Australian Government
Australian Digital Health Agency

# My Health Record FHIR Gateway
# Consent Requirements and Guidelines

19 March 2020 v1.1

Approved for external use

Document ID: DH-3088:2020

**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**

**Council of Australian Governments**
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.

**Copyright © 2020 Australian Digital Health Agency**
This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

OFFICIAL

# Document information

## Key information

|  |  |  |
|---|---|---|
| **Owner** | General Manager, Privacy and Policy | |
| **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 |
|---|---|---|
| v1.0 | 19/03/2020 | Final version for release |

# Table of contents

**1 Introduction ........ 5**

- 1.1 Purpose ........ 5
- 1.2 Intended audience ........ 5
- 1.3 Scope ........ 5
- 1.4 Background ........ 5
- 1.5 Types of applications ........ 6
- 1.6 Requirement Keywords ........ 7

**2 Consent Requirements ........ 8**

**Appendix A Interaction Models ........ 21**

**Appendix B Example consent flow ........ 22**

**Appendix C Consent ........ 24**

**Appendix D FAQs ........ 27**

**Acronyms ........ 28**

**Glossary ........ 29**

**References ........ 30**

# 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).

## 1.2 Intended audience

The intended audience for this document is:

- mobile application developers
- registered portal operators
- the System Operator
- the National Infrastructure Operator (NIO).

For the purposes of this document, registered portal operators and mobile application developers using My Health Record APIs are collectively referred to as "developers".

## 1.3 Scope

These requirements are limited to consumer apps with view-only connections to 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 user's My Health Record is defined as sensitive in the *Privacy Act 1988* (Privacy Act), which means that under the *Australian Privacy Principles* (APPs) developers collecting such information must first obtain a user's informed consent. This is because users must make an informed decision 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* to provide a collection notice under Australian Privacy Principle 5 (APP 5), which lists the information that needs to be provided to individuals at the time of collection, including:

- Who is collecting their personal information?
- Why is their personal information being collected?
- How is their personal information used and disclosed?

- Who has access to their personal information, including whether their personal information is sent overseas?
- The legal authority with which their personal information is being collected, used and disclosed?

The My Health Record System Operator has provided requirements to support developers with their consent design. These requirements are not intended to prescribe specific designs which developers must replicate. Instead, each requirement supports a design intention which the developer can utilise as a basis for obtaining 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.

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.

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 1988 (Cth)* [2] (the Privacy Act) regardless of whether or not the app developer is already subject to the Privacy Act. Within the Privacy Act, there are some Australian Privacy Principles (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.
- APP 5 requires that app developers provide a collection notice at the time they are collecting personal information from users.
- APP 11 requires that app developers take reasonable steps to protect the security of the personal information they collect.

Guidelines on the APPs are published by the OAIC and are available online [1].

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 (using a fictitious “Healthy Living” app that has been user tested and demonstrated to support the gathering of informed consent from users). See Appendix B for an end-to-end example of the consent flow that has been user tested.

The System Operator reserves the right to defer or reject a developer’s access to the production environment if an app's design does not satisfy the requirements as stated in this document. The app developer is responsible for understanding their privacy obligations and ensuring the information provided to users is accurate and up-to-date.

*Table 1 - Requirement C001*

| **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. |

*Table 2 - Requirement C002*

| **Req. C002** | **Provide evidence that the flow achieves express and informed consent.** |
|---|---|
| **Description** | Apps **SHALL** demonstrate to the System Operator that users are:<br>• adequately informed about how their information accessed from the user's My Health Record is collected, used and disclosed; and<br>• requested to consent to the collection, use and disclosure of their information.<br>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 may have their access to the production environment deferred or rejected. |

