



## My Health Record FHIR Gateway Security Requirements and Guidelines

20 February 2023 v1.2

Approved for external use

Document ID: DH-3706:2023

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

---

## **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 © 2023 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** Product Owner, Mobile

**Contact for enquiries** Australian Digital Health Agency Help Centre

Phone [1300 901 001](tel:1300901001)

Email [help@digitalhealth.gov.au](mailto:help@digitalhealth.gov.au)

### Product or document version history

---

Product or document version	Date	Release comments
v1.1	13/03/2020	Final for release
V1.2	20/02/2023	Final for release

---

## Table of contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
1.1	Purpose .....	5
	For the Purposes of this document:.....	5
1.2	Intended audience.....	5
1.3	Scope .....	5
1.4	Overview .....	6
1.5	Applicability of interaction models.....	6
1.6	Reviews of requirements and guidelines.....	7
1.7	Requirement keywords .....	7
1.8	Using this document.....	8
<b>2</b>	<b>Information security governance .....</b>	<b>10</b>
2.1	Mandatory requirements .....	10
2.2	Recommended guidelines .....	18
<b>3</b>	<b>Physical security.....</b>	<b>20</b>
3.1	Mandatory requirements .....	20
<b>4</b>	<b>Personnel security.....</b>	<b>22</b>
4.1	Mandatory requirements .....	22
4.2	Recommended guidelines .....	24
<b>5</b>	<b>Information technology security .....</b>	<b>25</b>
5.1	Mandatory requirements .....	25
5.2	Recommended guidelines .....	41
<b>Appendix A</b>	<b>Interaction models.....</b>	<b>45</b>
	<b>Acronyms.....</b>	<b>46</b>
	<b>Glossary.....</b>	<b>47</b>
	<b>References .....</b>	<b>49</b>

# 1 Introduction

## 1.1 Purpose

This document specifies the mandatory security requirements and recommended security 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).

The mandatory security requirements and recommended guidelines in this document describe the minimum baseline required to connect to the My Health Record system through its FHIR® gateway. Developers need to consider the security threats and risks applicable to their specific app solution, and the relevant mitigating controls to be implemented in order to protect all stakeholders (including healthcare recipients, providers, developers, and the System Operator). This document also specifies the security requirements regarding relevant technical assets (including mobile apps, web apps, hybrid apps, intermediary servers, end servers, and any other information systems, hardware, and software involved in the developer's app solution, the System Operator's systems, and consumers' systems and devices) and information assets (including the personal information, healthcare information, credentials, tokens, cryptographic keys, app ID and secret key, API specs, and other technical information).

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 “User” may 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 (including mobile application developers), and
- the System Operator (which includes the National Infrastructure Operator and the Gateway Operator)

## 1.3 Scope

As noted above, this document only addresses the requirements and guidelines for consumer apps using interaction models #1 and #4. It will be updated in the future to encompass further interaction models.

Moreover, this document does not address 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 and specifications and submission of specific B2B web-services forms. Information about connecting to the B2B web-services can be obtained from the My Health Record Operations team via [help@digitalhealth.gov.au](mailto:help@digitalhealth.gov.au).

## 1.4 Overview

The following types of apps can connect to the My Health Record FHIR® gateway 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 like a native application but will always run through a visible web 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.

If not stated otherwise, the term “app” in this document refers to all four types of application. Moreover, where an app connects to the My Health Record FHIR® gateway using an intermediary system (e.g. server), this system is to be treated as being part of the app.

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 its target audience will determine the model for interacting with the My Health Record system. For example, an app may connect directly to 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.

## 1.5 Applicability of interaction models

The models defined in Appendix A specify the interactions between an app and the My Health Record system. The requirements and guidelines detailed in this document are applicable to specific interaction models. The developers should only choose one of the interaction models listed in Appendix A. The System Operator may stipulate modifications or impose specific requirements on the listed interaction models.

## 1.6 Reviews of requirements and guidelines

To manage emerging threats and risks effectively, it is critical to continuously monitor and improve the security of digital health systems. The SO will regularly review the requirements and guidelines in this document and may revise them.

The requirements must comply with Australian Government law, standards, guidelines, and frameworks, including but not limited to:

- the *My Health Record Act 2012* [1]
- the *Privacy Act 1988* (Cth), including the *Australian Privacy Principles* (APPs) [2]
- the Notifiable Data Breach scheme (NDB) [3]
- the *Protective Security Policy Framework* (PSPF) [4]
- the *Australian Government Information Security Manual* (ISM) [5].

Appropriate requirements should also comply with international government standards, guidelines, frameworks, and regulations, including but not limited to:

- the *General Data Protection Regulation* (GDPR) (EU) [6]
- the *Health Insurance Portability and Accountability Act 1996* (HIPAA) (USA) [7]
- the *Personal Information Protection and Electronic Documents Act 2000* (PIPEDA) (Canada) [8].

When the System Operator publishes updated requirements, it is the developer's responsibility to maintain conformance with the latest requirements. Developers will be informed of any amendments to this document. Alternatively, developers can refer to the published requirements and guidelines available.

## 1.7 Requirement keywords

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

---

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

---

## 1.8 Using this document

The requirements and guidelines in this document are grouped into four high-level topics:

- information security governance
- physical security
- personnel security
- information and communication technology security.

Each of the topics are sectioned into mandatory requirements and recommended guidelines. The mandatory requirements are subject to verification during Notice of Connection (NoC) testing and/or declaration of conformance, as part of the conformance and compliance declaration (CCD) process.

The recommended guidelines are not verified via NoC or CCD, however developers are strongly encouraged to implement these guidelines to further enhance the security of their app solution.

The following table summarises these requirements and guidelines.

*Table 1: Summary of security requirements and guidelines*

Req #	Category	Brief description
<b>Information security governance</b>		
S1101	Requirement	Maintain the security of the technical assets and information assets related to the My Health Record system.
S1102	Requirement	Establish security and privacy policies.
S1103	Requirement	Security policies to be provided to the Agency on request.
S1104	Requirement	Establish a security incident management process.
S1105	Requirement	Establish a patch and vulnerability management process.
S1106	Requirement	Inform consumers that they can revoke the application’s access to the My Health Record system via the National Consumer Portal (NCP).
S1107	Requirement	Provide mechanisms for the removal of consumer data.
S1201	Recommendation	Review and test the security of relevant technical assets.
S1202	Recommendation	Obtain independent security accreditation.
<b>Physical security</b>		
S2101	Requirement	Implement a physical security policy.
S2102	Requirement	Implement a decommissioning process.
<b>Personnel security</b>		
S3101	Requirement	Implement robust hiring and onboarding procedures.
S3201	Recommendation	Provide security awareness and support materials.



Req #	Category	Brief description
<b>Information technology security</b>		
S4101	Requirement	Utilise strong cryptography to secure information assets at rest and in transit.
S4102	Requirement	Implement a Gatekeeper-accredited <sup>1</sup> digital certificate to provide mutual authentication.
S4103	Requirement	Provide a secure locking/unlocking mechanism for mobile apps.
S4104	Requirement	Maintain audit logs on the intermediary server (if any) and the end server.
S4105	Requirement	Store OAuth tokens securely.
S4106	Requirement	Cease use of OAuth tokens by the intermediary server following extended periods of inactivity.
S4107	Requirement	Complete myGov authentication using the system browser.
S4108	Requirement	Protect app IDs and secret keys issued for My Health Record environments.
S4109	Requirement	Access authorised document types only via the GetDocument API <sup>2</sup> .
S4110	Requirement	Enforce strong passwords.
S4111	Requirement	Enforce strong PINs.
S4112	Requirement	Follow security best practices during app development.
S4113	Requirement	Store passwords securely.
S4114	Requirement	Implement a strong identity and access management policy for employees and contracted staff.
S4115	Requirement	Implement user account lockout following multiple unsuccessful authentication attempts.
S4116	Requirement	Erase information assets from mobile devices following multiple unsuccessful attempts to unlock mobile apps.
S4117	Requirement	Limit caching of sensitive information.
S4118	Requirement	Implement session timeouts.
S4119	Requirement	Maintain audit logs on the mobile app.
S4120	Requirement	Ensure sensitive information is not displayed as part of push notifications.
S4201	Recommendation	Ensure digital certificates are validated by each component.
S4202	Recommendation	Ensure there is valid justification for requesting data.
S4203	Recommendation	Monitor the mobile device security environment.
S4204	Recommendation	Prevent data leakage through screenshots.
S4205	Recommendation	Provide multifactor authentication mechanisms.

