MINISTRY OF HEALTH
MANATŪ HAUORA

New Zealand Government

COVID-19

Contact Tracing Integration Platform

Proof of Concept API Integrations

Version 1.0 8 July 2020

Citation: Ministry of Health. 2020. *COVID-19 Contact Tracing Integration Platform – Proposed Use Cases and Integrations*. Wellington: Ministry of Health.

Published in July 2020 by the Ministry of Health
PO Box 5013, Wellington 6140, New Zealand

ISBN xx (online)
HP xx [Insert]

MINISTRY OF HEALTH
MANATŪ HAUORA

This document is available at health.govt.nz

Contents

1 Introduction

This document is intended as a discussion document to outline the Ministry of Health's APIs for allowing third party developers to provide data and high-level integration with the National Contact Tracing Solution (NCTS).

1.1 Purpose

This document has been produced as part of the COVID-19 epidemic response in New Zealand.

The contents of this document are to serve as information for use by industry partners to determine the feasibility, approach, and utility of integrating with the National Contact Tracing Solution (NCTS).

The detail expressed in this document are foundational. Whilst the Ministry of Health do not intend to change these APIs or the supporting data requirements, changes to public health guidance, legislation or decisions by the Government may require this to happen.

The detail in this document has not been subjected to formal clinical review.

1.2 Scope

This document covers several options for allowing developers of third-party technology and services to provide data that may support contact tracing.

1.3 Definitions

Casual contact is any person with exposure to the case who does not meet the criteria for a close contact.

Contact alert is a notification that indicates the presence of a suspect, confirmed or probable case of COVID-19, or a close contact of these, denoted by a location identifier (GLN) and time window.

Contact tracing is the process used by public health units and the national close contact service to track down people who may have been exposed to COVID-19 through contact with a suspect, confirmed or probable case during that person's infectious period.

Close contact means a person who has been exposed to a confirmed or probable case of COVID-19 during the case's infectious period, without appropriate personal protective equipment. For example, this could have been in a closed environment within 2 metres of the case for 15 minutes or more. See **here** for the full criteria.

1.4 Reference documents

Contact Tracing App Privacy Impact Assessment
HISO 10085:2020 COVID-19 Contact Tracing Data Standard
COVID-19 Contact Tracing Check-in QR Code Data Specification

1.5 Revision history

20 May 2020	Initial draft published
8 July 2020	Version 1.0 published

2 Background

In New Zealand, a nationwide state of emergency was imposed in response to the COVID-19 pandemic. Contact tracing is one of the pillars of the public health response to COVID-19, along with border control, testing and case isolation. A comprehensive contact tracing system will enable rapid identification and isolation of new cases and is central to breaking the chain of transmission and eliminating COVID-19.

2.1 Contact tracing process

Contact tracing starts with a phone call from the public health unit or national close contact service. The person is provided with advice on self-isolation and their health and wellbeing is checked. The person receives daily follow up calls during the isolation period.

Key to contact tracing is getting information about the contacts of persons with COVID-19 to identify the source of the infection and make close contacts aware of the risk and the need to get tested and self-isolate if required

The Ministry of Health will be broadcasting Exposure Events of Interest notifications through an API, which will contain a location identifier (GLN) and time window indicating the presence of a suspect, confirmed or probable case of COVID-19, or a close contact of these. Approved contact tracing solution developers will be able to match this information with any corresponding check-ins which users of their solution may have recorded and provide this information to the Ministry of Health.

Where a business has authorised the release of check-in details from their location or an individual has consented to allow details of their visited locations to be provided to contact tracers when requested. The contact tracer will provide a six-digit alpha-numeric code that can be entered into the third-party solution, and to authorise the transfer of this information to the Ministry of Health.

2.2 Integration

The Ministry recognises that a number of third-party solutions have been developed to support contact tracing, and the benefit that an ecosystem of solutions can bring to improving the contact tracing process.

This benefit needs to be carefully balanced with privacy and consent requirements, data security and integrity of any integrations, and overall clinical utility in collecting the information.

