MINISTRY OF HEALTH
MANATŪ HAUORA

Ministry of Health

COVID-19 Contact Tracing Integration Product (CTIP) Pilot Project

Privacy Impact Assessment

Date 27 January 2021

Document creation and management

This document has been prepared by the Data & Digital Directorate, Ministry of Health.

Consultations with the following have occurred during the development of this document:

- Manager, Data Governance, Data & Digital, Ministry of Health
- Group Manager, Emerging Health Technology and Innovation, Data & Digital, Ministry of Health
- Group Manager, Strategy and Investment, Data & Digital, Ministry of Health
- Programme Manager, Enablers, Data & Digital, Ministry of Health
- IT Security Manager, Data & Digital, Ministry of Health
- The Chief Privacy Officer of the Ministry of Health
- The Government Chief Privacy Officer
- The Office of the Privacy Commissioner

Disclaimer

This Assessment has been prepared to assist the Ministry of Health ("the Ministry") to review the Covid-19 Contact Tracing Integration Product (CTIP) purposes for which information collected via the CTIP mechanism can be used, and the privacy safeguards that are required to manage those purposes.

Every effort has been made to ensure that the information contained in this report is reliable and up to date.

This Assessment is intended to be a 'work in progress' and may be amended from time to time as circumstances change or new information is proposed to be collected and used.

Contents

Section One – Executive Summary - CTIP

1. The COVID-19 pandemic is forcing governments around the world to evaluate how standard public health approaches to managing and controlling infectious disease can be bolstered and augmented by technology.

2. The speed and efficiency of Contact Tracing is one of the most critical factors in a health system's ability to slow or stop the spread of communicable diseases[1]. In the case of COVID-19, it has been determined that under routine conditions of movement and contact amongst the population, the disease can spread too quickly to be contained by traditional Contact Tracing practices alone[2].

3. The Ministry has already identified opportunities to support national Contact Tracing processes by use of:

   3.1. the National Contact Tracing Solution (the NCTS) to support national management of Contact Tracing processes; and

   3.2. the COVID-19 Contact Tracing Application (the CCTA)[3].

4. The CCTA has provided useful information to Contact Tracers, and it is recognised that developing integrations with similar solutions (operated by third parties) would also be beneficial to the Contact Tracing processes.

5. The Contact Tracing Integration Product (CTIP), the subject of this Privacy Impact Assessment, is an additional technology opportunity to support Contact Tracing. It is intended to provide a secure product to industry partners, so they can exchange Contact Tracing information with the National Contact Tracing Solution (the NCTS)[4] when necessary.

6. CTIP will enable Notifications to be sent to, and uploads to be received from approved industry partners (CTIP Partners) who have an appropriate Vendor Solution. These information transfers will occur via a secure CTIP Application Programming Interface (API).

7. Contact Tracers will continue to control the process of identifying what Exposure Events are of sufficient risk that a Notification will be sent via CTIP. Standard Contact Tracing processes will also continue to apply to any uploaded information. The CTIP APIs may be used to upload information, when requested from a Consumer with a Digital Diary or a Location Manager with a Register. The Contact Tracers will use standard questioning processes to identify what the actual risk of exposure was in the case of each Consumer identified in the uploaded information, after discussions with them.

---

[1] *Rapid case detection and contact tracing, combined with other basic public health measures, has over 90% efficacy against COVID-19 at the population level, making it as effective as many vaccines. This intervention is central to COVID-19 elimination in New Zealand:* Dr Verrall,A 10 April 2020: Rapid Audit of Contact Tracing for COVID-19 in New Zealand page 1.

[2] https://science.sciencemag.org/content/early/2020/04/09/science.abb6936
https://www.health.govt.nz/system/files/documents/publications/contact_tracing_report_verrall.pdf

[3] The current version of the CCTA Privacy Impact Assessment can be found here (it is regularly updated).

[4] The NCTS is the IT solution used to support Contact Tracers.

8. The Ministry is developing standards, and a Certification Process, that will enable third party Vendor Solutions to participate in support of the public health Contact Tracing processes, provided that those other solutions can meet the necessary security and privacy standards[5]. They must also be able to demonstrate that they can limit the information to be supplied to that directly related to the risk of exposure of an individual to COVID-19. Vendor Solutions that can meet these requirements will be able to become CTIP Partners.

9. This document assesses the CTIP, and the approach taken to enable Vendor Solutions to integrate with CTIP where Vendors believe this will provide enhancements their customers will value.

10. The current Ministry CTIP Interfaces (APIs) available are:

    10.1. **Digital Diary upload**, recording locations visited by Consumers who have tested positive for Covid-19. This will enable the upload of relevant information for Contact Tracers to review, and to follow up as part of their existing Contact Tracing practices, to identify potential Close Contacts.

    10.2. **Register upload**, recording the Consumers who have visited a specific place (or Location) where an electronic Register was maintained (such as a workplace, or a transport service that keeps a record of travellers on a route).

        10.2.1. This additional information may provide Contact Tracers with the opportunity to identify people at locations where it is unlikely there will be a QR Code, or a site where there are potentially multiple ongoing contacts within a site (such as a building site, construction project or within an office).

        10.2.2. This may also assist in identifying people at locations where they haven't otherwise recorded their location using a QR Code.

    10.3. **Exposure Event notification**, distributing a Location identifier, time window, and corresponding guidance from the Contact Tracing team indicating the action(s) affected Consumers should follow.

11. The Office of the Privacy Commissioner and the Government Chief Privacy Officer have been consulted and are satisfied that the privacy implications of the CTIP, and the related mitigations have been appropriately recorded in this PIA.

Privacy focus

12. The intention of the Ministry has been to retain Consumer choice, minimise the collection of personal information to those matters most directly useful for Contact Tracing purposes, and limit who will have access to that information. It has also endeavoured to

[5] Ministry of Health. 2020. *COVID-19 Contact Tracing Integration Product – Proposed Use Cases and Integrations* is the discussions document that outlines the Ministry of Health's APIs for allowing third party developers to provide data and high-level integration with the NCTS.

minimise any potential privacy risks in its development of the CTIP and balance these against the public health benefits of enhanced contact tracing. Consumer trust is essential if use of the CTIP is to be accepted by Consumer contributors.

13. The purpose of development of this Assessment has been to review the process of collection, storage, use and sharing of personal and contact information associated with the CTIP to ensure that relevant risks are identified and mitigated.

14. This Assessment is to be a 'living' document that will be updated as the CTIP development progresses.

Clarity of purpose

15. The Ministry will incorporate an information statement as part of its web-based COVID information to clarify the role of the CTIP, and record CTIP Partner Vendor Solutions that are to contribute, and in what circumstances. That information statement will include a link to this Privacy Impact Assessment.

Information Collection Processes

16. Neither the Ministry, nor the Contact Tracers will routinely have direct contact with the Consumers associated with the authorised CTIP partners. Each Vendor, prior to becoming an authorised CTIP partner, will be required to demonstrate its Vendor collection processes comply with rule 3[6] of the Health Information Privacy Code, and authorise the proposed CTIP activity (although not necessarily specifically referring to the CTIP by name).

17. Each Vendor Solution, in order to meet CTIP Certification Process requirements, must either already have a Privacy Statement and purpose that supports the collection and use of information for contact tracing purposes, or must implement one to ensure that Consumers are aware of the use to which the information will be put, when that will occur and who the recipients of that information will be (including the NCTS). Ideally, this information will also link to the CTIP information statement for those individuals who wish to know more.

Upload Authorisation

18. In the Digital Diary use case Consumers who are a Case will have the choice of opting-in, if requested by a Contact Tracer, to use the Upload feature and provide their recorded Location and / or activity history.

