API owner onboarding form

# Purpose

Fill this form in when your API/service has been developed and system tested. Upon receiving this form, we will:

* Commence the build of your gateways allowing you to commence end to end and conformance testing
* Draft your API listing to put onto our public facing website
* Engage with Legal to draft your API schedule agreement
* Prepare your Mock+ environment for receipt of your reference data
* Notify our support teams of the support requirements for your API and make sure we have the right support in place upon publication of your API
* Give notification to our Security, Privacy and Clinical teams to ensure the path to getting their approvals for your Production release is smooth

Please return completed forms to: [digitalserviceshub@tewhatuora.govt.nz](mailto:digitalserviceshub@tewhatuora.govt.nz).

# Before you begin

Prior to filling in this form, you must have completed an Expression of Interest form and built and test of your API/service. It is also important that you have completed the API/service checklist and considered all activities mentioned.

ONBOARDING DETAILS

Key Contacts

Provide name, email address, and contact number. Our onboarding team will engage with your technical contact to configure the gateways.

|  |  |
| --- | --- |
| **Role** | **Name, email address and phone number** |
| Product Owner |  |
| Implementation / Technical Contact |  |
| Escalation Contact |  |

1. API/service Overview

API/service name

Name or short title of the API/service.

|  |
| --- |
|  |

Short description of your API/service

Please sum up your API/service in a single sentence.

|  |
| --- |
|  |

Brief description of your API/service

The information you provide in this area will be uploaded to the [Digital Services Hub website](https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/digital-services-hub/explore-apis-digital-services/) and used by API Subscribers to tell them what your API/Service provides and help them determine whether they might like to subscribe to this API/Service.

Tip: You might like to copy the summary statement made in your Expression of Interest form and review/update that statement..

|  |
| --- |
|  |

Overview

The information you provide in this area will be uploaded to the [Digital Services Hub website](https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/digital-services-hub/explore-apis-digital-services/) and used by API Subscribers to give them more information about your API/Service provides and help them determine whether they might like to subscribe to this API/Service.

Tip: You might like to copy the summary statement made in your Expression of Interest form and review/update that statement..

|  |
| --- |
|  |

1. Data and data accuracy

What data can be accessed with this API/service?

|  |
| --- |
|  |

Who is the data collected from?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Individual |  | Clinician | Other: |  |

Is your data source the master of all data points stored with in?

Or is there data you pull from other sources and surface with your API eg. NHI

|  |  |  |
| --- | --- | --- |
|  | Yes we are the master of all information in our data source. | |
|  | No. There is some or all data in our data source that we don’t master and is pulled from another source. | |
|  | What information is pulled from another source? | |
|  | |

Are there any known gaps in the data?

For example, unavailable or incomplete data; aggregated data etc

|  |
| --- |
|  |

Are there any prerequisites for accessing the data?

For example, in order to receive death events, a subscriber must first subscribe to the NHI FHIR API

|  |
| --- |
|  |

1. Use of data

Who can use this Service?

List the intended user groups for this service.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Healthcare consumers (or their specified delegates) | | |  | Healthcare Providers (eg. Doctors, nurses, specialists, pharmacists) |
|  | Healthcare Administrators (eg. Hospital/Clinic Managers, Practice Managers) | | |  | Health New Zealand internal resources (eg. Contact tracing teams) |
|  | Government agencies or crown entities (eg. Ministry of Justice, ACC, ESR). Please specify | |  | | |
|  | Public Health Officials (eg. Epidemiologists, policy makers). Please specify | |  | | |
|  | Other. Please specify |  | | | |

What is the general use case for the data you are surfacing?

|  |  |  |
| --- | --- | --- |
|  | [USE CASE 1: To allow a healthcare provider to access patient information to support direct care of a patient](https://mohits.atlassian.net/wiki/spaces/SI/pages/3890710847/General+API+Use+Cases#USE-CASE-1%3A-To-allow-a-health-care-provider-to-access-patient-information-to-support-direct-care-of-a-patient) | |
|  | [USE CASE 2: To allow a healthcare provider to supply patient information to HNZ](https://mohits.atlassian.net/wiki/spaces/SI/pages/3890710847/General+API+Use+Cases#USE-CASE-2%3A-To-allow-a-health-care-provider-to-supply-patient-information-to-HNZ) | |
|  | [USE CASE 3: To allow provision of information about a healthcare consumer to that consumer](https://mohits.atlassian.net/wiki/spaces/SI/pages/3890710847/General+API+Use+Cases#USE-CASE-3%3A-To-allow-provision-of-information-about-a-health-care-consumer-to-that-consumer) | |
|  | [USE CASE 4: To allow other authorised HNZ uses (HNZ systems only)](https://mohits.atlassian.net/wiki/spaces/SI/pages/3890710847/General+API+Use+Cases#USE-CASE-4%3A-To-allow-other-authorised-HNZ-uses-(HNZ-systems-only)) | |
|  | Other |  |

Expand on your use case

Include the lawful grounds for disclosure and who the information may be shared with. Your API privacy impact assessment (PIA) or privacy specialist should help you define this.

|  |
| --- |
|  |

Please detail any restrictions on sharing the data

For example: this data cannot be shared with anyone outside of mental health agencies as it could disproportionately impact or stigmatise vulnerable groups or individuals.