While the Ministry has developed the NZ COVID Tracer app and government issued QR codes to support contact tracing, these are not intended to be the only solutions, nor does the Ministry expect the first-party solutions will meet the needs of everyone in New Zealand.

As such, the Ministry is open to exploring ways for developers of third-party solutions to securely contribute the data they have collected,

2.3 Data collection principles

The Ministry's stance on data collection to support contact tracing is that any data collection should be minimised as much as possible. The **Health Information Privacy Code (1994)** sets out rules around the collection and storage of health information. Further information and your obligations about the Health Information Privacy Code can be found on our website[1].

The reason the Health Information Privacy Code is important is because some information collected will become health information during this process. For example, information collected on a contact tracing register becomes health information when a person in the register tests positive.

This stance also means the Ministry will not create a central database of the public's movements and close contacts. This information would only be collected from people who have, for example, tested positive, are a suspected close contact, or a suspected casual contact.

2.4 Integration benefits and assumptions

2.4.1 Potential benefits to integration

The following known opportunities for data to improve the contact tracing process related to visited locations are:

1. Improving the speed that contact tracers can obtain information about potential Close contacts at a location where there is a high transmission risk
2. Improving the speed at which a notification to a potential Close contact can be sent.
3. Improving the accessibility of current contact details for a business or location, meaning a contact tracer can contact a business quicker.
4. Reducing the risk of transmission by visitors needing to share a 'dirty pen' to sign a paper-based register.
5. Reducing the risk of personal information being disclosed to unauthorised staff or other customers (ie reading other people's information off a paper register).
6. In a decentralised model, giving the customer control over their own information, where it is only disclosed to contact tracers if they test positive, and to nobody else.

[1] https://www.privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/health-information-privacy-code-1994/

2.4.2 Assumptions

The following assumptions have been made for this use case:

1. Any recorded locations are identified by a Global Location Number (GLN).
2. A location without a GLN has less value to the contact tracing process, as it is more difficult to uniquely identify a location, undertake cluster identification, or send exposure event of interest notifications.
3. Developers of solutions that use QR codes are required to support the NZ COVID Tracer QR code format where possible and promote the use of these posters to their customers.

3 Rationale

The Ministry has identified the following opportunities for interoperability with third party technology solutions that could contribute data to support contact tracing. This capability is broken into two types – visitor registers and consumer digital diaries – depending on the model used to capture the data, and where it is stored.

3.1 Visitor registers

In this model when a user 'checks-in' to a location the record of that check-in is stored in a central database, accessible by the business or their delegate who would be responsible for sharing that data on behalf of the place that captured it. These are most often operated by a *location* and store information about *visitors*.

This model is most closely aligned to a traditional paper register, where a customer signs a physical piece of paper with their name, phone number, and other details.

This is the most commonly seen third party solution to date and relies on the business to provide that information to a contact tracer.

If the location is using an integrated third party solution for managing a visitor register, they will be given a 6 digit one-time-password and a time range over the phone to send the relevant data to contact tracers electronically.

This would require integrators to develop an interface for themselves or their customers to enter this code and time window, then use the API endpoint to upload this data to the Ministry.

Other solutions that match visitors to a location but are not specifically identified as visitor registers would also fit this model.

3.2 Consumer 'digital diaries'

This model targets individuals and allows them to record the places they have been.

This data could be stored on a centralised database, or locally on the consumers mobile device, however the functional outcome is the same. The diary is owned by the *individual* and records information about the *locations* they have been. Individuals can give their consent to the information being shared for contact tracing purposes.

The NZ COVID Tracer fits this model, where the data is stored locally on the consumer's mobile device. No requests are made to a central server when a scan is made, so there is no way to track an individual user's movements.

When a person is confirmed to test positive for COVID-19 they are called by their local Public Health Unit (PHU). During this call they are informed of their positive test result, and (in subsequent calls) asked for information about where they have been, and who they have been in contact with.

A contact tracer will then undertake an investigation process to trace any close contacts.