19. In the case of the Register scenario, the Contact Tracers will be attempting to identify individuals present at a Location of interest. In this use case:

    19.1. the Vendor may hold the record about its own Location(s) and be the Location Manager (for example a large distribution centre, or a transport organisation that maintains records of its own fleet);

[6] Although only contact and identity information is to be provided via the CTIP as these Consumers are being sought due to their potential status as Close Contacts it is considered that this fits within the class of information contemplated by the Health Information Privacy Code.

19.2. alternatively, the Vendor may hold the record on behalf of other organisations, such as multiple different employer Locations where the Vendor holds a centralised Register record. The Vendor in this case is providing a form of tracing service as a product, and controls a central register of information related to third parties.

20. As the records in the Register situation are not directly under the Consumer's control it is particularly important that each of the Vendors is explicit in advising the associated Consumers (about whom the Register holds information) that release of their information to Contact Tracers is a purpose for collection of this information.

21. During the Certification Process for each CTIP Vendor it will be necessary for the specific scenarios to be addressed whereby the Register information holdings may be requested for upload. A decision will need to be made in each case if section 92ZZF is the appropriate basis for the Contact Tracers to request that information be provided – or if the serious threat exception (supported by appropriate provision in the relevant Privacy Statement) will form the basis for the request.

22. There would be no ability to automatically upload the Register by the Vendor without prior personal contact (usually by phone) from the Contact Tracer, to provide the one-time password. This will prevent any 'unnecessary' information holdings being uploaded when there is no risk identified from a case or Exposure Event.

Necessity

23. A key feature that must be addressed is what information is 'necessary' to meet Contact Tracing purposes.

24. Identity and contact details are necessary, as the purpose of Contact Tracing is to identify and manage those who may have been exposed to COVID-19. Contact Tracers are already familiar with expectations and limitations on use and disclosure of personal information obtained for Contact Tracing purposes, whether it is collected under the Health Act or otherwise.[7]. This is consistent with their existing legislative responsibilities under the Health Act to manage this information appropriately.

25. The length of time over which information is collected is relevant. Contact Tracers have determined the 'necessary' time frames for collection of information.

25.1. For the Digital Diary upload, in respect of the recorded details about where the Consumer has been, a time frame up to 60 days[8] has been determined by Contact Tracer clinicians as clinically acceptable (four cycles of the virus) – particularly when the source of the infection is being sought.

25.2. For the Register, this will be more limited in time and extent to an Exposure 'window'.

[7] Section 92ZZG provides that information provided or obtained by a contact tracer under Part 3A of the Act must not be used or disclosed by anyone except for the effective management of infectious disease.

[8] As per the NZ COVID Tracer App PIA. If the Vendor Solution collects a shorter time frame that will also be acceptable – but it may not be longer than 60 days.

25.2.1. Any Register information uploaded must be able to be limited to the relevant time frames and location / place set by the Contact Tracers as being an Exposure risk – and should only include the specific individuals within the relevant Exposure description. The Vendor must be able to select the relevant information from its Register rather than simply uploading a full Register of all names / contacts for all times and locations in an unlimited fashion.

25.2.2. Once the Contact Tracers have been provided with the contact details of potential Close Contacts from selected and relevant Register details they will make contact with those Close Contacts and seek information directly from them.

Access and Security

26. The CTIP will implement robust security and authorisation controls to prevent unauthorised access to information, and encrypt data at rest and in transit.

27. Access to NCTS[9] information requires authentication, and all access is tracked and can be monitored.

28. The only information flows from the NCTS to the CTIP involve the Notification process, and that will be specific to a time and Location when an Exposure Event has occurred.

29. Prior to release, the CTIP will be independently security assessed by an All of Government approved supplier. Findings from the reviews will be remediated where appropriate.

30. Each Vendor that seeks authorisation will need to demonstrate appropriate Consumer authorisation processes as part of the Certification Process.

Future Privacy Impact Assessment Activity

31. Each future use case will be subject to additional Privacy Impact Assessment to confirm appropriate collection processes are in place and that access and security features are of an acceptable standard to connect with the CTIP environment. This document will be updated as CTIP development progresses to enable the Ministry of Health to maintain transparency about the CTIP with Consumers as their personal information is the subject of this project.

Action Points

Action – CTIP Project	**Planned Date for completion**
Interim Certification Process developed with three initial Partners including: • Information collection processes (identifying what can be standardised to all CTIP Partners). • How access to information advice is to be disseminated, including the NCTS, and the Rule 6 and 7 collection processes.	Prior to Go Live Initial Certification for three Partners completed Subsequent Certification Process is to be developed in alignment with overall Ministry

[9] The NCTS has been subject to a full Privacy Impact Assessment which has confirmed access and security controls are appropriate. This will shortly be posted to the Ministry of Health website.

• In the case of Register information holdings, the basis on which a Contact Tracer will request the upload of relevant Register information (s92ZZF or serious threat exception).	programme reviewing Certification requirements
Implement any necessary security testing of the CTIP	Prior to Go Live
Independent Certification & Accreditation process to be completed for CTIP	Prior to Go Live
Successful completion of testing for the integration component of the Vendor Solution	Prior to Go Live by each Vendor
Contact Tracing processes be confirmed and disseminated - in relation to Notification and Upload activities required for NCTS operation of the CTIP processes	Prior to Go Live

Section Two – Operational Details

Background

1. Technology can help with the process of Contact Tracing. The Ministry has worked with the health sector and the community to identify ways of improving access to relevant information, while still respecting individual privacy.

2. The Ministry has created a National Contact Tracing Solution (the NCTS), to greatly increase the capacity and reliability of tracing activity, and to support existing regional expertise. This hold the Contact Tracing records of cases and Close Contacts.

3. Initial key uses identified for technology to support the NCTS included:

    3.1. to enable faster access to the correct contact details for people who may come in contact with COVID-19;

    3.2. to record the movements of Consumers so that if they become infected with COVID-19 they can quickly and accurately identify others who may be Close Contacts or Casual Contacts; and

    3.3. for Contact Tracers to send a Contact Alert to some Consumers who may have been exposed to COVID-19.

4. The CTIP project has identified additional points where technology can assist contact tracing processes as follows:

    4.1. Improving the speed at which Contact Tracers can obtain information about potential Close Contacts at a location with a high transmission risk;

    4.2. Improving security of information holdings, such as avoiding issues created by use of manual tracing registers. Manual registers have a number of potential issues, such as accuracy/legibility of handwritten information, parties sharing a pen (possible risk of infection), and the risk of personal information being disclosed to unauthorised staff or other customers as the material is visible on a page, rather than ‘hidden’ in electronic format. Use of secure API transmission of electronically maintained records (in either a Digital Diary or Register) could enhance the privacy of these information collections; and

    4.3. Creating an additional contact avenue for otherwise unknown contacts at a common Exposure Event (such as public transport). The CTIP could provide a secure, swift and efficient mechanism to transfer information previously not readily available to Contact Tracers.

5. The intention of the CTIP project is that Contact Tracers will be able to use the CTIP product to generate targeted information to support the national case management of positive cases and Close Contacts.

6. In the August community outbreak multiple methods were used to try and locate potential Close Contacts, and notify of potential exposure to COVID-19. Activities included:

6.1. media communication of specific places, or transport journeys, where Consumers may have been in contact with a person who had been infected with Covid-19 at the time; and

6.2. contacting transport providers to identify travellers who may have been exposed.

7. The Ministry is to develop an AWS[10] – COVID Integration Hub and secure Application Processing Interfaces (APIs) – collectively called the Contact Tracing Integration Product (CTIP). The CTIP will enable CTIP Partner Vendor Solutions to share contact and location information, via the CTIP, with the NCTS Contact Tracers.

7.1. All anticipated points of CTIP contact with the NCTS, and with CTIP Partner Vendor Solutions are described in Appendix One of this Assessment.