<sup>1</sup> To find out more about the Gatekeeper Public Key Infrastructure Framework, and the Gatekeeper role, visit <https://www.dta.gov.au/our-projects/digital-identity/gatekeeper-public-key-infrastructure-framework>.

<sup>2</sup> Specific APIs including GetDocument are available in the *My Health Record FHIR Gateway - API Specification v2.2*: <https://developer.digitalhealth.gov.au/specifications/national-infrastructure/ep-3667-2022/dh-3669-2022>

## 2 Information security governance

This section sets out the information security governance requirements and guidelines related to the policies, definitions, processes, roles, and responsibilities in a developer’s organisation. Strong security governance enables developers to respond effectively to changing security priorities driven by threats, risks, and compliance needs.

### 2.1 Mandatory requirements

Table 2 - Requirement S1101

<b>S1101</b>	<b>Maintain the security of the technical assets and information assets related to the My Health Record system.</b>
Description	The developer <b>SHALL</b> take all reasonable steps to maintain the confidentiality, integrity, and availability of relevant technical assets and information assets.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will:</p> <ul style="list-style-type: none"> <li>• identify the security threats and risks associated with the proposed application(s) (and any related information systems, technologies, and business processes)</li> <li>• identify technical controls and process-based controls to mitigate all identified security threats and risks to an acceptable level</li> <li>• implement applicable technical controls and process-based controls to ensure all reasonable steps are taken to protect the security of relevant technical assets and information assets</li> <li>• continuously adapt and improve security controls to manage emerging threats, risks, and vulnerabilities effectively.</li> </ul>
Verification	The declaration of conformance is to be provided during the CCD process using the <i>Production Environment Access Request Form</i> , to confirm that the solution is fit for purpose from a security perspective.

---

**S1101**                      **Maintain the security of the technical assets and information assets related to the My Health Record system.**

---

Additional information

Due to the wide range of possible solution designs, technology architectures, interaction models, use cases, and business models available to developers, and the desire to support new and innovative approaches and solutions, it is not feasible to provide security requirements or guidelines covering all possible scenarios.

Therefore, this document lists the mandatory requirements and recommended guidelines to be considered by the developer in order to establish a minimum level of security maturity.

Ultimately, however, the developer has an obligation to assess the security threats and risks that are associated with their specific solution (and environment) and ensure that all reasonable steps are taken to protect relevant stakeholders and assets. Accordingly, the developer is required to ensure their security capability is appropriate for the threat and risk profile of their solution. This is driven by factors such as:

- the types of information processed
- the intended use of information by consumers, the developer, or other authorised parties
- the volume of sensitive data processed
- the technical assets involved.

The System Operator recommends an independent threat and risk assessment, vulnerability assessment, and penetration testing be carried out by the developer, preferably against an industry accepted assessment standard so as to achieve an objective measure of security maturity.

The following references provide valuable information and advice that should be considered by developers during the design, development, testing, and implementation of their app (and associated security controls):

- *OWASP Mobile Top 10 – 2016 Release Candidate* [9]
  - *OWASP Top 10* [10]
  - *OWASP Application Security Verification Standard v3.0* [11]
  - *National eHealth Security and Access Framework v4.0* [12]
  - *ASD Top 35* [13]
  - *Australian Government Information Security Manual* [5]
  - *OAIC Guide to securing personal information* [14]
  - *OAIC Mobile privacy – A better practice guide for mobile app developers* [15]
  - *ISO 27000 series* [16].
-

Table 3 - Requirement S1102

<b>S1102</b>	<b>Establish security and privacy policies.</b>
Description	The developer <b>SHALL</b> have documented both a security policy and a privacy policy that are accessible by the app user. The security policy and privacy policy may also be a combined documented policy.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that:</p> <ul style="list-style-type: none"> <li>• the developer’s security and privacy policy (which may be either a single publication, or separate publications) will be easily accessible to the app user, at a minimum during the process of gathering an app user’s informed consent to connect the app with their My Health Record</li> <li>• the security policy and privacy policy addresses how the app will interact with an app user’s My Health Record, and how it would collect, use, or disclose their My Health Record data and keep the data safe and secure</li> <li>• a contact channel (e.g. phone number, email address, contact form) is provided to the app user to enable the app user to seek more information about the security policy and privacy policy.</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD process.
Additional information	<p>Consumer willingness to use online health services is affected by their confidence in the privacy, confidentiality, and security of their data. In addition, there is a need for informed consent to be provided by consumers when authorising an app’s access to their My Health Record. Therefore, each developer is required to publish the security policy and privacy policy in plain English. The security policy will describe how the information assets entrusted to them by consumers and the System Operator will be protected. Similarly, the privacy policy will describe how they intend to collect, use, and disclose the information assets entrusted to them by consumers.</p> <p>A useful reference is the My Health Record security and privacy policy, which can be found at <i>Managing access, privacy, and security</i> [17].</p> <p>Developers should also consider their obligations under the <i>Privacy Act 1988</i> for obligations in relation to having a privacy policy.</p>

Table 4 - Requirement S1103

<b>S1103</b>	<b>Security policy to be provided to the Agency on request</b>
Description	The developer may be requested by the Agency in writing to provide a copy of the security policy. The developer <b>SHALL</b> comply with a request and provide the security policy within 7 days of receiving the request.
Applicable interaction models	1 and 4
Implementation guidance	In order to satisfy this requirement, it is expected that the developers establish and maintain their security policy in a timely manner. Further details on the implementation guidance for security policy are mentioned in the requirement S1102.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD process.
Additional information	<ul style="list-style-type: none"> <li>• The <i>My Health Records Rule 2016</i> [18], Part 6, details the participation requirements for developers.</li> <li>• Part 6, Division 2 details the Security requirements for operators [developers].</li> <li>• Part 6, Division 2, Rule No. 60 is about the provision of security policy upon request from the System Operator (the Agency) and its sub-rules are stated below:               <ol style="list-style-type: none"> <li>1) The System Operator may request in writing that an operator provide a copy of the policy mentioned in sub-rule 59(1), concerned with Operator policies.</li> <li>2) An operator must comply with a request from the System Operator under this rule within 7 days of receiving the request.</li> <li>3) The System Operator may request an operator’s current policy or the policy that was in force on a specified date.</li> </ol> </li> </ul>