*Table 3 - Requirement C003*

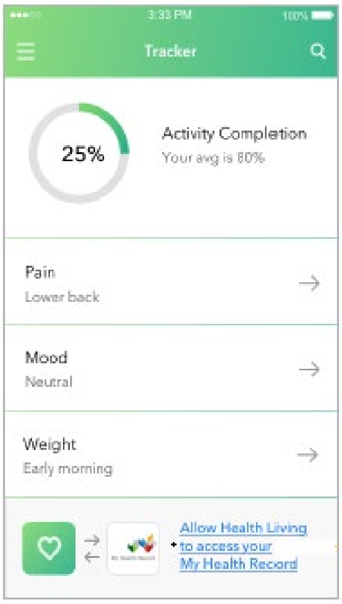
| **Req. C003** | **Initiating the process of linking an app to the My Health Record.** |
|---|---|
| **Description** | Apps **SHALL** have a process in place to initiate the linking of the app to the My Health Record. Suggested text is below:<br>*"Allow [app name] to access your My Health Record"*<br>The 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** |  <br>Allow Health Living to access your My Health Record |

*Table 4 - Requirement C004*

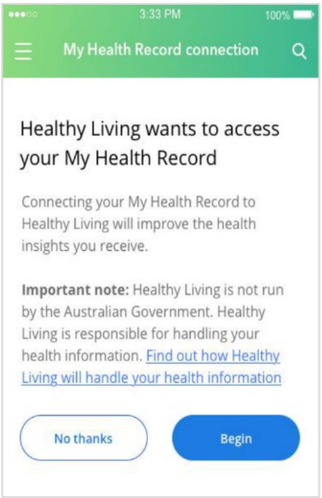
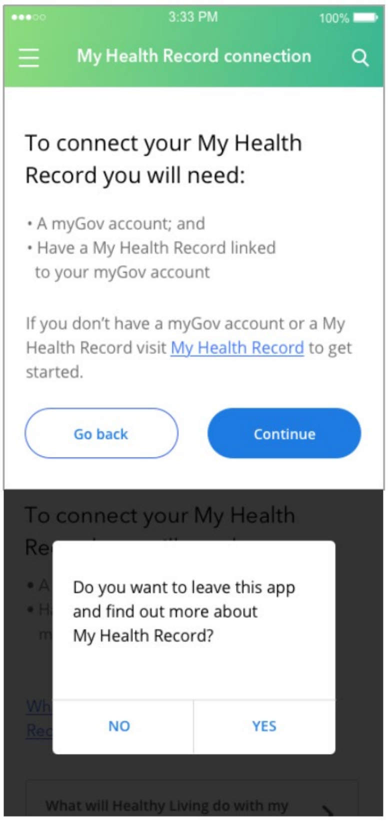
| **Req. C004** | **Introduce the My Health Record.** |
|---|---|
| **Description** | Early in the consent flow the developer **SHALL** include the following statement:<br>*Important note: [app name] is not run by the Australian Government. [app name] is responsible for handling your health information. Find out how [app name] will handle your health information.*<br>Applications **SHOULD** provide a brief introduction to the My Health Record (see Req C007).<br>Apps **SHALL** explain why they want access to a user's My Health Record and provide a link 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.<br>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.<br>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.<br>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** |  <br>Healthy Living wants to access your My Health Record<br>Connecting your My Health Record to Healthy Living will improve the health insights you receive.<br>**Important note:** Healthy Living is not run by the Australian Government. Healthy Living is responsible for handling your health information. Find out how Healthy Living will handle your health information |

*Table 5 - Requirement C005*

| **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.<br>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:<br>*If you don't have a myGov account or a My Health Record visit My Health Record to get started.*[1]<br>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.<br>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** | <br>To connect your My Health Record you will need:<br>• A myGov account; and<br>• Have a My Health Record linked to your myGov account<br>If you don't have a myGov account or a My Health Record visit My Health Record to get started.<br>Do you want to leave this app and find out more about My Health Record?<br> |

---

[1] Hyperlink to: https://www.myhealthrecord.gov.au/for-you-your-family/howtos/register-for-my-health-record

*Table 6 - Requirement C006*

| **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:<br>• what information the app will access from the My Health Record<br>• the specific intended uses of the user's My Health Record information<br>• any other information as required by the Privacy Act and APP 5.<br>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).<br>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.<br>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.<br>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.<br>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.<br>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.<br>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. |