7.2. In each case, information collected will relate only to situations where a positive case of COVID-19 has been identified, and the information to be made available by CTIP Partner Vendor Solutions will be for the purposes of locating Close Contacts.

Contact Tracing – the Health Act

8. The Health Act provides in Part 3A for management of infectious disease, and Subpart 5 contains the provisions related to Contact Tracing.

9. The purposes for Contact Tracing set out in section 92ZY of the Health Act are consistent with the basis for the CTIP collection of information. These are:

9.1. To identify confirmed and probable cases to enable case management (to identify the source of the infectious disease or suspected infectious disease – s92ZY(a));

9.2. To identify and contact Close Contacts (to make the contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary – s92ZY(b)); and

9.3. To limit the transmission of the infectious disease or suspected infectious disease (s92ZY(c)).

10. Contact Tracers also have the ability under section 92ZZF to approach third parties to request that they provide the Contact Tracer with the names and addresses of the contacts of a case, if known to them. Under section 92ZZF the individuals from whom such a request can be made, for the effective management of infectious disease, include:

10.1. The employer of the Case;

10.2. An educational institution attended by the Case;

10.3. Any business or other organisation that the Case has dealt with; or

[10] Amazon Web Services

10.4. An event coordinator or other person likely to have a list of persons attending an event.

11. There may be some instances where the nature of the information holdings may not fit directly within the wording of section 92ZZF[11]. This will be reviewed for each CTIP Partner during the Certification Process to identify if the Contact Tracers will make the request for information under the serious threat to public health or safety exception.

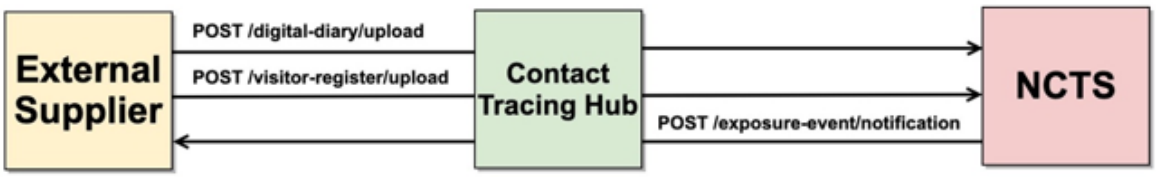
CTIP Processes

12. The CTIP will have three APIs to perform different functions.

12.1. One will enable Exposure Event Notification to be sent by Contact Tracers from the NCTS, via the CTIP, to Consumer, or authorised Vendor, recipients.

12.2. The second will enable Digital Diary information to be uploaded via the CTIP to the NCTS, after the Consumer chooses to Upload the information.

12.3. The third will enable Register information relevant to a notified Exposure Event to be uploaded via the CTIP to the NCTS, provided there is either a Consumer authorisation process in place, or a Contact Tracer request to the Location Manager under section 92ZZF.

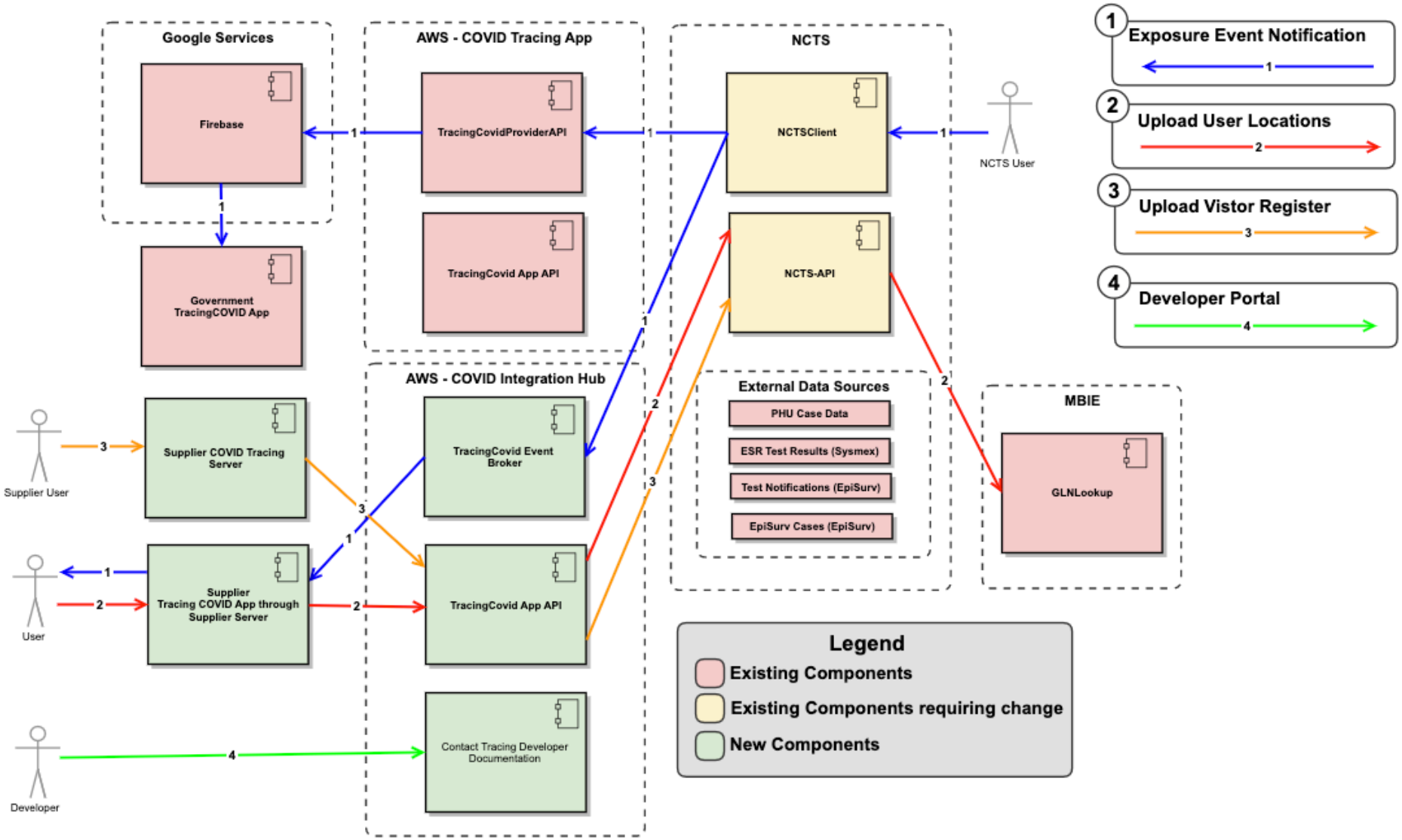


Data Flows

13. The following diagram shows the expected information flows:

[11] Essentially, under s92ZZF, a Contact Tracer can ask a location manager (who is an employer of a Case, an educational institute the Case attends, a business or organisation the Case has dealt with, or is a person who is likely to have a list of persons attending an 'event') for the names and addresses of the contacts known to the location manager. Presumably if the information holdings available to the location manager disclose the details of the 'contact' this information will fit within the 'known to' requirement. It is not clear, if the information holdings are centrally held by a CTIP Partner who is not a location manager, whether s92ZZF will apply on its wording. This request may need to be made under the 'serious threat' exception.

Proposed COVID Contact Tracing App System Context View



14. The green boxes in the lower left show the new use case interactions and the components of the CTIP Hub. The Contact Tracing Developer Documentation will be stored in the lowest green box – and available to developers to identify the latest standards and requirements that must be met. This will include the Certification Process requirements.

15. The Exposure Event Notifications that flow out from the NCTS (as authorised by the Contact Tracers) are shown in blue. These signal the existing Covid Tracer App pathway (boxes in pink) and the proposed new Notification process via the CTIP Hub to the API for the authorised Vendor with a Digital Diary product, and to the Vendor Register server (which may not receive Notifications in all instances – this will be determined during the Certification Process).