Table 5 - Requirement S1104

<b>S1104</b>	<b>Establish a security incident management process.</b>
Description	The developer <b>SHALL</b> establish a clearly defined security incident management process.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that:</p> <ul style="list-style-type: none"> <li>the process will include identified points of contact for the users (consumers) and the System Operator</li> <li>all security incidents and security events (i.e. suspected security incidents) will be reported to the System Operator as per incident reporting procedures that will be provided in the welcome pack (i.e. <i>Managing Your App in Production</i>).</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	<p>An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.</p> <p>Due to the varying security controls implemented by developers, the maturity levels of consumers, and the dynamic security threat and risk landscape of the digital health ecosystem, there is significant potential for security incidents to occur. To ensure each developer has the capability to identify, contain, and resolve security incidents effectively, it is mandatory that a security incident management process is in place to manage incidents that are:</p> <ul style="list-style-type: none"> <li>reported by consumers</li> <li>detected by developers</li> <li>identified by the System Operator, or</li> <li>discovered by other parties.</li> </ul> <p>The identified points of contact will enable efficient communication of information to facilitate the effective categorisation, prioritisation, investigation, remediation, and resolution of the security incidents.</p> <p>The following references provide valuable information and advice that should be considered by developers during the design, development, testing, and implementation of their information security management process:</p> <ul style="list-style-type: none"> <li><i>ISO/IEC 27035 Information security incident management</i> [19]</li> <li><i>NIST Computer Security Incident Handling Guide</i> [20].</li> </ul>

Table 6 - Requirement S1105

<b>S1105</b>	<b>Establish a patch and vulnerability management process.</b>
Description	The developer <b>SHALL</b> establish a clearly defined patch and vulnerability management process that ensures system components are patched and vulnerabilities are identified and addressed in a timely manner.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will:</p> <ul style="list-style-type: none"> <li>• implement processes or technology to identify applicable vulnerabilities</li> <li>• assess the security threats and risks associated with each identified vulnerability using a framework such as the Common Vulnerability Scoring System (CVSS)</li> <li>• prioritise the remediation or patching of the identified vulnerabilities based on the level of criticality indicated by the assessment</li> <li>• complete necessary remediation or patching activities in a timely manner (based on target timeframes for each level of criticality defined in the patch and vulnerability management process).</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	<p>The intent of this requirement is to ensure that developers effectively manage vulnerabilities relating to the application, supporting libraries, server software, and infrastructure. Timely patching and mitigation reduce the likelihood of the vulnerabilities being leveraged to negatively impact the confidentiality, integrity, and availability of the information processed.</p> <p>The developer must proactively identify, analyse, and resolve vulnerabilities associated with the mobile applications, web applications, or hybrid applications and their intermediary servers, end servers, and other infrastructure (e.g. associated source code, software libraries, development platforms, operating system software, middleware/application software).</p> <p>The developer must define and implement a vulnerability management process that includes regular patching of hardware and software; and fixing of security related bugs and vulnerabilities in a timely manner. <i>ISO/IEC 27001</i> [21] and <i>ISO/IEC 27002</i> [22] provide guidance on the establishment of a vulnerability management capability.</p>

Table 7 - Requirement S1106

<b>S1106</b>	<b>Inform consumers that they can revoke the application’s access to the My Health Record system via the National Consumer Portal (NCP).</b>
Description	The developer <b>SHALL</b> inform consumers that access to the My Health Record system by the given mobile app, web app, or hybrid app may be revoked via the NCP.
Applicable interaction models	1 and 4
Implementation guidance	In order to satisfy this requirement, it is expected that the developer will provide information to consumers that describes how to revoke the given app’s access to the My Health Record system using the NCP. This information must be accessible by consumers during the consent process and published on the developer’s website.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intent of this requirement is to ensure that the consumer is informed of their ability to revoke the access granted to one or more instances of a given mobile app, web app, or hybrid app. Additionally, enabling consumers to revoke access provides a mechanism to limit the potential for unauthorised access if a device is lost or stolen, and prevent further information sharing if the consumer decides to stop using the app.



Table 8 - Requirement S1107

<b>S1107</b>	<b>Provide mechanisms for the removal of consumer data.</b>
Description	The developer <b>SHALL</b> provide mechanisms for the removal of consumer data from relevant mobile apps, web apps, or hybrid apps, and any intermediary servers, end servers, or other associated information systems.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will:</p> <ul style="list-style-type: none"> <li>• provide a mechanism for consumers to delete mobile apps from mobile devices (including removal of any personal or healthcare information stored by the mobile app)</li> <li>• provide a mechanism for consumers to request the removal of their data from relevant intermediary servers, end servers, or other associated information systems</li> <li>• remove consumer data from relevant intermediary servers, end servers or other associated information systems (when requested), and</li> <li>• notify consumers once their request has been acted upon.</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	To allow consumers to retain control over their personal information and health information, there is a need for mechanisms that enable the consumer data held by developers' systems to be removed in the event that the consumer decides to stop using a given mobile app, web app, or hybrid app.

## 2.2 Recommended guidelines

Table 9 - Recommendation S1201

<b>S1201</b>	<b>Review and test the security of relevant technical assets.</b>
Description	The developer <b>SHOULD</b> review and test the security of relevant technical assets (including mobile apps, web apps or hybrid apps; intermediary servers; end servers; and any other supporting information systems, hardware, and software).
Applicable interaction models	1 and 4
Implementation guidance	Where internal capabilities exist, developers may perform these review and testing activities in-house. However, it is recommended that independent service providers (with CREST certification or similar professional qualifications) should be used where possible. Any findings should be addressed in accordance with the guidance given in requirement S1104.
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	<p>The developer is strongly encouraged to review and test their app and infrastructure from a security perspective to minimise the likelihood of compromise.</p> <p>The intent of this requirement is to increase confidence in the security of the app and the infrastructure that will be processing relevant information assets. The security review and test should be part of the software development lifecycle, and the independent assessment provides additional assurance.</p>

Table 10 - Recommendation S1202

<b>S1202</b>	<b>Obtain independent security accreditation.</b>
Description	The developer <b>SHOULD</b> obtain independent security accreditation for the server software and infrastructure involved in their solution (such as intermediary servers, end servers and other supporting information systems).
Applicable interaction models	1 and 4
Implementation guidance	Developers should identify appropriate security standards or frameworks (such as <i>ISO/IEC 27001 [21]</i> ) for their specific risk profiles and engage independent service providers (possessing relevant professional qualifications such as CREST or CRISC) to assess their app and infrastructure against the chosen standard or framework.
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	The intent of this requirement is for the developers to be confident of their own security posture in relation to processing sensitive consumer information. It can also demonstrate to the consumers the steps which are being taken to secure their information, and therefore increase the trust and confidence consumers have in the app.

### 3 Physical security

Physical controls are determined by the business impact resulting from compromise or loss of confidentiality or integrity, or unavailability of assets. The purpose of physical security is to prevent or mitigate threats or attacks against physical assets.

This section describes the mandatory physical security requirements that apply to the facilities, servers, network devices, ICT equipment, and media used by the developer to support given mobile apps, web apps, or hybrid apps. Where the developer chooses to subcontract these elements to a separate organisation (such as a cloud provider or a hosting provider), the physical security requirements are applicable to these subcontractors.

