Australian Government
Australian Digital Health Agency

My Health Record
Managing Your App in Production

20 February 2023 v2.9

Approved for external use

Document ID: DH-3711:2023

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

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

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	Director Operational Performance
Date of next review	10 October 2023
Contact for enquiries	Australian Digital Health Agency Help Centre Phone 1300 901 001 Email help@digitalhealth.gov.au

Table of contents

1 Introduction

1.1 Purpose

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

For the purposes of this document:

- Registered portal operators are referred to as “developers”
- The Agency is referred to as the System Operator (SO) for the purposes of the *My Health Record Act 2012* (Cth).
- References to “Consumer” 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 (app) which includes mobile application (app) developers.

1.3 Scope

This document covers the responsibilities of developers that have an app that connects to the My Health Record system in production, including incident management and performing app changes and upgrades.

2 Incident management

2.1 Incidents

An incident is a planned or unplanned event or occurrence that causes an interruption or reduction in the quality of the app. For example, installation, function, certification, connection, and infrastructure issues. Such issues may result in data loss, corruption, or unauthorised access during transfer to and from the My Health Record system.

Certain incidents need to be reported to the System Operator; these are outlined in the *Incident type* section.

2.2 Responsibilities

Developers play a key role in the identification, diagnosis and resolution of incidents. Your obligations are set out in the following:

- *My Health Records Act 2012* [MHRA2012]
- *My Health Records Regulation 2012* [MHRR2012]
- *My Health Records Rule 2016* [MHRR2016]
- *Privacy Act 1988* [PA1988]
- *Consent Requirements and Guidelines*
- *Operations Requirements and Guidelines*
- *Portal Operation Registration Agreement* [PORA]
- *Presentation Requirements and Guidelines*
- *Security Requirements and Guidelines*

Developers are required to assist the System Operator by doing things such as:

- reporting incidents, including developer app incidents, to the System Operator within two business days of their identification (refer to Contact details)
- undertaking or assisting in investigations to identify the root cause of an incident and, if required, implementing a technical solution to fix it
- ensuring that developer app incidents are contained and, where an immediate resolution is not possible, that an appropriate workaround is identified and implemented
- providing and maintaining up-to-date contact details of relevant help desks, incident coordinators/managers, or other individuals (such as technical or security specialists) involved in the incident management process to the System Operator
- communicating with customers (in consultation with the System Operator) about the details of any problems and their resolution
- implementing, at the developer's own cost, any remediation actions within the agreed timeframes for any incident
- providing the System Operator with information required to inform post-incident review reports, post-resolution
- protecting the confidentiality of personal and health information held in the My Health Record system
- notifying the System Operator when there are changes or upgrades to the app as per notification obligations. Refer to App changes and upgrades for more information.

The System Operator will:

- work cooperatively with developers in resolving developer app incidents and problems
- transition, where appropriate, unresolved developer incidents to the System Operator's incident management process for further diagnosis and resolution
- communicate with developers through Services Australia's Developer Support team or the My Health Record website about system releases, relevant planned changes to the My Health Record system, changes to requirements, and details of planned and unplanned outages.

2.3 Contact details

2.3.1 Incidents

Developers must report incidents, including developer app incidents or problems within two business days of their identification to the System Operator via the following support contacts:

- business hours: Digital Health Agency Help Centre - 1300 901 001 or help@digitalhealth.gov.au
- after hours: My Health Record Help Line - 1800 723 471 (select option 2 and please make it clear that the incident relates to a My Health Record connection).

2.3.2 Planned outages

Developers must report planned outages for their app at least three days prior to the outage to the Help Centre at help@digitalhealth.gov.au. This information will be used by the My Health Record Help Line to inform users who call regarding the app not being available.

Note: Any other reported issues from users about an app will be referred back to the developer's support channels.

2.4 Incident management governance

2.4.1 Developer incident management requirements

To access the My Health Record system's production environment, an incident management processes must be in place to identify, log, analyse, and resolve incidents as they occur and to minimise the possibility of a re-occurrence.

2.4.2 Incident types

Table 1 describes the incident types that must be escalated to the System Operator for resolution and/or consultation.

Initial triage will be performed by the System Operator before escalation to the appropriate functional area.