16. The options for upload are signalled in red for the Consumer user, and yellow for the Register scenario (the Location Manager will control the information upload in the Register scenario). Each of the upload options will be initiated by the Contact Tracer contacting the Consumer or the Location Manager and providing a unique one time password to allow the upload to occur, so the information can be identified when the information is received into the NCTS environment.

17. Appendices Two to Four of this Privacy Impact Assessment contain additional information in relation to the use cases.

Information distributed

18. In the case of the Notification processes no personally identifiable information will be included directly in the alert messages sent.

19. The Consumer Digital Diary Notification case will be aligned to the process already in place with the COVID Tracer App[12].

    19.1. The Digital Diary option is for mobile applications where information is stored locally on the device and is not transmitted to a central data repository.

    19.2. A Notification will be sent to the Consumer's device. This message will transit the CTIP hub to the Vendor server, and then be distributed to linked Consumer devices. If the Consumer holds a matching Location and time on their device, the device screen will display a message relevant to the potential contact, with some limited advice to that individual Consumer.

20. Notification to a Register user will be aligned to the processes set out in Appendix Three.

Information Collected – Uploads

21. The CTIP Proof of Concept API Integrations confirms the intent that any data collection should be minimised as much as possible. '*…the Ministry will not create a central database of the public's movements and close contacts. This information would only be*

[12] COVID TRACER APP PIA (this can be found on the Ministry of Health website in the 'Privacy and security for NZ COVID Tracer' section)

collected from people who have, for example, tested positive, are a suspected close contact, or a suspected casual contact.'[13]

22. The upload process (sending information via the CTIP to the NCTS) will involve a 'collection' of information about Consumers. Each of these 'collections' will be in response to a Consumer becoming a Case (for the Digital Diary upload) or an identified Exposure Event - someone who has tested positive for COVID-19 was at a Location (on a specified date and time) and there may have been exposure for Close Contacts.

23. The upload response may be either:

    23.1. the upload of a Consumer's Digital Diary – or not, at the Consumers choice, when they are identified as a Case; or

    23.2. upload of a Register extract by a Location Manager, (noting the Vendor may also be a Location Manager if the information in question is about a Location they are responsible for).

        23.2.1. This information will detail potential Close Contact interactions within the Exposure Event 'window' of time and location specified by the Contact Tracer.

        23.2.2. That upload must be part of the Consumer expectations associated with the Register use.

        23.2.3. The upload process will be initiated by the Contact Tracer in direct contact with the Location Manager (who will then authorise the release with the one time password provided by the Contact Tracer).

24. The 'upload' process will involve personally identifiable information collected onto the NCTS via the CTIP. This will include the following (based on the understanding that only 'necessary' information will be uploaded):

Information Field* *All of the following information fields will be uploaded if the device or register holds the information (subject to settings that will limit the information collection to the relevant time periods or Exposure Events)	**Purpose for collection**
Digital Diary (this will relate to the Location check-ins or manual entries for a Case who agrees to upload their Digital Diary). Information is only transmitted to NCTS (via the CTIP) with consent of the Consumer. The time frame of data uploaded will be set after clinical advice – it is currently up to 60 days maximum.	
One time password	To link the upload to the relevant NCTS Case file
If held on the App on the device: information about the Consumer including first, middle and last names and date of birth	To confirm identity of Consumer

[13] Section 2.3 of the COVID-19 Contact Tracing Integration Product Proof of Concept API Integrations Version 1.0 8 July 2020

All recorded Location check-ins within the specified time period • This will include the GLN for each location (and contact details of the relevant location) • If Location does not have a recognised GLN then other business identification and contact details will be collected where available	To identify Locations where other Consumers may have been exposed to the Case (or other Consumers if recorded in the Manual entries) Contact details for those GLN Locations (or other identified Locations) would be identified so Contact Tracers could make contact and identify other possible Contacts with the Case
The time the Consumer checked in to the Location and the time the Consumer checked out of the Location (the check out time is optional)	To assist in identifying the Exposure Event time frame during which the Consumer may have been in contact with the Case
Free text comments made by the Consumer	These comments will be reviewed for discussion with the Consumer by the Contact Tracer to identify additional potential contacts of the Case or Locations visited
Register Upload (will relate to dates for the start and end times of the Exposure Event at a specific Location where a CTIP compatible Register was in operation)	
One time password	To link the upload to the relevant NCTS Case file
Name of the Consumer who visited the Location	To identify the Consumer so the Contact Tracer can make contact
The time the Consumer checked in to the Location and the time the Consumer checked out of the location (the check out time is optional)	To assist in identifying the Exposure Event time frame during which the Consumer may have been in contact with the Case
Either the phone number or an email address for the Consumer	To provide a contact method by which the Contact Tracer can contact the Consumer

25. Digital Diary information and Register information Uploaded via the CTIP APIs will transit the CTIP and be passed to the NCTS via a 'gateway' that will enable the uploaded information to be stored against the relevant Case record in NCTS. As each Upload is assigned a unique one time password by the Contact Tracers they are able to identify the relevant information upload within the NCTS environment.

26. Register use cases will enable matching of the 'Register' held for a 'Location' (such as a workplace, or a bus travelling a set route) against a set date / time window to identify individuals present (the Close Contacts).

    26.1. Contact will be made with the organisations maintaining a CTIP connected Register, individually by Contact Tracers to obtain a specific and identifiable dataset held by those organisations. This is consistent with the ability of Contact Tracers to make a request for Close Contacts under s92ZZF of the Health Act.

    26.2. The information requested will be directly related to a Case[14], at a specific location (including a vehicle such as a bus, with a GLN) on a date and time that is designed to cover the relevant Exposure Event time frame. It is to be

[14] Without identifying who the Case is – only the GLN and time frame for the Exposure Event will be advised

limited to the information 'necessary' for the Contact Tracer purposes to identify potential Close Contacts.

26.3. A one time password (OTP) will be provided by the Contact Tracer to the Vendor to enable the relevant information to be forwarded electronically to the Contact Tracer via the CTIP to the NCTS.

Use of Information: Data Storage, Retention and Access

Use of Information

27. The use of the information collected via the CTIP is directly related to contact tracing processes, specifically identifying and contacting Close Contacts.

28. Data Standards and specifications that have application to CTIP include:

28.1. Covid-19 Contact Tracing Data Standard HISO 10085:2020 Draft standard published 21 May 2020 (Contact Tracing Data Standard).

28.2. Covid-19 Contact Tracing QR Code Specification – Data format and implementation specification published 21 May 2020 (QR Code Specification). This relates to the QR Codes used to identify Locations.

28.3. Covid-19 Contact Tracing Integration Product – Proof of Concept API Integrations (CTIP Proof of Concept).

29. Any Vendor Solution will need to successfully complete testing for any integration with the relevant CTIP API, to confirm compliance with the relevant requirements in relation to that integration.

CTIP Security

30. No personally identifiable information will be stored on the CTIP. Uploaded information will be encrypted in transit via the CTIP, and will be encrypted in storage within the NCTS environment.

31. A cache of Exposure Events will be held, until the CTIP connected Vendor system has retrieved them. This Exposure Event information is not identifiable to a person, and is typically also published publicly on the Ministry of Health website.

32. Prior to implementation the CTIP will undergo an independent security review by an All of Government approved supplier. Findings from the review will be remediated where appropriate. Future significant API releases or CTIP product updates will also be independently assessed to the same standards.

33. The CTIP is hosted on Amazon Web Services (AWS) with two availability zones in the ap-southeast-2 (Sydney) region. This is a Ministry-owned sub-tenancy of the main Ministry of Health AWS tenancy, which enforces a number of security, audit, and policy controls.