#### 3.1 Mandatory requirements

Table 11 - Requirement S2101

S2101	Implement a physical security policy.
Description	The developer <b>SHALL</b> implement a physical security policy that describes the arrangements for protecting the facilities, servers, network devices, ICT equipment, and media used by the developer to support given mobile apps, web apps, or hybrid apps.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will identify, assess, mitigate, and monitor applicable threats and risks to physical security. The two main aspects to consider are:</p> <ul style="list-style-type: none"> <li>• the facilities in which the ICT equipment is located in, or can be accessed from</li> <li>• the ICT equipment itself, in which information is processed or transmitted.</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	<p>The intent of this requirement is to ensure that physical security arrangements are in place to protect the facilities, servers, network devices, ICT equipment, and media used by the developer to support given mobile apps, web apps, or hybrid apps. These arrangements must be documented in a physical security policy, and these arrangements need to be proportional to the threats and risks arising from storing and processing the information assets.</p> <p>ISO/IEC 27001 [21] and ISO/IEC 27002 [22] provide further guidance on physical security. The Australian Government’s Protective Security Policy Framework [4], Information Security Manual (ISM) [5], and Common Criteria [23] contain information on the classifications of physical security, which can be used as part of the developer’s implementation.</p>

Table 12 - Requirement S2102

<b>S2102</b>	<b>Implement a decommissioning process.</b>
Description	The developer <b>SHALL</b> implement a decommissioning process that satisfies ISM requirements for the transport, sanitisation, destruction, and disposal of ICT equipment.
Applicable interaction models	1 and 4
Implementation guidance	In order to satisfy this requirement, it is expected that the developer will implement a documented process for decommissioning ICT equipment. This process must define secure methods for the transport, sanitisation, destruction, and disposal of ICT equipment that align with ISM requirements and reflect the sensitivity of the data processed.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	For a number of reasons (such as equipment failure, system upgrades, data centre migrations, and service provider contract changes), there may be a need for ICT equipment to be decommissioned. To prevent any leakage of sensitive information, ICT equipment that will be re-used (or sold as second-hand items), must be sanitised; furthermore, elements that will be retired must be destroyed. Valuable implementation references include <i>ISO/IEC 27040</i> [24] and the physical, product, and media security sections of the <i>ISM</i> [5].

## 4 Personnel security

The purpose of personnel security is to provide a level of assurance as to the honesty, trustworthiness, and loyalty of employees who access sensitive information, and the developer’s responsibility for the health and safety of employees at work. This subsection sets out the personnel security requirements for developers, the employees of the developers, and the consumers of the apps.

### 4.1 Mandatory requirements

Table 13 - Requirement S3101

<b>S3101</b>	<b>Implement rigorous hiring and onboarding procedures.</b>
Description	The developer <b>SHALL</b> implement rigorous hiring and onboarding procedures that apply to any staff members who interact with relevant technical assets and information assets.
Applicable interaction models	1 and 4
Implementation guidance	In order to satisfy this requirement, it is expected that the developer will implement hiring and onboarding procedures that include background checks, confidentiality agreements and security induction training for all relevant staff. These procedures must apply to any staff members who interact with relevant technical assets and information assets.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.

---

<b>S3101</b>	<b>Implement rigorous hiring and onboarding procedures.</b>
Additional information	<p>Developer staff members generally have higher access to resources (such as sensitive information, ICT infrastructure, and application source code) and responsibilities for operational processes than end users. Therefore, deliberate, or inadvertent activities by developer staff members could pose a significant risk. For example:</p> <ul style="list-style-type: none"><li>• A software developer may attempt to introduce malicious code or backdoors into mobile app software or subvert the design process.</li><li>• A system administrator may attempt to leak sensitive information to unauthorised third parties.</li></ul> <p>During hiring, background checks should be performed to verify the suitability of staff members whose duties are associated with relevant technical assets and information assets (e.g. Does the staff member have a good track record performing the duties required? Does the staff member have a previous history of criminal activity or breaching organisational policies and procedures?).</p> <p>Furthermore, confidentiality agreements should be used to prevent the disclosure of sensitive information.</p> <p>Security induction training should be provided to all relevant developer staff members to create an environment where those accessing sensitive information and performing operational processes are aware of organisational policies and procedures, as well as the responsibilities that are associated with their role and level of access.</p>

---

## 4.2 Recommended guidelines

Table 14 - Recommendation S3201

<b>S3201</b>	<b>Provide security awareness and support materials.</b>
Description	The developer <b>SHOULD</b> provide security awareness and support materials for consumers that are accessible within the mobile app, web app or hybrid app and published on the developer’s website.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this guideline, it is expected that the developer provides security awareness and support materials for consumers. This information should be accessible by consumers from within the mobile app, web app or hybrid app, and via the developer’s website.</p> <p>These security awareness and support materials should cover topics such as:</p> <ul style="list-style-type: none"> <li>• device security (e.g. how to enable the locking/unlocking mechanism and configure a PIN, password, or fingerprint)</li> <li>• password security (e.g. password complexity and confidentiality)</li> <li>• system security (e.g. use of up-to-date web browser and operating system software, potential issues with “jailbroken” devices)</li> <li>• special considerations for using apps and mobile devices in public settings (e.g. “shoulder surfing”)</li> <li>• availability of further information through the My Health Record website and Stay Smart Online</li> <li>• the ability to revoke access using the National Consumer Portal if a mobile device is lost (as per requirement <b>Req. S1105</b>)</li> <li>• procedures for reporting suspected security incidents to the developer.</li> </ul>
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	<p>The intent of this requirement is to promote the consumer’s awareness of potential risks in relation to the app, and the reasonable actions that can be taken by consumers to reduce their risk exposure. The following resources are worth consideration:</p> <ul style="list-style-type: none"> <li>• <i>Managing access, privacy, and security</i> [17]</li> <li>• <i>Stay Smart Online</i> [25].</li> </ul>



## 5 Information technology security

The purpose of information technology security is to mitigate threats or risks against the information assets through the implementation of technological controls. This section sets out the information technology security requirements, covering app security, authentication, access control, audit logging, network security and cryptography.

### 5.1 Mandatory requirements

Table 15 - Requirement SS4101

<b>S4101</b>	<b>Utilise strong cryptography to secure information assets at rest and in transit.</b>
Description	The developer <b>SHALL</b> utilise ASD Approved Cryptographic Algorithms (AACAs) and ASD Approved Cryptographic Protocols (AACPs) <sup>3</sup> to secure information assets at rest (e.g. personal information and healthcare information stored by the mobile apps, web apps or hybrid apps; intermediary servers; and end servers), and in transit (between mobile apps, web apps or hybrid apps; intermediary servers; end servers; and the My Health Record FHIR® gateway).
Applicable interaction models	1 and 4
Implementation guidance	In order to satisfy this requirement, it is expected that the developer will: <ul style="list-style-type: none"> <li>• secure all information assets at rest and in transit with AACAs and AACPs</li> <li>• store cryptographic keys in platform-specific key stores, away from the encrypted data, and</li> <li>• develop a key management plan to specify the key length, creation, rotation, destruction, archiving, and use.</li> </ul>
Verification	<ul style="list-style-type: none"> <li>• NoC testing of all communications (data in transit) with the My Health Record system.</li> <li>• The declaration of conformance is to be provided to the System Operator which will be verified during the CDD process.</li> </ul>

<sup>3</sup> ASD Approved Cryptographic Algorithms (AACAs) and ASD Approved Cryptographic Protocols (AACPs) are detailed in the Australian Government's *Information Security Manual Controls* **Invalid source specified.**

<b>S4101</b>	<b>Utilise strong cryptography to secure information assets at rest and in transit.</b>
Additional information	<p>The intent of this requirement is to ensure that the information assets stored or transmitted are protected from unauthorised or unintended leakage.</p> <p>The security of the network carrying the sensitive information cannot be guaranteed. The network can be compromised at the app layer (HTTP) down to the physical layer (Wi-Fi/cellular). The use of cryptography to protect the traffic provides additional assurance to the security of the sensitive information being carried.</p> <p>An example of unintended leakage is the use of cloud backup such as Apple iCloud, Google Drive, Microsoft OneDrive, and Dropbox. If the sensitive information at rest was encrypted, then any backup on the cloud would also be encrypted. Should the cloud service be compromised, the sensitive information would not be legible to an attacker without the corresponding cryptographic keys.</p> <p>Another potential point of data leakage is at the developer infrastructure. With appropriate data at rest encryption, the compromise of the storage (in active use, backup, or archive) does not result in the compromise of sensitive information without the keys.</p>

Table 16 - Requirement S4102

<b>S4102</b>	<b>Implement a Gatekeeper-accredited digital certificate to provide mutual authentication.</b>
Description	The developer <b>SHALL</b> implement a Gatekeeper-accredited digital certificate to provide mutual authentication between the intermediary server and the My Health Record FHIR® gateway.
Applicable interaction models	4 (including web app)
Implementation guidance	<p>A digital certificate issued by a Gatekeeper-accredited certification authority [26] must be installed on the intermediary server for communication with the My Health Record FHIR® gateway.</p> <p>The developer must communicate to the System Operator the chosen certification authority for issuing the digital certificate.</p>
Verification	<ul style="list-style-type: none"> <li>• NoC testing of the mutual authentication.</li> <li>• The declaration of conformance is to be provided to the System Operator which will be verified during the CCD process.</li> </ul>
Additional information	The requirement introduces strong authentication of the intermediary server. There are two main purposes; one is to protect against rogue intermediary servers, and the other is to establish traceability for the transactions initiated by intermediary servers.