To support this effort a person using a ‘digital diary’ app will be asked if they consent to sharing their diary electronically. If the user consents, they are given a 6-digit alphanumeric one-time-password. This one-time-password is read out to the person over the phone by the contact tracer for the person to enter into their digital diary app.

This authenticates the upload request and allows the data to be linked to the correct case in the national contact tracing solution.

4 API integrations

To support the opportunities above, the Ministry is developing the following APIs for integration with third party solutions. Note these APIs may be adapted in future, as required by contact tracing, public health, or government requirements.

4.1 API connectivity

Developers wishing to integrate with contact tracing APIs will be required to provide proof their solution meets a baseline set of criteria, including digital security, privacy, and clinical processes.

For the proof of concept this set of criteria will be developed in conjunction with industry partners to confirm it is fit for purpose and able to meet the needs of contact tracing.

Authentication to the proof of concept APIs will be using OAuth 2.0 Client Credentials that are issued to a developer once they have demonstrated their conformance to the minimum platform requirements.

Developers will be required to exchange their client credentials for an access token that can be used to authenticate with the Ministry APIs for contact tracing. This access token will identify the developer application to the Ministry. At this stage there is no plan to offer user-level authentication beyond a one-time-password for select endpoints, as outlined in later sections.

All endpoints send and receive data in a JSON format, over a HTTPs connection.

4.2 Subscribe to Exposure Event of Interest notifications

This feed allows authorised developers to receive a list of exposure events of interest (EEOI). An EEOI will contain a GLN location, a time window, and may contain other relevant data for a subscriber to take appropriate action.

For the proof of concept, this feed will be available as a HTTPs webhook, and subscribers will need to make a HTTPs endpoint available over the internet to receive these notifications.

There are two use cases for EEOI notifications and based on the target users of a solution.