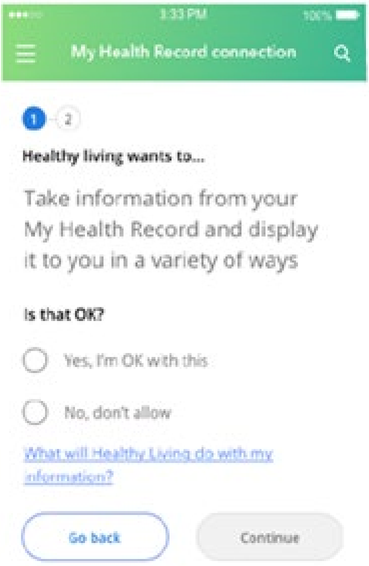
| **Req. C006** | **Gaining express and informed consent for the app to access a user's My Health Record.** |
|---|---|
| **Reference screens** | <br> <br>Healthy living wants to...<br>Take information from your My Health Record and display it to you in a variety of ways<br>Is that OK?<br>○ Yes, I'm OK with this<br>○ No, don't allow<br>What will Healthy Living do with my information?<br> <br>**NOTE:** See Appendix B Example consent flow for an expanded set of the above screens. |

*Table 7 - Requirement C007*

| **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.<br>• *What is the My Health Record?*<br>[For this first question, apps **SHALL** provide the following answer]<br>*The My Health Record system is a national digital health record system, managed by the Australian Government.*<br>*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, with your consent, 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.*<br>*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.*<br>*If you are unsure if you have a My Health Record, please visit www.myhealthrecord.gov.au for more information.*<br>• *Why does [app name] want access to My Health Record?*<br>• *What health information will [app name] download from the My Health Record?*<br>• *Will [app name] share my health information?*<br>• *Is my personal information safe?*<br>• *Is [app name] compliant with Australian privacy laws?*<br>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.<br>More information on having an APP compliant Privacy Policy is available in the OAIC's *Australian Privacy Principles Guidelines* [1]. |

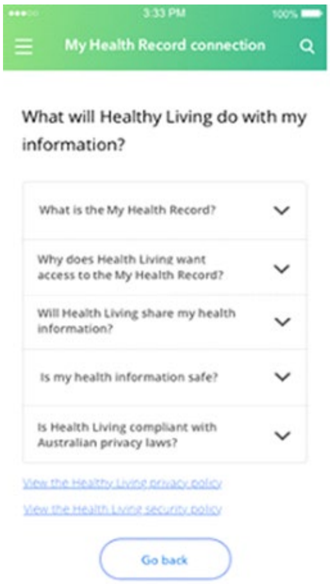
| **Req. C007** | **Detailed consent information.** |
|---|---|
| **Reference screens** | <br>My Health Record connection<br>What will Healthy Living do with my information?<br>What is the My Health Record?<br>Why does Health Living want access to the My Health Record?<br>Will Health Living share my health information?<br>Is my health information safe?<br>Is Health Living compliant with Australian privacy laws?<br>View the Healthy Living privacy policy<br>View the Health Living security policy<br> |

*Table 8 - Requirement C008*

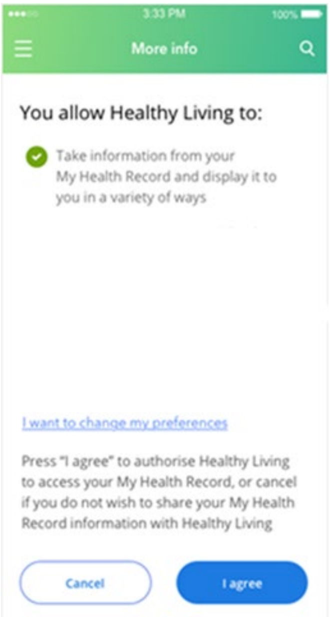
| **Req. C008** | **Consent summary.** |
|---|---|
| **Description** | Apps **SHOULD** clearly summarise what the user has agreed to when providing consent for an app to access their My Health Record.<br>The user **SHALL** be asked to agree to the use of their My Health Record information after the user 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:<br>*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].*<br>The user **SHOULD** also 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. |
| **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** | <br>You allow Healthy Living to:<br>✓ Take information from your My Health Record and display it to you in a variety of ways<br>I want to change my preferences<br>Press "I agree" to authorise Healthy Living to access your My Health Record, or cancel if you do not wish to share your My Health Record information with Healthy Living<br> |