Table 17 - Requirement S4103

<b>S4103</b>	<b>Provide a secure locking/unlocking mechanism for mobile apps.</b>
Description	The developer <b>SHALL</b> provide a secure mechanism for the consumer to lock and unlock the mobile app. The use of this feature is the choice of the consumer.
Applicable interaction models	1 and 4
Implementation guidance	The secure locking/unlocking feature must be enabled by default. The mobile app must be locked after no longer than 30 minutes of inactivity to prevent further access. The mobile app must be unlocked through the use of PIN code, fingerprint, password, or passphrase. The mobile app unlock process must be separate to any potential device level unlock already in place. If a fingerprint is used, a PIN code, password, or passphrase must also be set. In the event that five attempts of fingerprint matching were unsuccessful, the app must fall back to the PIN code, password, or passphrase.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	This requirement mitigates potential data leaks on a mobile device temporarily in the control of a third party (for instance, a mobile device repairer, a colleague, or a friend). The System Operator strongly encourages the requirements of <b>Req. S4201</b> be implemented after 10 consecutive unsuccessful unlocking attempts. The developer may wish to implement support for multiple users. This requirement also provides protection on a shared mobile device. The locking/unlocking functionality provides a way to authenticate the active user.

Table 18 - Requirement S4104

<b>S4104</b>	<b>Maintain audit logs on the intermediary server and the end server.</b>
Description	Audit logs detailing the date, time, subject, action, object and results of user, administrator, and system operations on the intermediary server and the end server <b>SHALL</b> be kept for a minimum of 12 months.
Applicable interaction models	4 (including web app)
Implementation guidance	Audit logs with the requisite fields must be collected from the app and supporting information systems and infrastructure. It is recommended that technical measures be deployed to prevent log tampering. The logs should be centralised and backed up.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intent of this requirement is to facilitate any investigations following a security incident, as described in mandatory security requirement <b>Req. S1102</b> .

Table 19 - Requirement S4105

<b>S4105</b>	<b>Store OAuth tokens securely.</b>
Description	The developer <b>SHALL</b> ensure that the OAuth tokens are stored securely.
Applicable interaction models	1 and 4
Implementation guidance	<p>The OAuth tokens must be encrypted as per mandatory security requirement <b>Req. S4101</b> before storing.</p> <p>On mobile devices, leverage a platform-specific key store (such as Keychain on iOS or KeyStore on Android) to store the OAuth tokens. If the platform provides hardware-backed protection for credential storage, then this must be used. Platform capabilities such as ThisDeviceOnly on iOS for preventing credential copying or backup must be used.</p> <p>On intermediary servers, the OAuth token storage (on raw disk or in a database) must have access control applied so that only necessary processes have access.</p>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	OAuth tokens are produced to provide a fundamental mechanism for managing access. The intent of this requirement is to leverage platform-specific privileged key storage mechanisms to securely store the OAuth tokens in order to minimise the likelihood of the tokens being compromised.

Table 20 - Requirement S4106

<b>S4106</b>	<b>Cease use of OAuth tokens by the intermediary server following extended periods of inactivity.</b>
Description	The developer <b>SHALL</b> cease the use of OAuth tokens (both the access token and the refresh token) by the intermediary server if the consumer has not accessed the mobile/web app for more than six months.
Applicable interaction models	4 (including web app)
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will:</p> <ul style="list-style-type: none"> <li>• implement a technical mechanism on the intermediary server to identify user inactivity on the mobile/web app; and</li> <li>• cease use of the user’s OAuth tokens after six months of inactivity.</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intent of this requirement is to ensure that the intermediary server cannot continue to access the My Health Record system on behalf of the consumer even after six months of consumer inactivity. The expiry period for OAuth tokens are two hours for the access token and six months for the refresh token.

Table 21 - Requirement S4107

<b>S4107</b>	<b>Complete myGov authentication using the system browser.</b>
Description	The app <b>SHALL</b> ensure that myGov authentication is completed using the system browser. The app <b>SHALL NOT</b> collect or process the consumer’s myGov credentials.
Applicable interaction models	1 and 4 (consumer apps)
Implementation guidance	In order to satisfy this requirement, it is expected that the developer will ensure myGov authentication is completed using either: <ul style="list-style-type: none"> <li>• the system browser (e.g. Safari or Chrome), or</li> <li>• an in-app WebView that is based on the system browser and runs in a separate process from the host app (e.g. in-app WebView using Safari View Controller or Chrome Custom Tab).</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intent of this requirement is to avoid the consumer’s myGov credentials being processed or intercepted by the mobile app.

Table 22 - Requirement S4108

<b>S4108</b>	<b>Protect app IDs and Secret keys issued for My Health Record environments.</b>
Description	The developer <b>SHALL</b> protect the app IDs and secret keys from being compromised or reverse engineered by an attacker.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will:</p> <ul style="list-style-type: none"> <li>• Ensure processes are in place to maintain the confidentiality of app IDs and secret keys issued for My Health Record environments, and ensure there is no unauthorised access, use or disclosure.</li> <li>• Use advanced techniques to protect the app IDs and secret keys embedded within an app from being compromised or reverse engineered by an attacker. Basic protections such as simple substitution must not be used. However, applicable advanced techniques include complex obfuscation (e.g. breaking up the app ID and secret key into smaller pieces and performing individual complex transformation or encryption before storing in different part of the mobile app binary).</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	<p>An app ID and secret key is used to uniquely identify the developer’s app in the My Health Record system test environment(s) and production environment. Therefore, an attacker wishing to impersonate a developer’s app may attempt to recover the app ID and secret key from the developer (e.g. by leveraging an app ID and secret key that may be disclosed or compromised as a result of an internal process failure) or from the mobile app (e.g. by revealing the app ID and secret key embedded within the app using reverse engineering techniques).</p> <p>Using robust internal processes and protection techniques will complicate any attempts to recover the app ID and secret key. Advanced techniques such as obfuscation discourage attempts to reverse engineer a mobile app.</p>

Table 23 - Requirement S4109

S4109	Access authorised document types only via the GetDocument API
Description	The developer <b>SHALL</b> access authorised document types only via the GetDocument API. Authorised document types are those that were requested by the developer (and approved by the Agency) as part of the registration process.
Applicable interaction models	1 and 4
Implementation guidance	In order to satisfy this requirement, it is expected that the developer will ensure only authorised document types are accessed via the GetDocument API. <b>NOTE:</b> Where document types were not requested by the developer (and authorised by the Agency) as part of the registration process, these document types must not be requested.
Verification	<ul style="list-style-type: none"> <li>NoC testing of limited user-initiated transactions to observe if unauthorised documents were requested.</li> <li>The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.</li> </ul>
Additional information	<p>The GetDocument API provides read-only access to clinical documents stored within the My Health Record system. However, apps are only authorised to access clinical documents that are relevant to their stated purpose.<sup>4</sup> Accordingly, the developer must ensure that their apps do not attempt to access other document types via the GetDocument API.</p> <p>The intent of this requirement is to ensure that apps only access documents where there is a valid “need to know” the information it contains. This minimises the level of information accessed by the app and reduces the level of risk facing the developer, app users and the My Health Record system. The use of the GetDocument API is monitored, and unauthorised use of the API may result in disconnection.</p>

<sup>4</sup> For example, if the purpose of an app is to display pathology information, there is no need for an app to access diagnostic imaging information. Therefore, during the registration process, it is likely that this app will be authorised to access diagnostic imaging documents via the GetDocument API, and not authorised to access other document types such as pathology documents.

