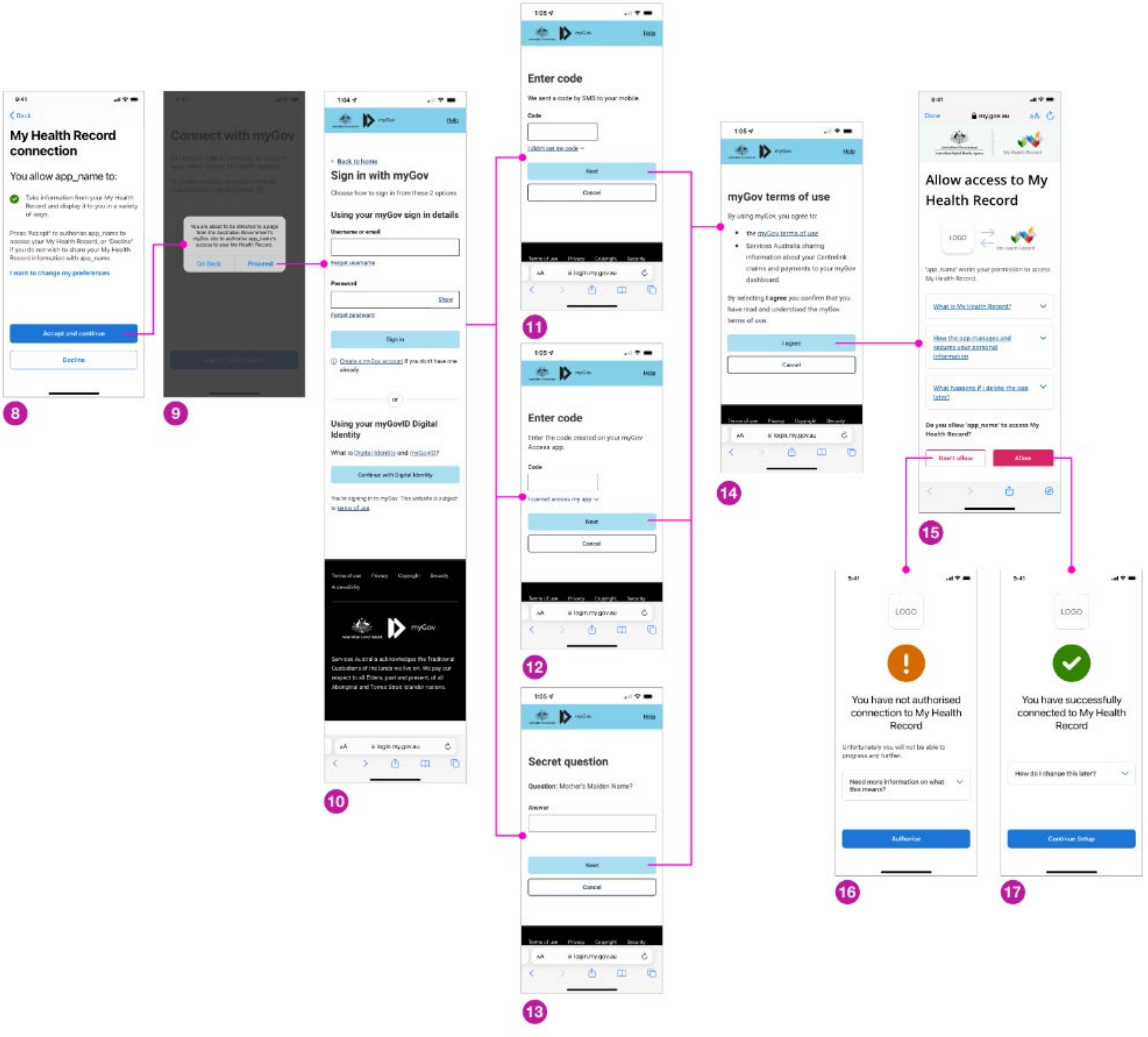
What will app_name do with my information?