*Table 9 - Requirement C009*

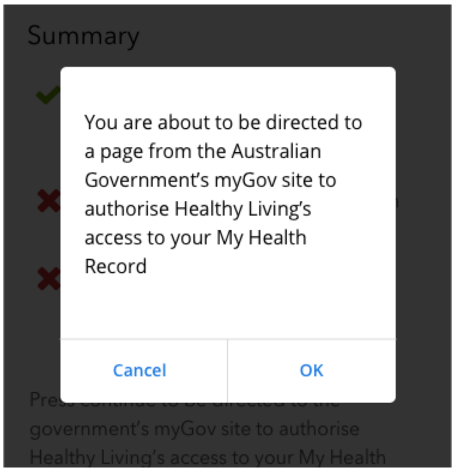
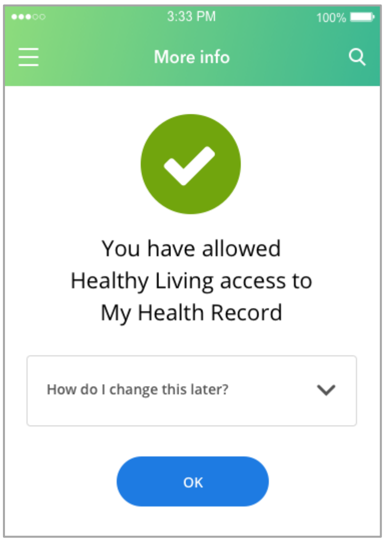
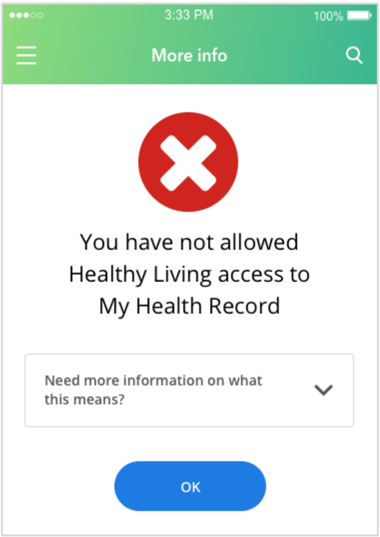
| **Req. C009** | **Prompt users prior to being directed to the myGov site.** |
|---|---|
| **Description** | Apps **SHALL** provide a statement that indicates the app will direct the user to the Australian Government's myGov site to authorise the app's access to their My Health Record. |
| **Additional 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** |  <br>You are about to be directed to a page from the Australian Government's myGov site to authorise Healthy Living's access to your My Health Record<br>Pres<br>government's myGov site to authorise Healthy Living's access to your My Health |

*Table 10 - Requirement C010*

| **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.<br>Input information required from apps includes:<br>1 the app logo - PNG format and 64 x 64 pixels in colour<br>2 the exact name of the app as it should be referred to on the consent screen.<br>For content that the My Health Record will include under each of the FAQs see Appendix D. |
| **Reference screen**<br>(Note: This screen is hosted by the My Health Record system) | <br><APP> is seeking your permission to access your My Health Record<br> |

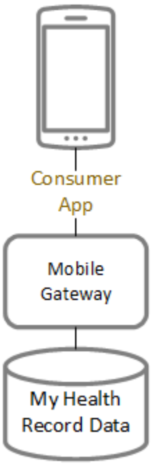
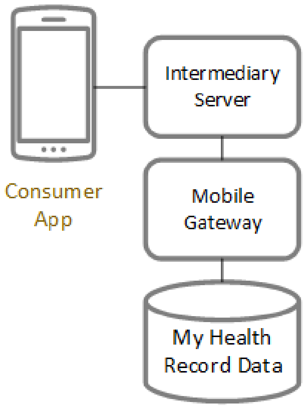
*Table 11 - Requirement C011*

| **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.<br>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.<br>If the user has withheld access, then the app **SHALL** provide guidance on the outcomes of withholding consent. |
| **Additional information** | User expect that – after completing this process – they will receive feedback as to whether it has been successful or not. |
| **Reference screens** | <br> <br>You have allowed Healthy Living access to My Health Record<br><br> <br>You have not allowed Healthy Living access to My Health Record |