Table 24 - Requirement S4110

<b>S4110</b>	<b>Enforce strong passwords.</b>
Description	The app <b>SHALL</b> enforce a strong password where a password is used.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will implement the myGov service’s password complexity rules at a minimum. For example:</p> <ul style="list-style-type: none"> <li>• The password must contain at least seven characters</li> <li>• The password must contain at least one letter</li> <li>• The password must contain at least one number</li> <li>• The password must not be the same as one of your last four passwords</li> <li>• The password must not use the same character repeatedly or have any sequential characters (for example, AAAA or 1234)</li> <li>• The password may contain any of the following characters: ! @ # \$ % ^ &amp; *</li> </ul> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• The password complexity rules above reflect the minimum requirement for apps interfacing with the My Health Record system. It is strongly recommended that stronger passwords should be supported where possible (so that users may select longer/more complex passwords if they wish).</li> <li>• Web apps and portals must assign unique usernames and enforce strong passwords within the user login mechanism. In addition, it is recommended that multifactor authentication mechanisms should also be provided where possible (e.g. as a security feature that may be enabled by the user).</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	<p>A password can be used under a number of contexts. For example:</p> <ul style="list-style-type: none"> <li>• unlocking an app (as per mandatory security requirement <b>Req. S4103</b>)</li> <li>• authenticating to the intermediary server or web app</li> <li>• providing additional mechanisms to control access to high-value information, features or processes.</li> </ul>



Table 25 - Requirement S4111

<b>S4111</b>	<b>Enforce strong PINs.</b>
Description	The app <b>SHALL</b> enforce a strong PIN where a PIN code is used.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will implement the following PIN complexity rules at a minimum:</p> <ul style="list-style-type: none"> <li>• The PIN must contain a minimum of four digits;</li> <li>• The PIN must contain non-consecutive digits; and</li> <li>• The PIN must contain no more than two repeated digits.</li> </ul> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• The PIN complexity rules above reflect the minimum requirement for apps interfacing with the My Health Record system. It is strongly recommended that stronger PINs should be supported where possible (so that users may select longer/more complex PINs if they wish).</li> <li>• Noting the usability challenges associated with a long and complex PIN code, alternative solutions are also supported (such as strong passwords or biometric authentication).</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	<p>A PIN can be used under a number of contexts. For example:</p> <ul style="list-style-type: none"> <li>• unlocking the app (as per mandatory security requirement <b>Req. S4103</b>)</li> <li>• providing additional mechanisms to control access to high-value information, features or processes.</li> </ul>

Table 26 - Requirement S4112

<b>S4112</b>	<b>Follow security best practices during app development.</b>
Description	The developer <b>SHALL</b> follow security best practices during the development of their app.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will:</p> <ul style="list-style-type: none"> <li>• implement the mitigation strategies specified in relation to the Open Web Application Security Project (OWASP) Top 10 Risks for mobile applications [9], or for web applications [10]</li> <li>• observe platform-specific secure coding guidelines: <ul style="list-style-type: none"> <li>○ for iOS (e.g. <i>Introduction to Secure Coding Guide</i> [27])</li> <li>○ for Android (e.g. <i>Security Tips</i> [28])</li> </ul> </li> <li>• complete testing to verify the effectiveness of security controls implemented within their app and associated infrastructure.</li> </ul> <p><b>NOTE:</b></p> <p>The mitigation strategies and coding guidelines above reflect the minimum requirement for apps interfacing with the My Health Record system. However, it is strongly recommended that developers should also verify the security of their apps (and associated infrastructure) using penetration testing performed by independent security consultants.</p>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intention of this requirement is to minimise the introduction of software vulnerabilities during the software development.

Table 27 - Requirement S4113

<b>S4113</b>	<b>Store passwords securely.</b>
Description	The developer <b>SHALL</b> ensure that passwords are stored securely (where passwords are used).
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will:</p> <ul style="list-style-type: none"> <li>• protect passwords by: <ul style="list-style-type: none"> <li>○ using salted password hashing based on an ASD approved hashing algorithm (e.g. SHA-256)</li> <li>○ ensuring that the developer does not store passwords as plaintext</li> <li>○ ensuring that ASD Approved Cryptographic Algorithms are defined within the Information Security Manual [5]</li> </ul> </li> <li>• apply access controls so that only necessary processes (such as the app’s identity and access management modules) have access to the password hashes</li> </ul>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	User account databases represent a valuable target for attackers. Accordingly, it is important for developers to mitigate the risk that passwords may be compromised if their app’s user account database is breached. The intention of this requirement is to prevent stored passwords from being read in plain text and to frustrate attempts to read stored passwords (hashes) if they are compromised by an attacker.

Table 28 - Requirement S4114

<b>S4114</b>	<b>Implement a strong identity and access management policy for employees and contracted staff.</b>
Description	The developer <b>SHALL</b> implement a strong identity and access management policy (and associated processes) governing their app and associated infrastructure.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will implement a strong identity and access management policy, including:</p> <ul style="list-style-type: none"> <li>• clear identity creation, modification and deletion processes;</li> <li>• clear role creation, modification and deletion processes;</li> <li>• adequately defined roles and responsibilities for each staff member; and</li> <li>• consistent application of the concepts of minimum privilege and segregation of duties.</li> </ul> <p><b>NOTE:</b> The policy must also include the use of strong passwords (as per mandatory security requirement <b>Req. S4110</b>) and multifactor authentication.</p>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intention of this requirement is to ensure that only staff members with a need to access certain functionality on a certain app or infrastructure component have this access. This minimises the impact and the likelihood of an accidental or intentional damage to the system. The use of strong password and multifactor authentication enforces the authentication and authorisation of the developer’s staff.

Table 29 - Requirement S4115

<b>S4115</b>	<b>Implement user account lockout following multiple unsuccessful authentication attempts.</b>
Description	The developer <b>SHALL</b> implement a user account lockout following multiple unsuccessful authentication attempts.
Applicable interaction models	1 and 4
Implementation guidance	<p>In order to satisfy this requirement, it is expected that the developer will implement a mechanism that temporarily locks the user account after five unsuccessful authentication attempts (i.e. enforces a delay before the user can complete further authentication attempts).</p> <p><b>NOTE:</b></p> <p>The duration of the delay may be configured at the discretion of the developer, based on the risk profile of their application. In addition, progressively longer timeout delays must be implemented to limit further unsuccessful attempts. For example, if a user has five unsuccessful authentication attempts in a row, a 15 minute lockout period may be placed on the account where the user cannot access the application or perform further authentication attempts. After this 15 minute lockout period has concluded, further authentication attempts may be performed. However, if there are a further five unsuccessful authentication attempts, a 24-hour lockout period should be placed on the account.</p>
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	<p>The intention of this requirement is to limit the potential for an attacker to mount a brute force attack by attempting an exhaustive set of possible username and password combinations.</p> <p>Although the re-authentication delay may be implemented at the discretion of the developer, the configuration should consider the risk profile associated with the given application and the need to prevent excessive authentication attempts.</p>

Table 30 - Requirement S4116

<b>S4116</b>	<b>Erase information assets from mobile devices following multiple unsuccessful attempts to unlock mobile apps.</b>
Description	Following mandatory security requirement <b>Req. S4103</b> , if the number of unlock attempts through PIN code, password or passphrase exceeds 10 times, the mobile app <b>SHALL</b> erase all private and sensitive information associated with the app from the mobile device.
Applicable interaction models	1 and 4
Implementation guidance	Progressively longer timeout delays should be put in place between each attempt after five unsuccessful attempts.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intention of this guideline is to address the potential risk of an attacker mounting a brute force attack by exhaustively trying all possible combinations of PIN codes, passwords, and passphrases.