34. .Data stored within AWS is encrypted. The Ministry controls access to the encryption keys and the data. Security and authorisation tokens will be used for API and NCTS communication.

NCTS Security

35. The NCTS Upload destination is the already- established National Contact Tracing Solution database and is subject to existing storage, access and retention requirements.

36. Full details of the data access and controls in place for NCTS are covered in a separate Privacy Impact Assessment for the NCTS[15]. In summary:

    36.1. The NCTS is made up of a number of components, including a rules engine, integration and AWS capability. Salesforce Service Cloud (Service Cloud) is the Salesforce customer service and case management Software as a Service platform. Service Cloud provides the core platform that supports all core capabilities of the NCTS.

    36.2. The Salesforce Service Cloud instance is served from Amazon Web Services (AWS) Cloud infrastructure based in Sydney, Australia.

    36.3. Information stored in the NCTS is covered by the NSS Data Policy, this aligns with the relevant HISO standards, including HISO 10029:2015 Health Information Security Framework, and the New Zealand Information Security Manual.

NCTS Retention

37. Identifiable Information is not retained in the CTIP. The only information that may be held on the CTIP product will relate to Notifications set by the Contact Tracers. These will contain information equivalent to that entered onto the Ministry website as notification of potential Exposure Event.

38. Information that transits the CTIP APIs and is sent to the NCTS will be securely stored under the following retention requirements in the NCTS:

    38.1. Digital Diary data and Register data uploaded will be retained in a secure location within the NCTS Salesforce platform (as a Case linked object – essentially a list that can be queried by the Contact Tracers) but will not be transferred into a NCTS case record unless a Contact Tracer determines it is relevant to an Exposure Event or Contact.

    38.2. Contact information extracted by a Contact Tracer from CTIP information submitted will be added to an NCTS case record only after confirmation with the Consumer concerned.

[15] The NCTS PIA will shortly be loaded to the Ministry of Health Website

38.3. Any information, including Location Information, not transferred into an Exposure Event or Contact record will be securely deleted on a regular basis (within six months of submission to the NCTS).

38.4. Identifiable Consumer information recorded in the NCTS will relate to one of the following categories:

- Related to an individual who has, or is a probable case of, COVID-19 (an NCTS case record) which is stored in the NCTS as part of the pandemic case management system; or
- Related to an individual who is identified as a Close Contact or a casual contact, within the exposure 'window' set by the Contact Tracers.

38.5. Information retention policies are fully detailed in the NCTS Privacy Impact Assessment, but in summary:

Information to be deleted within six months of collection: data that is not used as part of active Contract Tracing
Digital Diary and Register details uploaded to NCTS via the CTIP that are not incorporated into a NCTS case file as an Exposure Event or potential Contact.
Retained for two years post creation of the record
Any tracking and auditing information of User access within the NCTS.
Retained for the duration of the pandemic (until the COVID-19 Public Health Response Act 2020 is repealed)
Close Contact and Exposure event files – incorporating CTIP details, where the Consumer does not go on to develop COVID-19
Retained as a 'health record' for minimum of 10 years
Case records for confirmed cases that are a record of the disease (these are not clinical treatment records but are considered health records). These records will include the individual case name, identification and contact details, NHI, test result, daily check in records (record of the disease), Exposure Events and Close Contacts.
These records will also be retained for a probable case that becomes symptomatic.
It will be important to also retain a master record of the disease, which may need to be separately held after the end of the pandemic (this may need to be used for future immunisation, or location of those individuals known to have been infected if it is identified there may be additional health treatment repercussions in future).
Research and planning
Non-identifiable (or de-identified) information may be retained, to be used for purposes related to the public health response to COVID for as long as that information remains relevant for those purposes. Ideally a non-identifiable dataset for epidemiological data will be retained, which would include exposure event and close contact information to enable effective management of infectious disease as contemplated by the Health Act Part 3A.

Statistical Information

39. Statistical information collected about the use of the CTIP will be accessible to relevant Ministry staff and its suppliers, in order to make decisions about the features and functionality of CTIP. This information does not identify any individual Consumer, nor will Consumer personal information be accessible in this way.

40. Statistical information will include the number of:

    40.1. Exposure event notifications sent

    40.2. Digital diary uploads received

    40.3. Digital diary upload lines received

    40.4. Register uploads received

    40.5. Register upload lines received

Governance

41. Governance of the programme, and therefore the collection, management, authorised use and deletion of information, has a number of components to manage and maintain oversight of information arising from the CCTA processes:

    41.1. The COVID-19 Response: Technology Governance Group will perform the overall governance function, and the COVID-19 Response: Technology Steering Group will manage operational matters.

    41.2. The Senior Responsible Officer for Data and Digital's COVID-19 response

    41.3. The Business Design Council. This includes a sub-set of members from the Digital Investment Board, a Clinical Leader and Ministry (non-Data & Digital) employees.

42. Additional governance support of the CTIP programme will be developed as part of the Certification Process the Ministry is working on. This support will be provided in the form of operational controls, and enable CTIP Partners to evidence appropriate requirements have been achieved.

Section Three - Privacy Analysis

The Ministry has endeavoured to balance strong Consumer interests in privacy and autonomy with the potential for provision of additional identifiable Contact information to support of the Contact Tracing COVID-19 pandemic response. The CTIP will enable the amalgamation of relevant personal and contact information for Contact Tracing related purposes. Each contributing CTIP Partner will have a collection of Location or personal interactions that may assist to identify Close Contacts of a case of COVID-19.

The Ministry remains aware of the importance of Consumer trust, and has endeavoured to manage the balance of interests by:

- limiting the occasions on which information is sought to those where there is an actual risk of Contacts being in proximity to a Case. It is the expressed intention of the Ministry to only collect information via the CTIP when 'necessary': '*…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'.* The method by which the 'necessity' is determined is driven by the Contact Tracers, who decide whether it is appropriate for Digital Diary details to be requested, or when a notification to those who may have been at a location is required.

- requiring each CTIP Partner to meet certain requirements, in a Certification Process. It will be a requirement that each CTIP Partner establish that the use of the information they will supply to CTIP (when necessary) is consistent with the expectations of the Consumers whose information is involved. CTIP Partners will be required to meet the rule 3 collection processes before becoming authorised CTIP users, to ensure that Consumers they represent are informed about the potential CTIP use of their information.

- Conducting this Privacy Analysis during the proof of concept stage of the development to enable consideration of relevant privacy and security issues at an early point in the development of the CTIP.

The Ministry has conducted its analysis under the Health Information Privacy Code as the information is ultimately about individuals who may test positive for COVID-19, are a probable case of COVID-19, or may be a Close Contact of a person with COVID-19. Under clause 4(1)(e) it is considered that this could be information about an '*individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual'.* The Ministry has therefore chosen to analyse the high standards associated with health information in the HIPC for the purposes of this Privacy Impact Assessment.