Table 1 - Incident Types

Type of incident	Description	Scenario examples
System	An unplanned interruption or degradation to the My Health Record system's operations which results in a reduction or loss of system functionality.	• An Application Programming Interface (API) is not responding.
Security	A data breach of the My Health Record system's security measures resulting in a threat to the integrity, availability, or confidentiality of the My Health Record system. This type of event could also have compliance and privacy implications	• The developer's app is hacked and redirects to a 'clone' site to capture usernames/passwords. • The developer's app is hacked and/or a vulnerability is exploited that affects multiple consumers. • A coordinated denial of service attack is identified. • Identifiable healthcare or personal data are exposed. • A developer's app is infected with malware and starts leaking data to a malicious user. • An access token (OAuth) is stolen. • The private keys to a Gatekeeper digital certificate are stolen or compromised. • The App ID and Secret Key are compromised. • Secure communications between a developer's app and the My Health Record system is compromised. • A consumer identifies that an unrecognised person has accessed their record.
Clinical safety	An event or circumstance that resulted, or could have resulted, in unintended or unnecessary harm to a person.	• Consumers or healthcare providers advise health information displayed in their app is incorrect, incomplete or misleading.
Regulatory incident/breach	An identified breach of My Health Record policy, rules, regulations or legislation. This type of event may also have security and privacy implications	• A person overrides a healthcare recipient's access controls and views a clinical record without having grounds to do so.

Type of incident	Description	Scenario examples
Privacy	My Health Record consumers have had their personal information collected, shared, stored, or used in an unauthorised way.	• A consumer identifies an unrecognised person or organisation in the access history of their My Health Record. • Medical information in a healthcare recipient's My Health Record is discussed widely by a developer's staff without the consumer's consent. • Not all attached documents are successfully shared when the consumer attempts to use the in-app share function to share multiple attached documents. • The developer's app retains MHR system data for a period greater than 28 days. • Unauthorised access by another consumer.
Fraud	Identified or potential deception intended to result in financial or personal gain. This type of event may also have security and privacy implications.	• A developer captures clinical data in transit and provides the de-identified data to a medical research company. • A developer's system administrator with access to the system sells the IHIs, or other uniquely identifiable data such as HPI-O, and personally identifiable information such as names and dates of birth, of several high-profile individuals. • A developer's system administrator with access to the system gathers individual's information from the My Health Record system to enable them to access services or payments.
Developer app	Any issues with the functions or performance in the app.	• Trouble accessing or viewing information, incorrect information or missing information in the app. • Trouble acquisitioning or downloading the relevant app.

3 App changes and upgrades

This section describes developer obligations when connecting a new or revised version of an app to the My Health Record system.

3.1 App ID authentication

All apps granted My Health Record production environment access for the first time will be provisioned with an Application ID (App ID) and Application Secret Access Key (Secret Key). The App ID and Secret Key are both used by the app as part of authentication and authorisation to the My Health Record system. An app with My Health Record production environment access that has a significant update will be required to obtain a new App ID and Secret Key.

If developers produce the same app for multiple platforms (e.g. Android and iOS), each platform version will need to be provisioned with a separate App ID and Secret Key. Notice of Connection (NOC) testing must be completed and conformance and compliance declared for each platform version. For further information on NOC testing and conformance requirements refer to NOC testing and conformance requirements.

To facilitate access to the APIs utilised to access the My Health Record system, the following fields must be populated in the app's request header:

- *App ID* – the unique identifier assigned to the app
- *App Version* – the app release version specified by the developer in the *Production Environment Access Request* form.

3.2 Production access after an app change or upgrade

The following types of changes will require a developer to formally notify the System Operator:

- significant interaction or transaction changes
- administrative changes.

3.2.1 Significant interaction or transaction changes

A significant change is one which:

- changes the way the app interacts with the My Health Record system, and/or
- has any technical, clinical, security or privacy impacts.

If developers make a significant change to an app connected to the My Health Record production environment, they must advise the Help Centre at help@digitalhealth.gov.au of proposed changes.

For information on the impacts of certain changes, refer to Examples of software changes and upgrades.

3.2.2 Administrative changes

In the event of a significant administrative change, developers must email the Help Centre at help@digitalhealth.gov.au using the subject line of "Developer administrative change", and include the confirmed details of the change/s for the Agency's consideration under the Portal Operator Registration Agreement. All significant administrative changes must be provided within two business days after the developer becomes aware of the change. Significant administrative changes include:

- change to the developer's business, legal, or support structure
- change in app name
- cancellation of the appointment of an Operator Officer (noting that a developer must have at least one and up to a maximum of three Operator Officers)
- change in professional or business details of an appointed Operator Officer
- appointment of a new Operator Officer (requires completion of a *Portal Operator Registration Form*).