Table 31 - Requirement S4117

<b>S4117</b>	<b>Limit caching of sensitive information.</b>
Description	The developer <b>SHALL NOT</b> allow a browser to cache sensitive information such as personal information and healthcare information.
Applicable interaction models	1 and 4
Implementation guidance	This can be implemented using relevant HTTP headers such as Cache-Control, Pragma and Expires.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intention of this guideline is to reduce the likelihood of sensitive information leakage via the temporary browser cache.

Table 32 - Requirement S4118

<b>S4118</b>	<b>Implement session timeouts.</b>
Description	The developer <b>SHALL</b> implement a session timeout mechanism to ensure that app sessions do not remain open indefinitely across all web applications. Hybrid apps <b>SHALL</b> utilise device timeout features where applicable.
Applicable interaction models	1 and 4
Implementation guidance	The web app should terminate a consumer user session after a defined period of time such as 15 minutes.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intention of this guideline is to avoid an indefinite or long running web app session. A limited session lifetime reduces the likelihood of attacks.

Table 33 – Requirement S4119

<b>S4119</b>	<b>Maintain audit logs on the mobile app.</b>
Description	The developer <b>SHALL</b> ensure audit logs detailing the date, time (including time zone), subject, action, object and results of user, administrator and system operations are maintained for a minimum of three months.
Applicable interaction models	1 and 4
Implementation guidance	Audit logs with the requisite fields should be collected by the developer’s app or intermediary servers. Due to the limited storage capacity of mobile devices, the log rotation can also be based on the maximum log size, instead of being time-based.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intent of this guideline is to facilitate any investigations following any suspected or confirmed security incident, as described in mandatory security requirement <b>Req. S1102</b> .

Table 34 – Requirement S4120

<b>S4120</b>	<b>Ensure sensitive information is not displayed as part of push notifications.</b>
Description	The app <b>SHALL NOT</b> display sensitive information as part of push, SMS, or email notifications.
Applicable interaction models	1 and 4
Implementation guidance	If a notification is known to contain private and sensitive information, display a prompt for the user to access it from the mobile app rather than as part of the notification.
Verification	The declaration of conformance is to be provided to the System Operator which will be verified during the CCD and/or NoC process.
Additional information	The intention of this requirement is to reduce the likelihood of sensitive information leakage through push notifications. Since these push notifications can be viewed from the mobile device’s notifications list when the mobile device is in a locked state (or when the mobile application is not in use), it is recommended that these notifications should not contain personal and healthcare information.



## 5.2 Recommended guidelines

Table 35 - Recommendation S4201

<b>S4201</b>	<b>Ensure digital certificates are validated by each component.</b>
Description	The developer <b>SHOULD</b> ensure digital certificates are validated by each component (e.g. mobile apps, web apps, hybrid apps, intermediary servers, and end servers).
Applicable interaction models	1 and 4
Implementation guidance	Validation should be through the use of a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP). Where the network operation to access the CRL or OCSP fails, the certificate validation should not fail. Certificate pinning should be considered. Where certificate validation fails, the transaction or the connection must not continue.
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	Validating the revocation status of a digital certificate is an essential tool to evaluate the trustworthiness of a server. Certificate pinning should be considered with the operational management overhead in perspective.

Table 36 - Recommendation S4202

<b>S4202</b>	<b>Ensure there is valid justification for requesting data.</b>
Description	The developer <b>SHOULD</b> ensure that their app and intermediary servers only request data that is necessary for the app to function.
Applicable interaction models	1 and 4
Implementation guidance	Once a piece of data is no longer required for the purpose of the app, it should be removed from the device and the intermediary server.
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	The intent of this guideline is to limit the sensitive information requested by developers from the My Health Record system. Limiting the distribution of sensitive information reduces the risk exposure carried by the consumer, developers and the My Health Record system.

Table 37 - Recommendation S4203

<b>S4203</b>	<b>Monitor the mobile device security environment.</b>
Description	The developer <b>SHOULD</b> ensure that mobile applications implement the detection of the security environment of the device it is installed on. The security environment includes (but is not limited to) the device’s jailbreak status, operating system version and device PIN status.
Applicable interaction models	1 and 4
Implementation guidance	The mobile app should obtain and record the consumer’s explicit acceptance to run the app on a device determined to be insecure by the app.
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	The intention of this guideline is to gain a level of confidence that the mobile device is not compromised (e.g. jailbroken) or easily manipulated by another individual (e.g. lack of device PIN). An insecure operating environment can lead to the compromise of sensitive information.

Table 38 - Recommendation S4204

<b>S4204</b>	<b>Prevent data leakage through screenshots.</b>
Description	The developer <b>SHOULD</b> ensure that apps prevent the device from capturing a screenshot of the mobile app.
Applicable interaction models	1 and 4

---

<b>S4204</b>	<b>Prevent data leakage through screenshots.</b>
Implementation guidance	Prevention of screenshots can be achieved through the use of appropriate operating system calls and flags, such as <b>UIApplicationUserDidTakeScreenshotNotification</b> for iOS and <b>WindowManager.LayoutParams.FLAG_SECURE</b> for Android.
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	The intention of this guideline is to avoid leakage of sensitive information through screenshots. The screenshot function could be activated manually by the user, or it could be activated automatically during a transition between tasks.

---

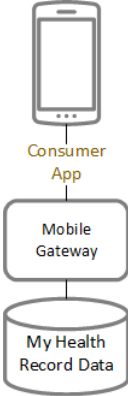
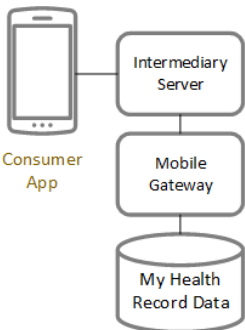
Table 39 - Recommendation S4205

<b>S4205</b>	<b>Provide multifactor authentication mechanisms.</b>
Description	The developer <b>SHOULD</b> provide multifactor authentication mechanisms.
Applicable interaction models	1 and 4
Implementation guidance	<p>This guideline suggests that developers should include multifactor authentication mechanisms within their apps that users may enable at their discretion (e.g. to provide additional control over privileged operations). These mechanisms should include a minimum of two factors from:</p> <ul style="list-style-type: none"> <li>• something the consumer knows, such as a password</li> <li>• something the consumer has, such as a software or hardware token, and</li> <li>• something the consumer is, such as a fingerprint.</li> </ul> <p>The use of multifactor authentication should be the consumer’s choice.</p>
Verification	Not applicable – recommended guidelines will not be verified by the System Operator.
Additional information	<p>The intention of this guideline is to ensure a higher level of assurance for privileged operations (such as changing the password or PIN or uploading healthcare information to the My Health Record system).</p> <p>Primarily, this feature is recommended for web apps and registered portals, but it may also be applicable to mobile apps and hybrid apps.</p>