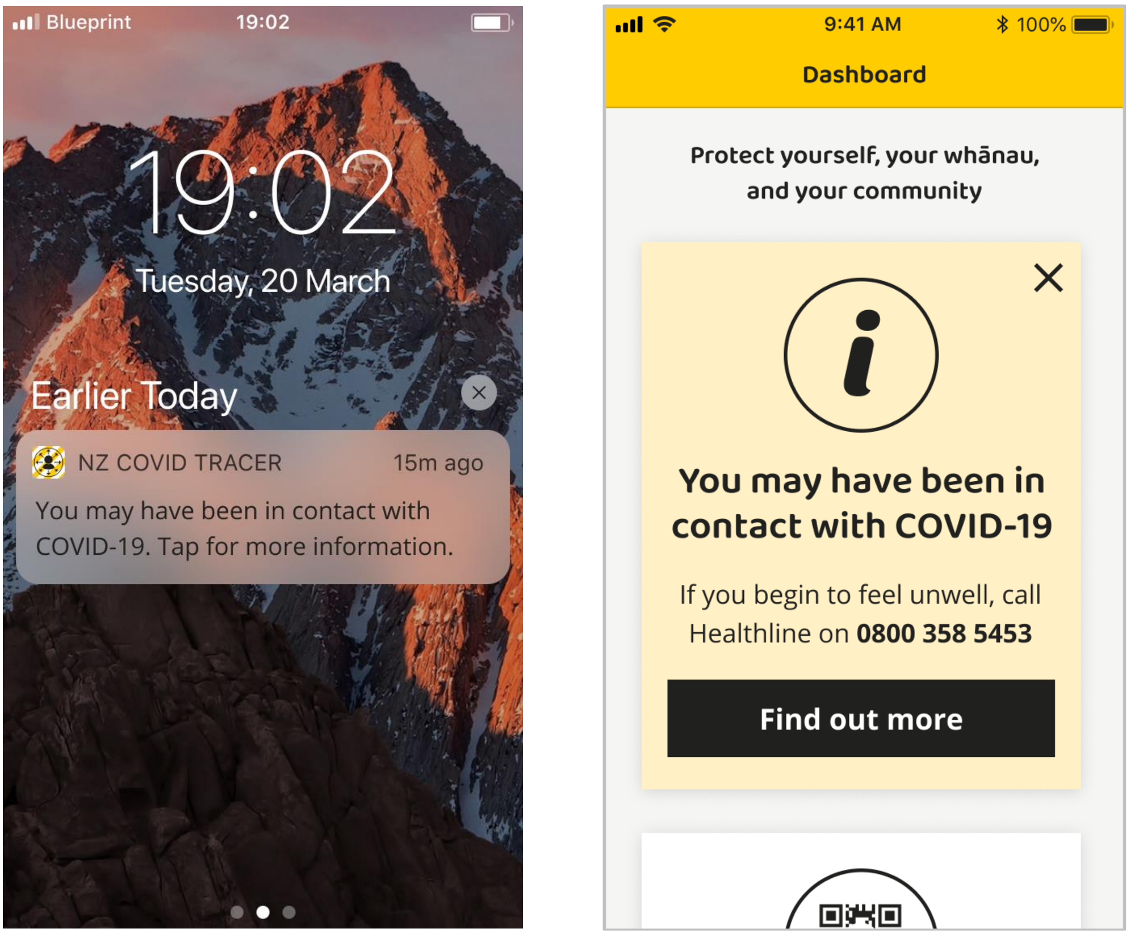
4.2.1 Contact alerts

For developers of consumer ‘digital diaries’, an EEOI may be translated to a contact alert to notify an individual of a potential contact with COVID-19.

A contact alert notification presents the user with some messaging letting them know they have potentially been at the same place around the same time as a person who has tested positive.

Currently, a person being shown this alert is classified only as a casual contact, so the alert is informational only. The person should monitor their health and if they begin to experience symptoms they should seek a test, however they are not required to speak to contact tracers or self-isolate. They are not required to share their digital diary or otherwise identify themselves to contact tracers.

The NZ COVID Tracer app currently implements contact alerts, as shown in the following screen designs.



You may have been in contact with COVID-19. Tap for more information.

Protect yourself, your whānau, and your community

You may have been in contact with COVID-19

If you begin to feel unwell, call Healthline on **0800 358 5453**

Figure 1: Screen designs from the NZ COVID Tracer app showing the contact alert functionality.

4.2.2 Visitor register matching

For developers of visitor registers, or solutions that hold information about people at a place within a given time, an alternative use case is to request that information through electronic means.

Using the GLN and time range in the EEOI the subscriber can search their dataset for matching visitor entries at the location within the time period. Any matching records can then be sent back to contact tracers electronically and linked to the appropriate case record for investigation. This process is shown at a high level in Figure 2.

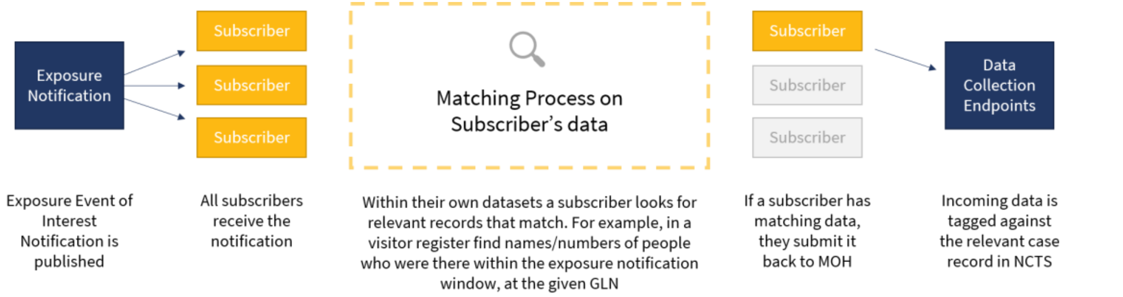

Exposure Notification
Subscriber
Subscriber
Subscriber
Matching Process on Subscriber's data
Subscriber
Subscriber
Subscriber
Data Collection Endpoints
Exposure Event of Interest Notification is published
All subscribers receive the notification
Within their own datasets a subscriber looks for relevant records that match. For example, in a visitor register find names/numbers of people who were there within the exposure notification window, at the given GLN
If a subscriber has matching data, they submit it back to MOH
Incoming data is tagged against the relevant case record in NCTS

Figure 2: A high level process flow for the visitor register data matching process

Consideration must be given to whether a visitor has knowingly consented to having their data shared through this means, and that the subscriber is authorised to share the person's name and contact details on their behalf.
Developers will be required to provide proof their solution meets a baseline set of criteria for which this requirement is likely to form part of.