3.3 Examples of software changes and upgrades

Table 2 outlines examples of app changes and upgrades and the developer NOC testing and conformance declaration actions required.

Table 2 - Examples of software changes and upgrades

Description of change	NOC test required?	PEAR form required?	New App ID required?
Change to the purpose of the app. (e.g. the purpose of an app changes from being used to only display My Health Record data to transforming the My Health Record data using decision support mechanisms)	Yes, a subset of test cases apply to validate new functionality.	Yes	No

Description of change	NOC test required?	PEAR form required?	New App ID required?
Changes that impact the app's conformance with the mandatory requirements to which the app has declared conformance to, or the developer's compliance with the signed contract. (e.g. a developer installs a new security system that changes its ability to meet the mandatory security conformance requirements)	Yes, a subset of test cases apply to validate new functionality.	Yes	No

Description of change	NOC test required?	PEAR form required?	New App ID required?
Developer produces another iteration of their app that is designed to run on another platform	Yes, all test cases apply.	Yes	Yes
Change to app functionality, utilising an additional My Health Record API (e.g. currently using Get PBS Items, then adds Get MBS Items).	Yes, a subset of test cases apply to validate new functionality.	Yes	Yes

Description of change	NOC test required?	PEAR form required?	New App ID required?
Change to the use of an existing API (e.g. using Get Document to access allergies, but later requires use of Get Document to also access pathology)	No	Yes	No
Change to upgrade to an updated API	Yes, a subset of test cases apply to validate new functionality.	Yes	Yes
Change to app functionality and no longer requires use of an API (e.g. no longer has a need for MBS data)	No	No	No

Description of change	NOC test required?	PEAR form required?	New App ID required?
Change to the Interaction Model utilised (e.g. a developer introduces an intermediary server or end server)	Yes, all test cases apply.	Yes	Yes
A code change to address a problem or incident reported by the System Operator	Change needs to be assessed to determine required actions.	Yes	No
Developer makes a change to conform to changes in mandatory conformance requirements	Change needs to be assessed to determine required actions.	Yes	No – as long as the changes do not result in a change to the way the app interacts with the My Health Record system (see below)

Description of change	NOC test required?	PEAR form required?	New App ID required?
Developer releases a major app version – involves changes to the way the app interacts with the My Health Record system (including the way it consumes APIs)	Yes, all test cases apply.	Yes	Yes
Change to the way personal information is communicated, handled or disclosed	No	Yes	No

Description of change	NOC test required?	PEAR form required?	New App ID required?
Developer makes a change to the version number of their app	Formal NOC not required as it is considered a minor update. However, a test transaction in SVT is required.	No	No
Developer builds a new in-app feature such as 'Share' (complying with the Agency's interoperability requirements).	NOC is not required as it is an in-app feature, however app developers may need to perform self-assessment to validate new functionality	Yes	No

3.4 NOC testing and conformance requirements

To satisfy NOC and conformance requirements, developers must do the following:

1. Perform self-assessment testing of the changed or upgraded app functionality using either existing or new test cases and test data in the My Health Record SVT environment.
2. Submit the self-assessment test evidence for assessment.
3. Attend a virtual session with the My Health Record Software Vendor Test team to test the connectivity of the app with the My Health Record system, demonstrating that the app is functioning according to the API specifications.
4. Update and re-submit a *Production Environment Access Request Form* to the System Operator, including:
    - providing details of the app change or upgrade, inclusive of all existing functionality and
    - declaring conformance to all mandatory My Health Record requirements relating to the functionality being delivered.

Once the above steps have been successfully completed, the System Operator will issue a production environment access letter, acknowledging that the updated app has been approved and granted access for specific transactions with the My Health Record system.

3.5 Insignificant interaction changes

An insignificant app change that does ***not*** change the way the app interacts with the My Health Record system and does ***not*** have any technical, clinical, security or privacy impacts. It can include: a graphical user interface change; an app logo change; or a self-contained change, such as a localised bug fix to keep the app operational.

If an insignificant change is made to an app, developers should:

1. regression test the app in the My Health Record SVT environment.
2. continue to transact with the My Health Record system utilising the App ID and App Version previously provisioned to access the My Health Record system.

3.6 System Operator-initiated changes

The System Operator may introduce new mandatory requirements, withdraw support for previous versions for the API, or make changes to API or OAuth specifications. The System Operator will consult with affected developers about any such changes.

To respond to System Operator-initiated changes, developers are required to:

- maintain the ability to prevent users from logging on until updates to the latest version of the app are completed
- keep the app up-to-date with the new or updated specifications.