## Appendix A Interaction models

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

Table 40 - Current interaction models

Interaction model	Description
<p>#1 Consumer/Self-Care</p>  <pre> graph TD     App[Consumer App] --- MG[Mobile Gateway]     MG --- Data[(My Health Record Data)]             </pre>	<p>Consumer mobile app connects with the My Health Record system via the FHIR® gateway.</p>
<p>#4 Consumer Connection via Platform</p>  <pre> graph TD     App[Consumer App] --- IS[Intermediary Server]     IS --- MG[Mobile Gateway]     MG --- Data[(My Health Record Data)]             </pre>	<p>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).</p> <p><b>Note:</b> 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).</p>

## Acronyms

<b>Acronym</b>	<b>Description</b>
AACA	approved cryptographic algorithm
AACP	Australian Signals Directorate-approved cryptographic protocol
API	application programming interface
ASD	Australian Signals Directorate
CA	certification authority
CCD	conformance and compliance declaration
CDA	Clinical Document Architecture
CIS	clinical information system
CREST	Council of Registered Ethical Security Testers
CRISC	Certified in Risk and Information Systems Control
CRL	certificate revocation list
CVSS	Common Vulnerability Scoring System
EU	European Union
FHIR	Fast Health Interoperability Resources
ICT	information and communications technology
ISM	Information Security Manual
NCP	National Consumer Portal
NIO	National Infrastructure Operator
NoC	Notice of Connection
OCSP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
PIN	personal information number
PSPF	Protective Security Policy Framework

## Glossary

Term	Meaning
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)	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Mobile applications</b> are developed to run natively on a specific mobile device or platform (e.g. iOS, Android).</li> <li>• <b>Web applications</b> 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.</li> <li>• <b>Hybrid applications</b> 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).</li> <li>• <b>Progressive web applications</b> can appear and behave as native applications on mobile devices, but do not require installation of the application on the device.</li> </ul>
clinical information system	A system that deals with the collection, storage, retrieval, communication and optimal use of health-related data, information, and knowledge. A clinical information system may provide access to information contained in an electronic health record, but it may also provide other functions such as workflow, order entry, and results reporting.
conformance and compliance declaration	Process for vendors to self-declare conformance to the My Health Record conformance profiles and specifications.
Gatekeeper Accreditation	<p>Gatekeeper accreditation covers the issuing of digital keys and certificates to subscribers that need to work in:</p> <ul style="list-style-type: none"> <li>• open environments, such as the internet</li> <li>• closed environments, such as communities of interest</li> <li>• hybrid communities.</li> </ul> <p>See <a href="https://www.dta.gov.au/our-projects/digital-identity/gatekeeper-public-key-infrastructure-framework">https://www.dta.gov.au/our-projects/digital-identity/gatekeeper-public-key-infrastructure-framework</a> for more information.</p>

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)
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	<p>A notice issued by the My Health Record System Operator indicating that a system is ready to connect to the My Health Record system.</p> <p>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).</p>
OAuth Tokens	OAuth provides to clients a secure delegated access to server resources on behalf of a resource owner. It specifies a process for resource owners to authorise third-party access to their server resources without sharing their credentials. OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third party then uses the access token to access the protected resources hosted by the resource server.
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.
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.
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

1. Australian Government - Federal Register of Legislation, *My Health Records Act 2012*, [Online]. Available: <https://www.legislation.gov.au/Details/C2017C00313> [Accessed 05 02 2020].
2. Office of the Australian Information Commissioner, *Australian Privacy Principles*, [Online]. Available: <https://www.oaic.gov.au/privacy/australian-privacy-principles/> [Accessed 05 02 2020].
3. Office of the Australian Information Commissioner, *Notifiable data breaches*, [Online]. Available: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/> [Accessed 05 02 2020].
4. Australian Government Attorney-General's Department, *The Protective Security Policy Framework*, [Online]. Available: <https://www.protectivesecurity.gov.au/> [Accessed 05 02 2020].
5. The Australian Cyber Security Centre, *Australian Government Information Security Manual*, 2017. [Online]. Available: <https://www.cyber.gov.au/ism> [Accessed 05 02 2020].
6. Privacy Europe, *General Data Protection Regulation (GDPR)*, [Online]. Available: <https://gdpr-info.eu/> [Accessed 05 02 2020].
7. National Center for Biotechnology Information, *Health Insurance Portability and Accountability Act (HIPAA)*, [Online]. Available: <https://www.ncbi.nlm.nih.gov/books/NBK500019/> [Accessed 05 02 2020].
8. Office of the Privacy Commissioner of Canada, *The Personal Information Protection and Electronic Documents Act (PIPEDA)*, [Online]. Available: <https://www.priv.gc.ca/en/about-the-opc/working-at-the-opc/> [Accessed 02 05 2020].
9. OWASP, *OWASP Proactive Controls*, [Online]. Available: <https://owasp.org/www-project-proactive-controls/> [Accessed 05 02 2020].
10. OWASP, *OWASP Top Ten*, [Online]. Available: <https://owasp.org/www-project-top-ten/> [Accessed 05 02 2020].
11. OWASP, *OWASP Application Security Verification Standard*, [Online]. Available: <https://owasp.org/www-project-application-security-verification-standard/> [Accessed 05 02 2020].
12. Australian Digital Health Agency, *National eHealth Security and Access Framework v4.0*, [Online]. Available: <https://developer.digitalhealth.gov.au/specifications/ehealth-foundations/ep-1544-2014> [Accessed 05 02 2020].
13. The Australian Cyber Security Centre, *Strategies to Mitigate Cyber Security Incidents*, 2017. [Online]. Available: <https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents> [Accessed 05 02 2020].
14. Office of the Australian Information Commissioner, *Guide to securing personal information*, [Online]. Available: <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/> [Accessed 05 02 2020].
15. Office of the Australian Information Commissioner, *Mobile privacy: a better practice guide for mobile app developers*, [Online]. Available: <https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/> [Accessed 05 02 2020].
16. *The ISO 27000 Directory*, [Online]. Available: <https://www.27000.org/index.htm> [Accessed 05 02 2020].

17. Australian Digital Health Agency, *Security practices and policies checklist*, [Online]. Available: Security practices and policies checklist. [Accessed 05 02 2020].
18. *My Health Records Rule 2016*, [Online]. Available: <https://www.legislation.gov.au/Series/F2016L00095>
19. ISO, *ISO/IEC 27035-1:2016 [ISO/IEC 27035-1:2016] Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*, <https://www.iso.org/standard/60803.html> , 2016.
20. National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>, August 2012.
21. ISO, *ISO/IEC 27001 - Information security management*, [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html> [Accessed 05 02 2020].
22. International Organization for Standardization, *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls*, ISO, 2013.
23. *The Common Criteria*, [Online]. Available: <http://www.commoncriteriaportal.org/> [Accessed 05 02 2020].
24. International Organization for Standardization, *ISO/IEC 27040:2015 -- Information technology -- Security techniques -- Storage security*, 2015.
25. *Stay Smart Online*, [Online]. Available: <https://www.staysmartonline.gov.au/> [Accessed 05 02 2020].
26. Digital Transformation Agency, *Gatekeeper Public Key Infrastructure Framework*, [Online]. Available: <https://www.dta.gov.au/standard/design-guides/authentication-frameworks/gatekeeper-public-key-infrastructure-framework/> [Accessed 02 05 2020].
27. Apple Inc., *Introduction to Secure Coding Guide - Apple Developer*, [Online]. Available: <https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html> [Accessed 05 02 2020].
28. Google Developers, *Security tips | Android Developers*, [Online]. Available: <https://developer.android.com/training/articles/security-tips> [Accessed 05 02 2020].