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 1	Purpose of collection of health information - Only collect health information if you really need it	The purpose of collecting information via CTIP upload processes is to assist with Contact Tracing activities as part of the COVID-19 pandemic response. This includes the purposes set out in s92ZY of the Health Act: • identifying the source of the infectious disease • making contacts aware that they too may be infected, encouraging them to seek testing and treatment if necessary; and • limiting the transmission of COVID-19 Identifiable information is required to meet these purposes. The type of information being contemplated for collection under the CCTA is aligned with that addressed under Part 3A of the Health Act,	The Notification processes via the CTIP are not a collection of information, but are aligned to the purpose of enabling Consumers to be made aware that they may have been in Contact with a Case, and providing appropriate advice to help them keep themselves and others safe.	*Purpose* Collection via CTIP upload of this Digital Diary Contact and Location information related to a positive COVID case is for the lawful purposes of the COVID-19 pandemic response. This involves Contact Tracers obtaining information from Cases about potential Contacts of COVID-19 positive individuals. This includes: • identifying Locations where an Exposure Event may have occurred (if the individual has chosen to opt in to the Location-related recording facilities on their App of choice); or • identifying potential Close Contacts using Digital Diary entries as a prompt. The Digital Diary information can be used as a memory aid to Consumers (if they choose not to upload it) or as an uploaded list of information to help the Contact Tracer to identify Locations, and therefore potential Close Contacts. *Necessary*	*Purpose* Collection of Register Contact and Location information is for the lawful purposes of the COVID-19 pandemic response. This involves Contact Tracing to identify individuals who may have been present at an Exposure Event, and who are therefore contacts. Contact Tracers will make contact with the relevant Location Manager who will be either: • the Vendor (if the Register relates to a Location where the Exposure Event occurred and they are the Location Manager) or • the relevant Location Manager if a Vendor Solution relates to multiple Locations. The Contact Tracer will request the provision of potential Contacts who had been at the Location during the relevant Exposure Event window of time. This will be using the process determined during the Certification Process.	**Low**

		subpart 5 – Contact Tracing. In the case of a Register upload this will be based on either a direct request under section 92ZZF from a Contact Tracer, or the exception as a serious threat to public health or safety (if that has been identified as applicable during the CTIP Certification Process). The Digital Diary collection will not be under those powers but will be a collection on a voluntary basis of the range of information authorised under the Contact Tracing provisions. Contact Tracing involves 'ascertaining the identity' of each of the Case's contacts – s92ZZ(a). Location information (place, date and time) is aligned to the information a Contact Tracer may require under Health Act clause 92ZZC(3) if an individual has, or is a probable case of, COVID-19, as being 'information about the circumstances in which he or she believes that he or she contracted, or may have transmitted, the infectious disease'.		The Location and Digital Diary data is necessary for Contact Tracing purposes to enable Consumers to more easily recall events where the Consumer may have interacted with Close Contacts, or Locations where Close Contacts may have congregated, and to support Exposure Event Notifications. *Limiting collection of data fields*: Part of the Certification Process requirements will be to set a maximum dataset that may be collected – only those fields determined as relevant and necessary (in consultation with the Contact Tracers) will be incorporated into the CTIP collection process. This will assist to minimise the amount of information collected. *Time limitations*: A cap of a maximum of 60 days-worth of Digital Diary records is part of the CTIP Digital Diary Certification Process requirements. This equates to four cycles of COVID-19. This timeframe is to assist with identification of the source of an original infection (and has been determined by the Contact Tracing clinical team). No dataset longer than this timeframe is to be collected by the CTIP (although some Vendor Solutions may only retain records for a shorter time frame – and only that shorter period will then be collected). One potential challenge created by any free field text entries for the CTIP Partner Digital Diary product is that individuals can put as much	• This may be a direct request under section 92ZZF where the '*names and addresses of the contacts'* of the case are known to the Location Manager. • If the information holdings are centrally held by a CTIP Partner who is not a Location Manager, the request may need to be made under the 'serious threat' exception. • If the only contact details available on the Register are emails, then it is suggested that the serious threat exception be used to make the request as appropriate. *Necessary* It is noted that the Register upload will record Consumers (and their contact details) who were at a Location, or may have been in contact with a Case within a limited window. No information other than names and contact details for Consumers meeting that date and time frame would be included in the upload. The upload will also need to be limited to the relevant time period. It will be part of the Certification Process requirements that	

		Limiting data collection The opportunity for review and challenge will be provided by reference to the Office of the Privacy Commissioner prior to adding new development features to ensure only data aligned to these purposes is collected. **Data Governance:** The Ministry Data Governance Group will provide oversight of the use of the data to ensure that any proposed future use matches the purpose.		information as they wish (up to the character limit) and are not constrained in the information they wish to include. Some individuals may put personal comments about themselves or others that they may not wish others to see. This could result in information not 'necessary' for the Contact Tracing purposes being collected (if it was Uploaded). There is however a significant mitigation feature is that the Digital Diary information will not leave the Consumer's device for review by a Contact Tracer unless the Consumer chooses to Upload it in response to a Contact Tracer Request. Part of the Contact Tracer training will be to reinforce with the Consumer that it is optional to Upload the information (but that if the Consumer does choose to Upload, that all Digital Diary information – both scanned Location and manual entries - will be uploaded).	Vendors establish that these limits will apply to any upload of a Register.	

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 2	Source of information - Get it straight from the people concerned	The CTIP process collects Digital Diary and Register information uploaded via CTIP Partner product integration tools. Compliance with Rule 2 can be achieved by collecting information directly from the individual Consumer, as with a Case / Contact Tracer discussion where the Case chooses to directly upload the Digital Diary. Even if the Consumer does not agree to Upload the information from their device it could be used as a reminder to the Consumer in their discussions with the Contact Tracer. Compliance can also occur if the Consumer authorises collection from someone else, having been made aware of the matters set out in Rule 3. • The Certification Process will be designed to require that before being approved as a CTIP Partner that each Vendor will have	The collection of information to enable Contact Tracers to determine when to make a Notification, and what to include in the text, relates to the Contact Tracing processes. These are set out in the NCTS PIA, and not further addressed in this PIA. The CTIP Notification process itself does not collect information – it sends it. • The Notification process does not have an embedded call back option for Consumers to receive a call from Contact Tracers (in contrast, this is enabled in the COVID Tracer App – where the Ministry has developed this facility within that App design). This feature would have required identification details to be added as part of the call back – but will not be implemented at this stage into CTIP processes. • There is no automatic Notification response where the CTIP Partner will respond with an upload of key information related to a Notification. No uploads are to occur without an authorisation process consistent with Rule 3 collection processes. This is a Certification Process	Most information collected via digital diary upload is collected with the authority of the individual concerned (they authorise the upload via the CTIP process via Rule 2(2)(a)). There may be instances where information about third parties is collected if individuals have recorded information about others in their manual digital diary entries. In those circumstances, information about the other individuals will be collected in reliance on rule 2(2)(d) – as compliance is not reasonably practicable. It is also consistent with the information that will be collected from a positive case about their contacts. Section 92ZZC(4) confirms a case may be required to provide the name, age, sex, address and other contact details of each contact. In addition Rule 2(2)(c) provides an exception where compliance would prejudice the health or safety of any individual – in this instance it is in the interests of the Close Contact to be contacted by a Contact Tracer and advised '*that they too may be infected, encouraging them to seek testing and treatment if necessary*' in accordance with s92ZY of the Health Act..	Any Register upload by a CTIP Partner will be required to comply with Rule 3 collection processes – and confirm authorisation to Upload any identifiable information from Consumers (in accordance with Rule 2(2)(a)). This will be part of the Certification Process. In addition, a request will be made under the authority of s92ZZF to a Location Manager (or under the serious threat exception if identified as appropriate during the Certification Process).	

		ensured that they have a Rule 3 compliant collection / authorisation process for any upload activity they will undertake. This will be of particular importance to the Register upload. • It is not reasonably practicable for the Contact Tracers to identify Consumers listed on a Register when they are unable to identify who they are until the information is uploaded.	requirement for any CTIP Partner.			