- What is My Health Record?
- Why does app_name want access to My Health Record?
- Will app_name share my health information?
- Is my health information safe?
- Is app_name compliant with Australian privacy laws

View the app_name privacy policy

View the app_name security policy

Figure 1: Example flow – page 1



8

Back

My Health Record connection

You allow app_name to:

Take information from your My Health Record and display it to you in a variety of ways.

Press 'Accept' to authorise app_name to access your My Health Record, or 'Decline' if you do not wish to share your My Health Record information with app_name.

I want to change my preferences

Accept and continue

Decline

9

Connect with myGov

You are about to be directed to a page from the Australian Government's myGov site to authorise app_name's access to your My Health Record.

Go Back

Proceed

10

Back to home

Sign in with myGov

Choose how to sign in from these 2 options

Using your myGov sign in details

Username or email

Forgot username

Password

Show

Forgot password

Sign in

Create a myGov account if you don't have one already

or

Using your myGovID Digital Identity

What is Digital Identity and myGovID?

Continue with Digital Identity

You're signing in to myGov. This website is subject to terms of use

Terms of use Privacy Copyright Security Accessibility

Services Australia acknowledges the Traditional Custodians of the lands we live on. We pay our respect to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.

login.my.gov.au

11

Enter code

We sent a code by SMS to your mobile.

Code

I didn't get my code

Next

Cancel

12

Enter code

Enter the code created on your myGov Access app.

Code

I cannot access my app

Next

Cancel

13

Secret question

Question: Mother's Maiden Name?

Answer

Next

Cancel

14

myGov terms of use

By using myGov, you agree to:

- the myGov terms of use
- Services Australia sharing information about your Centrelink claims and payments to your myGov dashboard.

By selecting **I agree** you confirm that you have read and understood the myGov terms of use.

I agree

Cancel

15

Done my.gov.au

Allow access to My Health Record

LOGO

My Health Record

'app_name' wants your permission to access My Health Record.

What is My Health Record?

How the app manages and secures your personal information

What happens if I delete the app later?

Do you allow 'app_name' to access My Health Record?

Don't allow

Allow

16

LOGO

You have not authorised connection to My Health Record

Unfortunately you will not be able to progress any further.

Need more information on what this means?

Authorise

17

LOGO

You have successfully connected to My Health Record

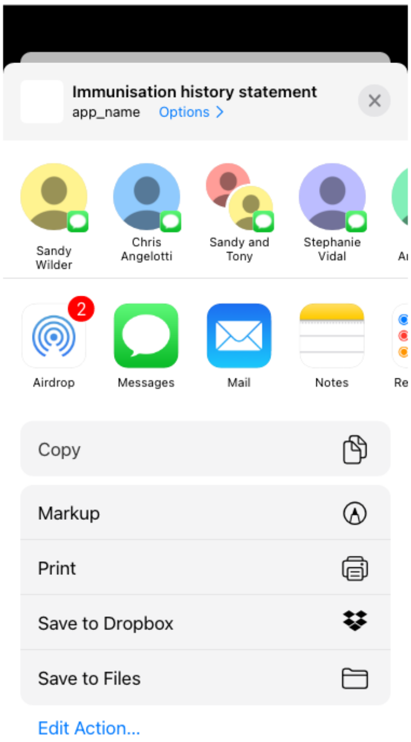
How do I change this later?

Continue Setup

Figure 2: Example flow – page 2

Appendix C Sharing immunisation history statement

Below is an illustrative example of how an Immunisation history statement can be shared.



Immunisation history statement

app_name Options >

Appendix D Consent

The OAIC's *Australian Privacy Principles guidelines* [1] specify that the four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific
- the individual has the capacity to understand and communicate their consent.

Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower the person's will. Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the individual, if they choose not to consent
- the seriousness of any consequences if an individual refuses to consent
- any adverse consequences for family members or associates of the individual if the individual refuses to consent.

Bundled consent refers to the practice of the "bundling" together of multiple requests for an individual's consent to a wide range of collections, uses, and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses, and disclosures they agree to and which they do not. This practice has the potential to undermine the voluntary nature of the consent.