|  |
| --- |
|  |

What labels/tags should we assign to your API/service

Using tags or labels on your APIs enhances discoverability, organisation and management making it easier for subscribers to find and understand your services.

|  |
| --- |
|  |

1. Risk Assessment

Please complete the [API Risk Score](https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/digital-services-hub/knowledge-hub/api-risk-framework/privacyidentity/) assessment and provide the risk score for each operation below per example provided. Add rows as required.

| Operation | Privacy Risk Score | Clinical Risk Score |
| --- | --- | --- |
| e.g. GET patient | HIGH  8 | MEDIUM  11 |
|  |  |  |
|  |  |  |

Specific Risk Controls

Please list any risk controls or use restrictions that must be explicitly understood and implemented by a subscriber or consumer of this API or service. These are often but not always specific requirements from a privacy, security, or clinical assessment. This information will form part of the conditions of use.

|  |
| --- |
|  |

1. Technical Details

Solution Design

Please provide a link (and access) to your Solution design or attach it

|  |
| --- |
|  |

Implementation Guide

Please provide a link to your Implementation Guide below.

|  |
| --- |
|  |

OpenAPI Spec

Please provide a link to your OpenAPI spec below.

|  |
| --- |
|  |

Does the API gateway currently have a public or private facing interface, or will it have one in the future?

Please provide public URL if applicable

|  |
| --- |
|  |

What is used for API authentication?

e.g. Azure AD, Keycloak, Cognito

|  |
| --- |
|  |

What access controls have you allowed?

|  |  |  |  |
| --- | --- | --- | --- |
|  | [HEART](https://openid.net/specs/openid-heart-uma2-1_0.html) (Health Relationship Trust) Working Group specifications | | |
|  | Attribute Based Access Controls (ABAC) | | |
|  | Other | |  | | --- | |  | |

What is the endpoint for the Identity Provider?

|  |
| --- |
|  |

Are there any rate limits or is throttling required?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | We have a rate limit of: |  | | |
|  | We require throttling at a burst measure of: | |  | |
|  | We don’t have a rate limit or require throttling | | |

Does the API support HTTPS for secure data transmission?

|  |  |  |  |
| --- | --- | --- | --- |
|  | No |  |  |
|  | Yes |  |  |
|  | What are the encryption protocols? | | |
|  |  | TLS 1.2 |  |
|  |  | TLS 1.3 |  |
|  |  | Other | |  | | --- | |  | |

What audit logging and monitoring do you have in place?

|  |
| --- |
|  |

Volume and Performance

Please provide future measures to reflect anticipated growth in service usage where possible.

| Objective | Current | Future |
| --- | --- | --- |
| Transactions per day |  |  |
| Maximum transactions per hour |  |  |
| Maximum concurrent users |  |  |
| Service response time(s)  (e.g. 95% of requests will be responded to within 1 sec) |  |  |
| Service usage growth  (% transaction volume increase per annum) |  |  |

What is your standard process for onboarding?

We would like to know if there are special considerations to be aware of, eligibility checks that must be done, further access granted in EntraID etc. Please also specify any mappings we need to do with business functions and OAuth scopes if necessary.

|  |
| --- |
|  |

What is the usual way you will grant credentials to your API?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Credential by application**  A ClientID and secret is assigned to the subscribing application. This scenario can occur with cloud-based applications. | | |
|  | **Credential by Organisation-application**  A ClientID and secret is unique to the organisation using the application ie. Each pharmacy/GP practice/dental surgery gets their own set of credentials for a common application. | | |
|  | Other | |  | | --- | |  | |

Elaborate if necessary

|  |
| --- |
|  |

1. Operations

Key Support Contacts

Who will be the contacts that will be contacted for support when your API/service is in Production?

|  |  |
| --- | --- |
| Support Contact  Name, title, email & phone number |  |
| Escalation Contact  Name, title, email & phone number |  |

Service Levels

| Objective | Measure |
| --- | --- |
| Service Availability (%)  What is the uptime of your API? |  |
| Support Hours  When can integrators expected to get support from an operational team if there are issues with your API? |  |
| Maintenance Window  Do you have specific times where you will make updates to the API? |  |
| Recovery Time Objective (RTO)  The maximum acceptable time that an application, computer, network, or system can be down after an unexpected disaster, failure, or comparable event. |  |
| Recovery Point Objective (RPO)  Maximum data loss (as measured by time) after a recovery from a disaster, failure, or comparable event. |  |
| Support Response Time(s)  e.g. P1: 2 hours |  |

Planned Releases

Please provide a roadmap of any planned releases and expected release dates. Alternatively, you may wish to attach a copy of your product roadmap.

|  |
| --- |
|  |

1. Funding

Please confirm the funding mechanism for this piece of work.

What is the cost centre we can on charge the setup and operational costs to?

|  |
| --- |
|  |

1. Additional Information

Is there any additional information that should be documented regarding your API/service?

For example: our API has the ability to enrich data and will query the NHI and HPI APIs to bring back demographic information. For this to work, subscribers will also have to subscribe to the NHI and HPI API.

|  |
| --- |
|  |