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • **Notification**	Key Controls • **Digital Diary Upload**	Key Controls • **Register Upload**	Residual risk
Rule 3	Collection of information from individual - Tell them what you're going to do with it	This collection process requirement will be a key feature of the CTIP Partner Certification Process. In order to support trust in the Contact Tracing process all contributing components (including the CTIP) need to be carefully managed to ensure Consumer trust is established and maintained. Failure to do this may result in reduced cooperation by Consumers – which will be detrimental to Contact Tracing activities, and increase the risk of outbreaks not being promptly contained. The Certification Process will require each CTIP Partner to take all reasonable steps to ensure any Consumer involved in use of the CTIP contributing solution is aware that: • information is being collected, • the purpose of the collection (including the CTIP processes), • the intended use, and users of the information (including the information recipients –the NCTS) • the processes for access to and correction of information, • The retention periods that will apply The Consumers must also be made aware: • of the name and address of the collecting agency and the agency that will hold the information in the case of the upload processes (NCTS), • that the supply of the information to the CTIP is voluntary (including any consequences for the Consumer if the information is not provided) It can reasonably be assumed if a Consumer has opted in to use Vendor Solution features that explicitly include the CTIP Processes (or opted not to opt out when advised of the potential for their information to be used in CTIP processes) that the Consumer accepts the CTIP processes will apply to their information. If the supply of information becomes mandatory under section 92ZZC of the Health Act the Contact Tracers will engage with the affected consumers directly, outside of the CTIP process.			**Low**

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 4	Manner of collection of information - Be considerate when you're getting it	The CTIP Partners must not collect personal information by unlawful, unfair or unreasonably intrusive means. The proposed processes will be reviewed as part of the Certification Process, and CTIP Partners requested to demonstrate compliance to the Ministry – particularly in relation to children or young persons. For comparison, the Ministry has included the following in the Privacy and Security Statement: '*If you are under 16 years old you may choose to use the NZ COVID Tracer app. Please note, however, that if it becomes necessary for a Contact Tracer to contact you they may need to ask your parent or guardian to provide any necessary information for you.*' Any upload of a Digital Diary will only occur after a contact by a Contact Tracer. If information was uploaded as part of a Register and information about a young person was included it would be the responsibility of the Contact Tracer to manage the interaction when they made contact to discuss the matter with the young person. Information from under 16 year olds would be managed by Contact Tracers consistently with section 92ZZC(5) of the Health Act. This enables the Contact Tracer to seek any necessary information from a parent or guardian if the individual is under 16 years of age if that is considered appropriate.				

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 5	Storage and security of information - Take care of it once you've got it	Personal information is held and managed in accordance with the Privacy Act and Health Information Privacy Code. Each Vendor will be required to comply with Ministry prescribed security standards before becoming a CTIP Partner. Uploaded data will be held securely within the NCTS, within the strict controls applied to that solution. The NCTS operates on Salesforce Service Cloud on a secure AWS platform based in Sydney. The CTIP application will be required to pass the Ministry Certification and Authorisation Process as well as an independent security review before commencing operation.	Prior to go live the CTIP will be independently security and penetration tested, and the Ministry will take steps to remediate any identified issues. The CTIP product is hosted using the secure Ministry Amazon tenancy, and will be subject to standard Government cloud environment controls. No information (other than Notifications) is stored in the CTIP. All information that transits the CTIP is encrypted in transit. Notifications sent do not include any personally identifiable information. All Locations are also published on the Ministry website (so the Notification information can be identified independently of the CTIP Notification) The NCTS security has been reviewed in the NCTS – Contact Tracing PIA This document is available on the Ministry website.			

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • **Notification**	Key Controls • **Digital Diary Upload**	Key Controls • **Register Upload**	Residual risk
Rule 6	Access to personal information - People can see their health information if they want to	It is recommended that the Certification Process require Vendors to demonstrate how these Rules will be met in relation to the CTIP processes. This would require the Vendors to have appropriate processes for access to and correction of personal information which are consistent with Part 4 of the Privacy Act 2020. The Vendor must also advise the Consumers using their product about these processes, including: • where to make a request for information, (and a process internally if any request needed to be transferred to the NCTS); and • how to make a request for correction of information. The Ministry will not hold identifiable information in CTIP but it will hold uploaded information in the NCTS. This will need to be incorporated into the rule 3 collection process information.				**Low**
Rule 7	Correction of information They can correct it if it's wrong					

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 8	Accuracy etc. of information to be checked before use - Make sure health information is correct before you use it	Much of the information to be obtained by NCTS via the CTIP upload process will be unverified. It will be attached to an NCTS Case or Exposure Event file if uploaded. The format of the upload will however essentially be a list that must be reviewed and verified by the Contract Tracer – after direct communication with the Consumer concerned. Information will not be added to an NCTS Exposure Event or Contact file until that verification has taken place to establish the accuracy of the information. Ultimately, a balance has been struck (between accuracy and retention of consumer choice and privacy) that appears acceptable in the context of Contact Tracing activity. There are some steps to assist in ensuring information is accurate and up to date prior to use:	The Ministry does not have full control over allocation and use of the QR codes, which will be used to initiate Notifications. There are multiple processes to obtain the QR code, two of which are operated by the Ministry and these rely on information provided by the QR code requester. The Ministry does not control accuracy in the use of QR Codes by Locations (for example for a single organisation using one code for multiple Locations instead of a different code for each Location). In each case, however, the submitted NCTS Location information will be reviewed by a Contact Tracer who will ask further questions of the Consumer and verify the correct information (as far as is possible). There is also the challenge of over or under reporting of EEOI in terms of the number of Notifications generated. Too few (or too narrow an assessment of the Events to be included or the time frames to be applied), and those at risk will not receive a Notification. In contrast, too wide a range of events and times, and high levels of anxiety, and potentially needless self-isolation, could occur. The involvement of experienced clinicians in determining whether an Event has genuine risk of Exposure will help to limit these risks. A small number of authorised users with clinical	The CTIP will have no control over the accuracy / completeness of the data Uploaded as a representation of a Consumers movements. Digital Diary information will be subject to the accuracy and completeness of the information provided by the Consumer. Consumers could choose not to provide all information. The Consumer may not scan all venues they attended, because they chose not to, they forgot or that venue did not display a QR Code. This also applies to manual Digital Diary entries It can be reasonably assumed that Consumers will provide details that are true and correct. In the event that it is not correct, or the information submitted becomes out of date, the information will be confirmed by the Contact Tracer with the relevant Consumer before further use. Information that is not verified by the Contact Tracer will not be moved into an Exposure Event or Contact file, and will be deleted from the NCTS file upload location within 6 months.	Contact Tracer Review will be used to ensure the information uploaded as part of a Register is accurate and matches to the correct person before use (where possible – if contact details provided for a Consumer are incorrect, the Consumer may not be identifiable until the Consumer has been located by other means). The Contact Tracer will contact the list of individuals who were recorded in the upload file as being at a location during a target time frame – they can directly verify with them the accuracy of the information about them, including contact details and movements. Information that is not verified by the Contact Tracer will not be moved into an Exposure Event or Contact file, and will be deleted from the NCTS file upload location within 6 months.	

			expertise will make the final decision on what Exposure Events to notify. This will enable a nationally consistent application of clinical oversight to best meet the balance between under and over Notification.			

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 9	Retention of information - Get rid of it when you're done with it	This PIA does not address the retention of information by the CTIP Partners for their existing Vendor Solution, it only addresses the information that will be collected onto the NCTS via the CTIP. If information uploaded is incorporated into an Exposure Event record or Contact record by a Contact Tracer, then any uploaded information will be deleted at the end of the pandemic (noting however that aggregated and statistical information may be retained in a non-identifiable format to assist with public health research and analysis, and for future planning purposes). Uploaded Location data that is not considered by a Contact Tracer to be a potential Exposure Event, nor a potential Contact, will not be entered into the NCTS. The remaining upload information will be deleted from the uploaded file on a regular basis – currently	Notifications will persist	If the Digital Diary information has become part of the Consumer's NCTS Case record it will then be subject to retention requirements within the NCTS. Once transferred to the NCTS any 'health record' details for a Case will be stored in accordance with the Health (Retention of Information Retention) Regulations 1996.[16] All other information will be deleted at the end of the pandemic	If the Register information becomes part of an NCTS Case record it will then be subject to retention requirements within the NCTS. Once transferred to the NCTS any 'health record' details for a Case will be stored in accordance with the Health (Retention of Information Retention) Regulations 1996.[17] All other information will be deleted at the end of the pandemic	

[16] http://www.legislation.govt.nz/regulation/public/1996/0343/latest/DLM225616.html
[17] http://www.legislation.govt.nz/regulation/public/1996/0343/latest/DLM225616.html

		planned as a 6 month rolling deletion.				

