Australian Government
Australian Digital Health Agency

My Health Record – FHIR Mobile Gateway
CCD Risk Based Approach – Risk Assessment Questionnaire

20 February 2023 1.1
Approved
Document ID: DH-3709:2023

1 Background

As a part of the vendor onboarding process, the proposed app or new functionality must undergo a risk assessment. The System Operator performs the risk assessment by reviewing user stories, requirements and consent workflows. A demonstration of the app and the solution description may be required to determine if the proposed app:

- presents a significant clinical, security, privacy, legal, policy, operational or hazard risk
- presents a non-conformance risk due to the developer lacking the capability to meet mandatory mobile requirements.

This document details the information required from vendors to initiate the risk assessment process. Please send your completed Risk Assessment Questionnaire to help@digitalhealth.gov.au.

2 Solution deployment timeframe

To assist with your release schedule, we require you to answer the following:

2.1 - When do you intend on releasing and deploying the app into production?

2.2 - Are there any external dependencies to going live in production?

3 Overview of user stories

User stories are to be provided by the developer. They should clearly articulate how a consumer interacts with the app and the My Health Record data/system to produce a health or wellness outcome.

The user stories must provide a comprehensive understanding of the business workflows and benefits associated with sourcing a consumer's My Health Record data, providing the following information – from the point of view of the consumer:

- actor/s (i.e. consumers) [actor]
- action describing what will happen [action]
- a description of the purpose of the feature [purpose]
- acceptance criteria
- provide screenshots of the health or wellness outcomes presented to the consumer as a result of interfacing with the My Health Record system [image].

Please see an example below describing the preferred format:

> *As a consumer [actor] I want to be able to login into the Website [action], so I can access my account [purpose].*
>
> *Acceptance criteria*
>
> - *User enters in credentials and clicks login.*
> - *User is authenticated.*
> - *User lands on 'my account' page post authentication.*
> - *If authentication is unsuccessful, prompt user to re-enter credentials.*

Developers can choose to embed the user stories in this document or provide a separate document containing the user stories with a reference to the separate document embedded in this document.

4 Operational

Please respond to all the questions within this section.

4.1 - Will the app be for consumer use only?

○ Yes ○ No

4.2 - Please describe the function of each component in the system.

4.3 - Please describe your incident management processes, including identification, logging, analysis and resolution processes.

4.4 – In the event of an incident, what processes are in place to prevent a reoccurrence?

5 Security

Any questions in this section that are not applicable, respond with *"N/A"* and provide reasons.

5.1 - Please briefly describe the system security policy for the solution (including all components etc.)

5.2.1 - Has any external assessment (e.g. penetration testing or code review) been completed on your solution?

○ Yes ○ No

5.2.2 - If **Yes**, please provide copies of any security certifications or assessments (such as ISO certifications, IRAP assessments and penetration testing reports).

5.3 - How do you assess, record, mitigate, and accept security risks related to the solution?

5.4.1 - Has the solution been assessed against the ASD essential Eight?

○ Yes ○ No

5.4.2 - What maturity level did the solution rate in each mitigation strategy? See - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

5.5 - Please describe the security incident management process for the solution, including the timeframe for notification of breaches to your customers.

5.6 - Please describe the solution’s hosted environment, including any service partners in use e.g. Amazon Web Services.

5.7 - Which geographic region is the solution’s datacentre(s) located in?

5.8 - Please describe how your solution uses end-to-end encryption, including SHA level, transit and at rest.

5.9 - Please describe how the solution’s encryption key management is handled.

5.10 - Please describe what controls are applied to privileged access of the solution (e.g. multi-factor authentication, secure privilege access workstations, jump hosts).

5.11 - Please describe the controls that are in place to restrict access to and tampering of the solution’s audit and security logs.

5.12 - Are the solution’s audit and security logs stored in a central repository?

○ Yes ○ No

5.13 - Please provide details of the solution’s audit logging processes, including type of logs collected and where they are stored.

5.14 - Please describe the controls that are in place for authentication and session management models when accessing the solution or system(s) used for managing the solution.

5.15 - Please describe the identity and access management policy for employees, and contracted staff that access the solution or access systems used for managing the solution.

5.16 - Do you maintain separate production and non-production environments, for development and testing of the solution?

○ Yes ○ No

5.17.1 - Do you maintain security baselines of solution servers and cloud configurations (hardening) e.g. Center for Internet Security Benchmarks - https://www.cisecurity.org/cis-benchmarks/?

○ Yes ○ No

5.17.2 - If Yes, please describe.

5.18 - Please describe how the solution isolates My Health Record data from other applications that share a common device or platform (for example, Apple's Health Kit).

5.19 - Please describe the role of the intermediary server in the provision of features to the end-user.

5.20 - Will My Health Record data undergo any transformation or alteration as part of the application features, and what are the measures incorporated to ensure data integrity is maintained?

5.21 - Please provide confirmation that you have completed and returned the OWASP security checklist.

○ I confirm I have completed and returned the OWASP security checklist

6 Privacy

Please provide a response to the following questions.

6.1 - Please describe the Health Service being provided by your app. Refer to Privacy Act 1988 – Section 6FB > Meaning of Health Service.

6.2 – Who is your designated officer responsible for privacy compliance in your organisation? Please provide their contact details below

- https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information/
- https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/

6.3 - Describe the practices, procedures and systems that are in place within your organisation to enable compliance with the Australian Privacy Principles, that will enable you to deal with privacy enquiries and complaints.

6.4 - How do you ensure staff awareness of privacy obligations associated with your application and its use of My Health Record data?

6.5 – If your organisation is considered to be a ‘Small Business Operator’ as defined in the Privacy Act, your organisation must opt-into being treated as an organisation under the Privacy Act

If you are not a Small Business Operator, it is mandatory for your organisation to opt-in to the ‘Office of the Australian Information Commisioner’ opt-in register. Has your organisation opted in?

○ Yes ○ No

You are required to provide evidence that you have opted in, by attaching the evidence in your email of submission to help@digitalhealth.gov.au and labelling it as “[OrganisationName]_opt-in evidence”.

Note, if you have answered **‘No’**, you will not be provisioned access to the production environment, until you have opted in and provided evidence. For guidance on the ‘opt-in’ process, please visit: https://www.oaic.gov.au/privacy/privacy-registers/privacy-opt-in-register/opting-in-to-the-privacy-act/

6.6 - Does your organisation have a privacy policy and how can users and potential users find it?

6.7 - **Optional** - describe your process for privacy planning, including ‘Privacy by design’.
This means considering privacy from the beginning of the design process, including in developing the architecture and specifications of the app; such as thinking about privacy in the user journey, from when users first interact with your app until such time as they may choose to delete their account.

For guidance, please refer to: https://www.oaic.gov.au/privacy/guidance-and-advice/mobile-privacy-a-better-practice-guide-for-mobile-app-developers/

7 Technical

A response is required for all questions in this section.

7.1 - Please outline how you will isolate My Health Record data from any default or automated access, including upload to central repositories, through Software Development Kits.

7.2 - Within your application, what other health-related data is transmitted or linked to any other devices (i.e. anything other than a mobile device, e.g. Fitbit or other wearables)?

Thank you for completing the Risk Assessment Questionnaire, please send your completed Risk Assessment Questionnaire to help@digitalhealth.gov.au.

Publication date: 20 February 2023

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

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.

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