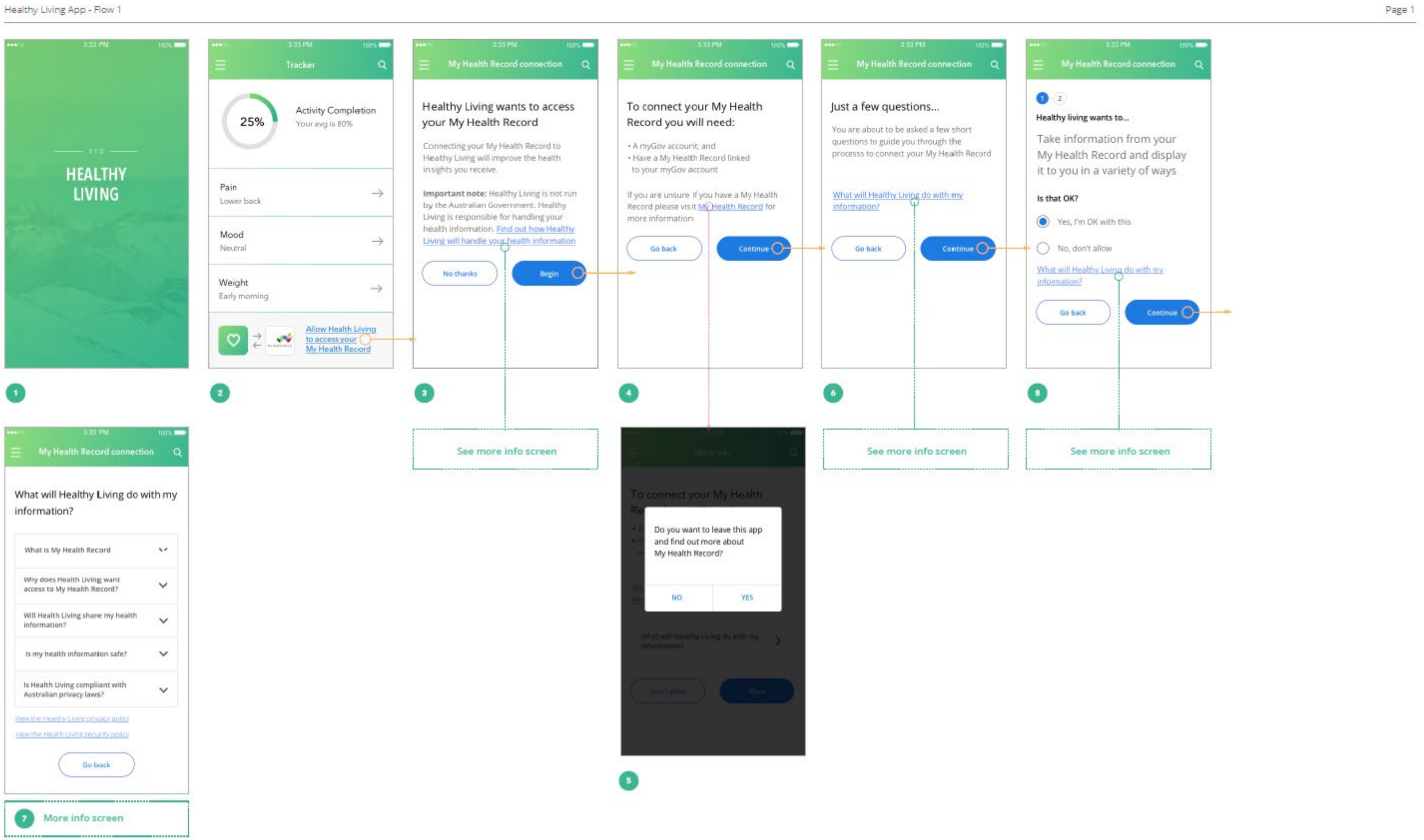
# Appendix A Interaction Models

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.