If a bundled consent is contemplated, you could consider whether:

- it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more proposed collections, uses, or disclosures
- the individual will be sufficiently informed about each of the proposed collections, uses and disclosures
- the individual will be advised of the consequences (if any) of failing to consent to one or more of the proposed collections, uses, or disclosures.

An individual must be aware of the implications of providing or withholding consent; for example, whether access to a service will be denied if consent is not given to collection of a specific item of personal information. You should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent (see also, discussion of "capacity" below). The information should be written in plain English, without legal or industry jargon.

Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice to inform the individual of the period for which the consent will be relied on in the absence of a material change of circumstances.

Developers should not seek a broader consent than is necessary for your purposes, for example, consent for undefined future uses, or consent to "all legitimate uses or disclosures" (see also, discussion of “bundled consent” above). When seeking consent, an entity should describe the purpose to which it relates. The level of specificity required will depend on the circumstances, including the potential harm relating to any misuse of the personal information involved.

An individual may withdraw their consent at any time, and this should be an easy and accessible process. Once an individual has withdrawn consent, you can no longer rely on that past consent for any future use or disclosure of the individual’s personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

An individual must have the capacity to consent. This means that the individual is capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. You can ordinarily presume that an individual has the capacity to consent, unless there is something to alert it otherwise; for example, the individual is a child or young person (see below). If an entity is uncertain as to whether an individual has capacity to consent at a particular time, it should not rely on any statement of consent given by the individual at that time.

Issues that could affect an individual’s capacity to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia
- limited understanding of English.

You should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent. If an individual does not have capacity to consent, even with support or the provision of additional resources such as an interpreter or alternative communication methods, and consent is required, an entity should consider who can act on the individual’s behalf. Options include:

- a guardian
- someone with an enduring power of attorney
- a person recognised by other relevant laws, for example in NSW, a “person responsible” under the *Guardianship Act 1987* (NSW) (this may be an individual’s spouse, partner, carer, family member or close friend)
- a person who has been nominated in writing by the individual while they were capable of giving consent.

An individual who lacks the capacity to consent should nevertheless be involved, as far as practicable, in any decision-making process. To the extent practicable in the circumstances, you should ensure that privacy issues are discussed with individuals who have impaired decision-making capacity in a way that is understandable and comprehensible.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves. If it is not practicable or reasonable for you to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

For further information refer to the following:

- OAIC's *Mobile privacy: a better practice guide for mobile app developer*[3] which has been developed by the OAIC to help mobile app developers embed better privacy practices in their products, including practical suggestions for obtaining meaningful consent on small screens.
- OAIC's *Australian Privacy Principles guideline*[4]*s* explains key concepts around compliance with the APPs, and includes more specific guidance for each APP and the obligations they place on organisations.
- OAIC's *Australian Privacy Principles guidelines* – Chapter 5: APP 5[5] explains more specifically the requirements for notifying individuals about the collection of their personal information. Complying with APP 5 will help to ensure the individual is informed about how and why their personal information is being collected and can subsequently provide meaningful consent to the collection of their personal information.

[3] https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/

[4] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/

[5] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information

Appendix E FAQs

The following text is provided for context for each app to ensure that the there are no conflicts in statements between the My Health Record and the app within the end-to-end consent flow. The text is included on screen 15 in Appendix B – Example consent flow.

What is My Health Record?

My Health Record contains your health information such as prescription medications and treatments you've had. It may also contain an overall summary of your health, vaccination information, advance care planning information and health-related notes that you or your healthcare provider have uploaded. Find out more about My Health Record https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record.

How the app manages and secures your personal information

There are multiple ways of accessing My Health Record. Each app has its own privacy policy and terms of use.

The app will access your personal information in My Health Record after you authenticate your identity through myGov. You will be required to provide your personal information during this authentication process. You will be asked to renew your authentication on a periodic basis.

The handling of your personal information is authorised under the My Health Records Act 2012 (Cth), the Healthcare Identifiers Act 2010 (Cth) and the Privacy Act 1988 (Cth). The app will manage and secure your personal information in accordance with its own privacy policy which will be made available to you via the app.