4.2.3 Webhook format

The webhook format is a plain JSON object sent via a POST request to a nominated HTTPs endpoint. The following points must be noted by a subscriber:

1. The endpoint must be served with valid CA-signed HTTPs certificate otherwise the request will not proceed.
2. A HMAC SHA384 signature of the payload will be sent as a `X-Hook-Signature` header, using a pre-shared secret. This is so subscribers can verify the payload was sent from the Ministry and has not been forged.
3. The endpoint must respond with a HTTP 200 OK response to be considered successful. There will be limited failure handling and retry capability during the proof of concept phase and guaranteed once-only delivery is not a requirement.

The parameters of the webhook payload are as follows:

Name	Format	Description
`EventId`	String, required	A unique ID for the exposure event.
`NotificationId`	String, required	A unique ID for this notification. Multiple notifications may be sent for the same EventId, but the same NotificationId should only be received once.

`GLN`	String, required	The 13-digit number representing the location the exposure event happened at
`Start`	Timestamp, required	An ISO9601 timestamp representing the start of the time window of interest. Matching records must occur after this time.
`End`	Timestamp, required	An ISO9601 timestamp representing the end of the time window of interest. Matching records must occur before this time.
`TTL`	Timestamp, required	An ISO8601 timestamp of when this notification should expire. Subscribers must not process a notification after this time has passed.
`ContactAlert`	Object, optional	If this parameter is present, a contact alert may be raised in response to this notification. This object has the following parameters: **`AlertNotification`** The message to show to a user in an alert (ie. a mobile notification) when a matching record has been found. For example *You may have been in contact with COVID-19.* You may append an additional call to action (eg. *Tap for more information*) as long as it does not change the meaning of the alert and is relevant to medium the alert is delivered through. **`AlertMessage`** A more detailed message explaining to the user what this contact alert means, and what they should do next. This message must be displayed directly to affected users without modification. **`InformationUrl`** A URL that can be visited by the user for more information about the contact alert. This is typically shown behind a “Find out more” call to action or link after a user has acknowledged an alert.

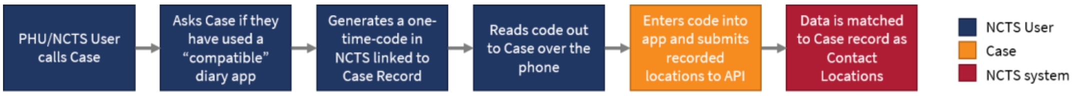
4.3 Push entries from a “digital diary”

When a person is confirmed to test positive for COVID-19 they are called by their local Public Health Unit (PHU). During this call they are informed of their positive test result, and (in subsequent calls) asked for information about where they have been, and who they have been in contact with.

A contact tracer will then undertake an investigation process to trace any close contacts.

To support this effort a person using a ‘digital diary’ app, like NZ COVID Tracer, will be asked if they consent to sharing their diary electronically. If the user consents, they are given a 6-digit alphanumeric one-time-password. This one-time-password is read out to the person over the phone by the contact tracer for the person to enter into their digital diary app.

This authenticates the upload request and allows the data to be linked to the correct case in the national contact tracing solution.