*Table 12 - Current interaction models*

| **Interaction model** | **Description** |
|---|---|
| #1 Consumer / Self-Care  | Consumer mobile app connects with the My Health Record system via the FHIR® gateway. |
| #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).<br>**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



**Screen 3**

Healthy Living wants to access your My Health Record

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

**Important note:** Healthy Living is not run by the Australian Government. Healthy Living is responsible for handling your health information. Find out how Healthy Living will handle your health information

**Screen 4**

To connect your My Health Record you will need:

- A myGov account; and
- Have a My Health Record linked to your myGov account

If you are unsure if you have a My Health Record please visit My Health Record for more information

**Screen 5**

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

**Screen 6**

Just a few questions...

You are about to be asked a few short questions to guide you through the processs to connect your My Health Record

What will Healthy Living do with my information?

**Screen 7**

What will Healthy Living do with my information?

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

View the Healthy Living privacy policy

View the Health Living security policy

**Screen 8**

1 2

**Healthy living wants to...**

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

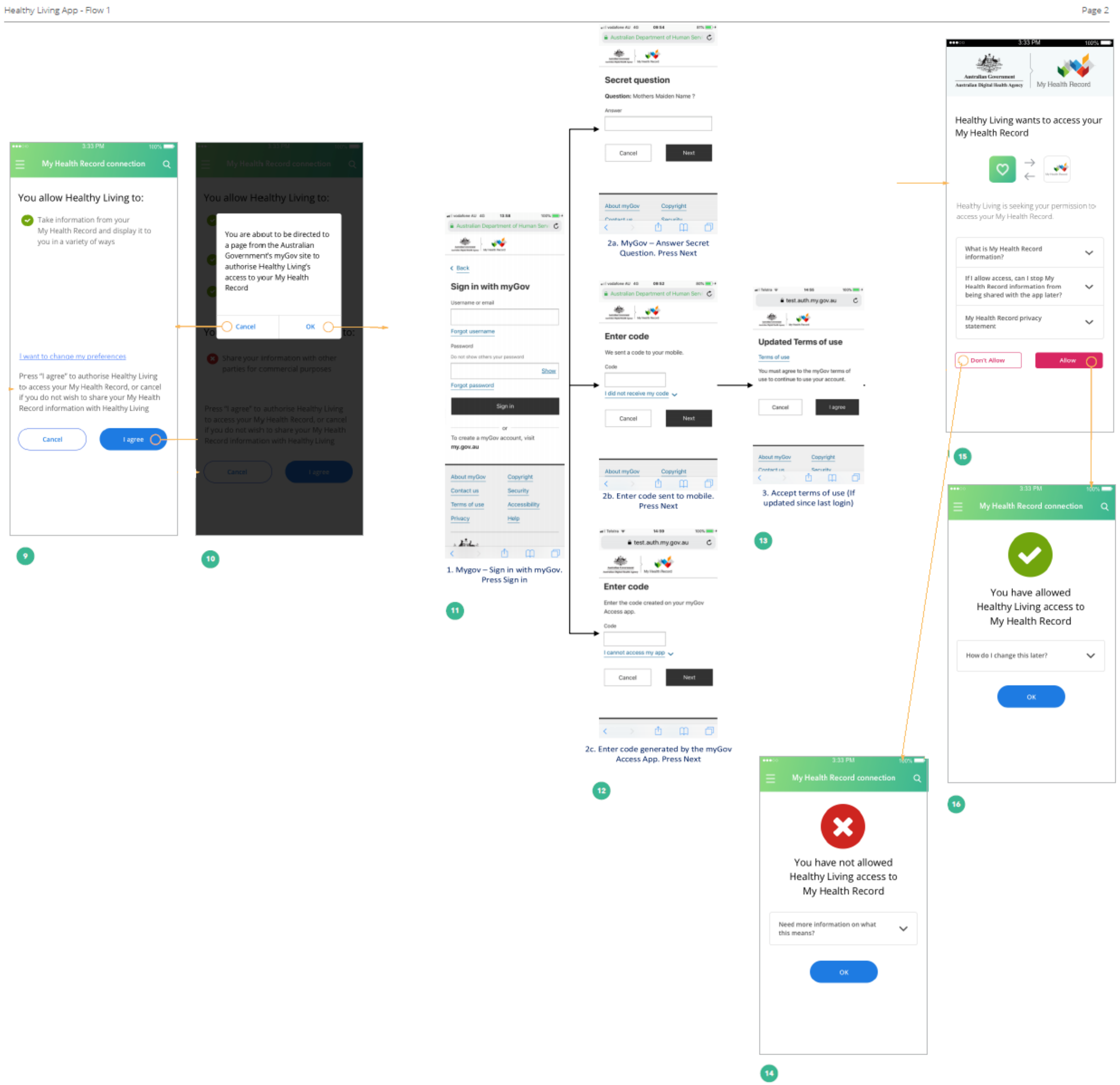
**Is that OK?**

● Yes, I'm OK with this

○ No, don't allow

What will Healthy Living do with my information?

*Figure 1: Example flow – page 1*



You allow Healthy Living to:

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

Press "I agree" to authorise Healthy Living to access your My Health Record, or cancel if you do not wish to share your My Health Record information with Healthy Living

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

Share your information with other parties for commercial purposes

Sign in with myGov

To create a myGov account, visit my.gov.au

1. Mygov – Sign in with myGov. Press Sign in

Secret question

Question: Mothers Maiden Name ?

2a. MyGov – Answer Secret Question. Press Next

Enter code

We sent a code to your mobile.

2b. Enter code sent to mobile. Press Next

Enter code

Enter the code created on your myGov Access app.

2c. Enter code generated by the myGov Access App. Press Next

Updated Terms of use

You must agree to the myGov terms of use to continue to use your account.

3. Accept terms of use (If updated since last login)

Healthy Living wants to access your My Health Record

Healthy Living is seeking your permission to access your My Health Record.

What is My Health Record information?