Failure to do the above may result in the app no longer having access to the My Health Record system.

3.7 Support for software changes or upgrades

To check if an app change requires NOC testing and a conformance declaration, email the Help Centre at help@digitalhealth.gov.au using the subject line: *Developer app change* and include the following information:

- app details (developer's name, contact details and app name)
- new version number (if applicable)
- proposed functionality change/s to the app
- proposed release date.

3.8 More information

The My Health Record Operational Performance team manages the day-to-day operational activities of the My Health Record system. For more information or assistance, please email: myhealthrecord.operations@digitalhealth.gov.au.

See also: http://www.myhealthrecord.gov.au.

Acronyms

Acronym	Description
API	application programming interface
FHIR	Fast Healthcare Interoperability Resources
GO	Gateway Operator
HPI-O	Healthcare Provider Identifier – Organisation
IHI	Individual Healthcare Identifier
MBS	Medicare Benefits Schedule
NIO	National Infrastructure Operator
NOC	Notice of Connection
OTS	Online Technical Support
PBS	Pharmaceutical Benefits Scheme
RPO	Registered Portal Operator
SVT	Software Vendor Test Environment

Glossary

Term	Description
application programming interface	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	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)
Healthcare Provider Identifier – Organisation (HPI-O)	A unique 16-digit number used to identify organisations which deliver healthcare in the Australian healthcare setting.
Individual Healthcare Identifier (IHI)	A 16-digit unique number used to identify individuals who receive or may receive healthcare in the Australian health system.

Term	Description
Interoperability requirements	Interoperability requirements means the requirements published by the System Operator from time to time specifying the technical and compliance prerequisites that entities must meet in order to connect and remain connected to the System: • Operations Requirements and Guidelines • Consent Requirements and Guidelines • Security Requirements and Guidelines • Presentation Requirements and Guidelines.
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.
Notice of Connection	A notice issued by the My Health Record System Operator indicating that a system is ready to connect to the My Health Record system. NOC testing is the process of testing an app using test cases and test data provided by the System Operator. Tests are executed in the My Health Record Software Vendor Test (SVT) environment and are verified by the (GO).
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)
Operator Officer	Operator Officer has the same meaning as in the My Health Records Rule 2016.
Portal Operator Registration Agreement (PORA)	The conditions that the System Operator imposes on the registration of a Registered Portal Operator.
Registered Portal Operator	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.
Software Vendor Test Environment	The My Health Record system test environment managed by the Gateway Operator (GO) to facilitate functional and integration testing of developer apps in order to obtain a Notice of Connection (NOC).
System Operator	System Operator has the same meaning as in the My Health Records Act 2012 (Cth).

References

Australian Digital Health Agency, *My Health Record - Consent Requirements and Guidelines V1.2*,

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3702-2023/dh-3705-2023

[MHRA2012] Australian Government, *My Health Records Act 2012*, https://www.legislation.gov.au/Details/C2015C00602/Html/Text

[MHRPOPE] Australian Digital Health Agency, *My Health Record - Portal Operator Production Environment Access Request Form*, available by emailing help@digitalhealth.gov.au

[MHRR2012] Australian Government, *My Health Records Regulation 2012*, https://www.legislation.gov.au/Details/F2016C00093

[MHRR2016] Australian Government, *My Health Records Rule 2016*, https://www.legislation.gov.au/Details/F2016L00095

Australian Digital Health Agency, *My Health Record FHIR Gateway - Operations Requirements and Guidelines v1.2*

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3702-2023/dh-3704-2023

[PA1988] Australian Government, *Privacy Act 1988*, https://www.legislation.gov.au/Details/C2020C00025

[PORA] Australian Digital Health Agency, *Portal Operation Registration Agreement*, available by emailing help@digitalhealth.gov.au

Australian Digital Health Agency, *My Health Record FHIR Gateway - Presentation Requirements and Guidelines v1.2*,

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3702-2023/dh-3707-2023

Australian Digital Health Agency, *My Health Record - Security Requirements and Guidelines v1.2*,

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3702-2023/dh-3706-2023

Additional reading

My Health Record FHIR Gateway - API Specification v2.2

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3667-2022/dh-3669-2022

My Health Record FHIR Gateway - Release Note v2.2

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3667-2022/dh-3668-2022

My Health Record FHIR Gateway - Error Mapping v2.2

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3667-2022/dh-3671-2022

My Health Record FHIR Gateway - Data Mapping v2.2

https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3667-2022/dh-3670-2022