PHU/NCTS User calls Case
Asks Case if they have used a “compatible” diary app
Generates a one-time-code in NCTS linked to Case Record
Reads code out to Case over the phone
Enters code into app and submits recorded locations to API
Data is matched to Case record as Contact Locations
NCTS User
Case
NCTS system

4.3.1 Endpoint specification

This endpoint accepts a POST request with the following parameters

Name	Format	Description
`RequestCode`	String, required	The alphanumeric one-time-password given to the user by a contact tracer. This code must be valid otherwise an error will be returned
`Metadata`	Object, required	An object that contains metadata about the data. This object includes: **`DataFrom`** and **`DataTo`** timestamps that show the window used to select data from. By default this should be the last 31 days inclusive, however may be changed at the contact tracer’s request. It is included so contact tracers have a signal for how complete the uploaded dataset is.
`Locations`	Array of objects, required	This parameter is a list of all recorded location check-ins within the given time window in the Metadata.DataFrom and Metadata.DataTo time window.

		Each recorded location is an object as described in the next table.

Each location takes the following format:

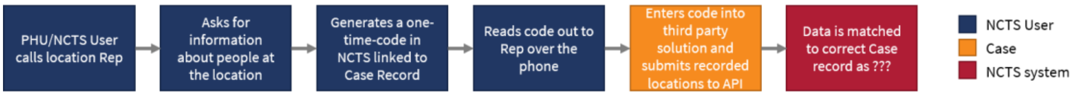
Name	Format	Description
GLN	String, recommended	The 13-digit Global Location Number for the location, obtained from a NZ COVID Tracer poster or other means.
CheckInTime	Timestamp, required	An ISO8601 timestamp representing the time the person arrived or checked-in at the location
CheckOutTime	Timestamp, optional	An ISO8601 timestamp representing the time the user left or checked-out of the location
LocationName	String, required if GLN missing	The name of the location, ideally unique enough that a human reader could identify the location
LocationAddress	String, optional	The physical address of the location, as precisely as possible. Multiple lines can be separated by a newline character.
LocationType	String, required	Either a Business Industry Classification (BIC) code, or a human readable description of the venue
LocationContactName	String, optional	The name of a responsible person who can be contacted by contact tracers if required
LocationContactNumber	String, recommended	A phone number to contact the responsible person. Either this or an email address is preferred
LocationContactEmail	String, optional	An email address to contact the responsible person. Either this or a phone number is preferred

4.4 Publish a visitor register from a location

As part of a case investigation a contact tracer will investigate locations of possible exposure events and may need to make a phone calls to a responsible people at an affected locations for more information. This could include requesting a copy of a visitor register for a particular time period.

If the location is using an integrated third party solution for managing a visitor register, they will be given a 6 digit one-time-password and a time range over the phone to send the relevant data to contact tracers electronically.

This would require integrators to develop an interface for themselves or their customers to enter this code and time window, then use the API endpoint to upload this data to the Ministry.


PHU/NCTS User calls location Rep
Asks for information about people at the location
Generates a one-time-code in NCTS linked to Case Record
Reads code out to Rep over the phone
Enters code into third party solution and submits recorded locations to API
Data is matched to correct Case record as ???
NCTS User
Case
NCTS system

4.4.1 Endpoint specification

This endpoint accepts a POST request with the following parameters.

Name	Format	Description
`RequestCode`	String, required	The alphanumeric one-time-password given to the user by a contact tracer. This code must be valid otherwise an error will be returned
`Metadata`	Object, required	An object that contains metadata about the data. This object includes: `DataFrom` and `DataTo` timestamps that show the window used to select data from. This will be given by a contact tracer and returned to verify the selection window was correct.
`Visitors`	Array of objects, required	This parameter is a list of all recorded location check-ins within the given time window in the `Metadata.DataFrom` and `Metadata.DataTo` time window. Each recorded location is an object as described in the next table.

Each visitor takes the following format:

Name	Format	Description
`Name`	String, required	The name of the person who visited the location
`CheckInTime`	Timestamp, required	An ISO8601 timestamp representing the time the person arrived or checked-in at the location
`CheckOutTime`	Timestamp, optional	An ISO8601 timestamp representing the time the user left or checked-out of the location

ContactPhone	String, recommended	A phone number to contact the responsible person. Either this or an email address is mandatory
ContactEmail	String, optional	An email address to contact the responsible person. Either this or a phone number is mandatory