If I allow access, can I stop My Health Record information from being shared with the app later?

My Health Record privacy statement

You have allowed Healthy Living access to My Health Record

You have not allowed Healthy Living access to My Health Record

*Figure 2: Example flow – page 2*

# Appendix C 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.

You 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 developers*[2] 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 guidelines*[3] 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[4] 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.

---

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

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

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

# Appendix D 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 information?**

My Health Record contains your health information, such as prescription medications and treatments you have received. It may also contain an overall summary of your health, advance care planning information, and health-related notes that you or your healthcare provider have uploaded. For more details go to http://myhealthrecord.gov.au.

**If I allow access, can I stop My Health Record information being shared with the app later?**

Deleting the app from your device or cancelling your account may not stop the service accessing your information in the My Health Record system. If you want to stop access, go to myhealthrecord.gov.au, sign into your My Health Record and go to the access control screen to cancel the service's access. Alternatively, call the My Health Record Help Line 1800 723 471 and we'll help you cancel access. Even if you cancel access in one of these ways, your information may still be stored by the service supplier or third parties to whom the supplier has disclosed your information; check out the supplier's privacy policy for further details.

**Where do I go to find out more about My Health Record?**

Please read our Privacy Policy at https://www.myhealthrecord.gov.au/about/privacy-policy and our Frequently asked questions pages at https://www.myhealthrecord.gov.au/for-you-your-family/howtos/frequently-asked-questions for more information about My Health Record.

# Acronyms

| Acronym | Description |
|---|---|
| API | application program interface |
| APP | Australian Privacy Principles |
| FHIR | Fast Healthcare Interoperability Resources |
| NIO | National Infrastructure Operator |
| OAIC | Office of the Australian Information Commissioner |
| OAuth | Open Authorization |

# Glossary

| Term | Meaning |
|---|---|
| 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. |

# 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 - Security Requirements and Guidelines v1.1,” Contact help@digitalhealth.gov.au to obtain this resource. , 2020.