The app may collect and use technical information about your interactions with the app, including details about your device, device location, system, and application software. The information held and accessed by the app is described in the app's privacy policy.

To find out more about how your personal information is managed, please see the app's privacy policy and the My Health Record privacy policy Privacy policy | Australian Digital Health Agency

What happens if I delete the app later?

You may delete the app at any time. If you delete the app your device will no longer be able to access the My Health Record information. The information held and accessed by the app is described in the app's privacy policy.

Acronyms

Acronym	Description
API	application program interface
APP	Australian Privacy Principles
FHIR	Fast Healthcare Interoperability Resources
GO	Gateway Operator
MHR	My Health Record
NIO	National Infrastructure Operator
OAIC	Office of the Australian Information Commissioner
OAuth	Open Authorization

Glossary

Term	Meaning
Application Programming Interface (API)	An application programming interface (API) is a particular set of rules and specifications that software programs can follow to communicate with each other. It serves as an interface between different software programs and facilitates their interaction, similar to the way the user interface facilitates interaction between humans and computers.
application (app)	A type of application software that for the purposes of this document, can connect to the My Health Record APIs. The types of applications that can connect to the My Health Record APIs are: • **Mobile applications** are developed to run natively on a specific mobile device or platform (e.g. iOS, Android). • **Web applications** are powered by a web browser (e.g. Chrome, Firefox, Safari etc.) through the internet. Web applications are typically built using HTML, CSS and JavaScript and served through a mobile or desktop browser. Web applications can be built to look and feel just like a native application but will always runs through a visible browser. • **Hybrid applications** are usually coded in HTML, CSS and JavaScript. They are run through an invisible browser which has been packaged into a native application. This enables the application to have the look, feel and functionality of a native application. Hybrid applications allow developers to minimise development time as minimal work is required to target various mobile operating systems. An additional benefit of using a hybrid application framework includes allowing developers to access Native API calls which can be used to enable binary security mechanisms from the device itself. Hybrid applications can also be distributed through native application stores (allowing for additional vetting). • **Progressive web applications** can appear and behave as native applications on mobile devices, but do not require installation of the application on the device.
Gateway Operator (GO)	The Gateway Operator (GO) is the business area responsible for providing and managing the My Health Record system on behalf of the System Operator.
Healthcare Recipient	Healthcare recipient has the same meaning as in the My Health Records Act 2012 Cth).
My Health Record system	Has the same meaning as in the My Health Records Act 2012 (Cth).
National Infrastructure Operator (NIO)	The National Infrastructure Operator (NIO) is the business area responsible for providing and managing the My Health Record system on behalf of the System Operator.
Open Authorization	A framework to enable a third-party application to obtain limited access to an HTTP service. Also commonly used to implement login interactions.

Term	Meaning
Portal	An electronic interface that facilitates access to the System by Representatives and Registered Healthcare Recipients and has the functionality set out in the Portal Operator Registration Agreement (PORA)
Portal Operator Registration Agreement (PORA)	The conditions that the System Operator imposes on the registration of a Registered Portal Operator.
Privacy Act	Privacy Act means the Privacy Act 1988 (Cth).
Registered portal operator (RPO)	Registered Portal Operator means “registered portal operator”, as defined in the My Health Records Act 2012 (Cth).
Representative	Representative means a Nominated Representative or an Authorised Representative.
System Operator	System Operator has the same meaning as in the My Health Records Act 2012 (Cth).

References

[1] Office of the Australian Information Commissioner, “Australian Privacy Principles Guidelines - Privacy Act 1988,” 31 March 2015. [Online]. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles/.

[2] Australian Government, “The Privacy Act 1988,” [Online]. Available: https://www.legislation.gov.au/Series/C2004A03712.

[3] Australian Digital Health Agency, “My Health Record FHIR Gateway - Security Requirements and Guidelines v1.2,2022” Contact help@digitalhealth.gov.au to obtain this resource.