Health Information Privacy Code Rules		**Solution Details and commentary**	**Key Controls** • **Notification**	**Key Controls** • **Digital Diary Upload**	**Key Controls** • **Register Upload**	**Residual risk**
Rule 10	Limits on use of information - Use it for the purpose you got it	Consumer information uploaded via the CTIP will only be used for the NCTS related purposes of the COVID-19 pandemic response. The use of the Vendor applications may be for wider purposes than the CTIP purposes. Clear parameters must be placed around the CTIP use of information – and this must be conveyed in a clear and easy to understand manner to affected Consumers to avoid confusion. The Certification Process must require the CTIP Partners to clearly establish all purposes for which their solution information will be used, including CTIP uploads, and specifically detail these as part of their Rule 3 collection processes. It can reasonably be assumed if a Consumer has opted in to any of the CTIP Partner features (or opted not to opt out when advised of the potential for CTIP use) that the Consumer is in agreement with the proposed CTIP uses associated with those features. Data Governance will be an important feature of ensuring the potential for function creep is limited. This control will be directed at the NCTS use of the information. The Ministry does not have end-to-end control of some of the CTIP Partner processes, and their products may have been developed for purposes different to those solely focussed on NCTS related contact tracing. It will be important to establish a governance structure that remains informed about CTIP partner activity, and with the ability to remove a CTIP Partner if concerns arises about their activities (including expansion of purpose for the underlying solution). It is understood that the Ministry contract with each CTIP Partner contains terms that will require any CTIP Partner to advise the Ministry if it is to make '*any material changes to the application or supporting processes that impact on: the data collected; how this is secured or transmitted; the privacy statement; build quality; alignment with required standards and specifications; or which could be perceived as detrimental to the end user experience, they will be required to seek approval from the Ministry in advance of these changes. Failure to obtain approval may result in certification of the application being revoked'***.** This will become part of the Certification Process.			

,

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 11	Limits on disclosure of information - Only disclose it if you have good reason	Consumer information received via CTIP upload will be disclosed by Contact Tracers only for use by the public health system in relation to the COVID-19 pandemic response, for purposes related to Contact Tracing. This will be consistent with the required Rule 3 collection information. If relevant to a Consumer who has tested positive for (or is a probable case of) COVID-19, information uploaded via the CTIP processes may be incorporated into a Consumer's NCTS case record. This will include contact details and relevant Digital Diary information provided. Any interactions following engagement with a Contact Tracer will be governed by the Health Act provisions related to Contact Tracing, and / or in a manner consistent with the Privacy Act, and are beyond the scope of the CTIP. The Data Governance Group will provide oversight of the use of the CTIP upload data to ensure that use matches the purpose Only those required to have access to the data for COVID-19 Contact Tracing related purposes will have access. This will be enforced by Ministry policy and subject to audit monitoring of logged access activity. It is also noted that it is common practice for the Contact Tracing team to add Exposure Events to the Ministry website, so in the event a notification was received via the CTIP for a workplace or similar where it might be possible to identify who could have been a Case or a Contact that information will already be publicly available.			

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • Notification	Key Controls • Digital Diary Upload	Key Controls • Register Upload	Residual risk
Rule 12	Disclosure of health information outside New Zealand	No disclosure of information is to be made outside New Zealand under the rules identified in Rule 12.				

Health Information Privacy Code Rules		Solution Details and commentary	Key Controls • **Notification**	Key Controls • **Digital Diary Upload**	Key Controls • **Register Upload**	Residual risk
Rule 13	Unique identifiers - Only assign unique identifiers where permitted	The CTIP process will not use unique identifiers as part of its processes. A one time password (OTP) will be assigned by the NCTS. This will not be used other than for the upload and linking process of Digital Diary or Register information to link to the relevant Case or Exposure Event in the NCTS.				

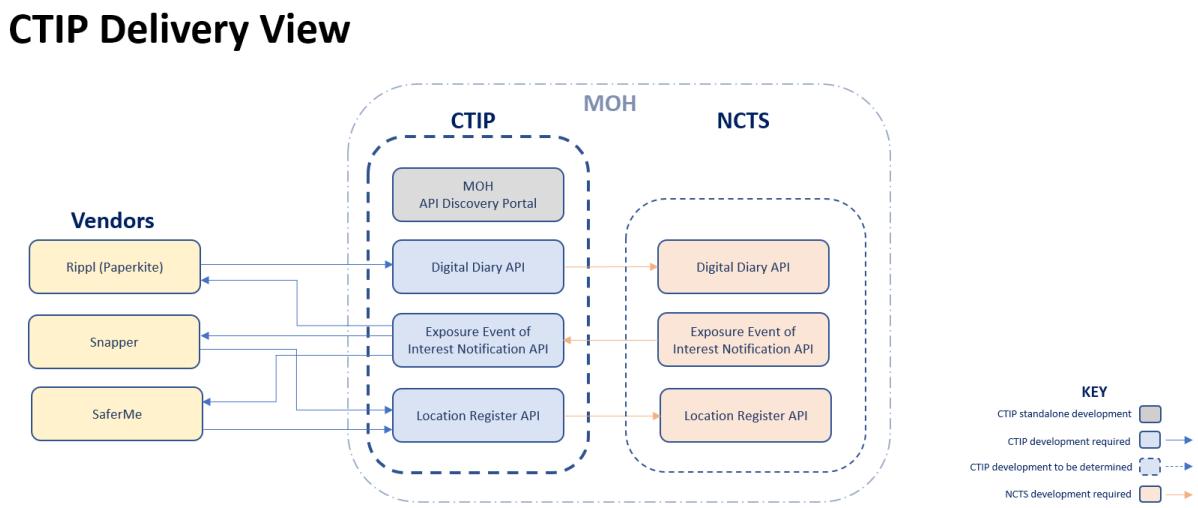
Appendix One – CTIP Product and APIs, and NCTS

1. This Appendix addresses the following:

   - The CTIP Product
   - APIs enabling Notification and Upload Features
   - Interactions with the NCTS
   - Statistical and Analytical information

   CTIP Product

2. The general plan for CTIP development with the initial three Vendors is set out in the following diagram:



3. This shows the information flows between Vendor Solutions and the NCTS:

   - One flow originates with the NCTS (Exposure Event of Interest Notification API). This involves the Contract Tracer initiated Notification being sent from the NCTS through CTIP to the Vendors.
   - If there is a positive case who agrees to upload their Digital Diary in discussion with a Contact Tracer, once they submit the one-time password, the information will flow from the Vendor Solution through the CTIP API to the NCTS.
   - If there is a Register containing information related to an Exposure Event this will flow through the CTIP gateway to the NCTS if the Location Manager authorises that release with the one-time password provided by the Contact Tracer.

4. The MoH API Discovery Portal contains technical information about the CTIP and does not include any identifiable information.

   APIs enabling Notification and Upload Features

5. The CTIP APIs provide the ability for systems to communicate with each other, subject to certain criteria. Information will transit CTIP APIs only when:

- There is an identified Exposure event – where the NCTS will send a Notification communication to the Vendors via the CTIP API; or
- A Case (or a Location Manager) authorises an upload of a Digital Diary or a Register after a request by a Contact Tracer.

6. The upload APIs are to be limited to only the supported information fields considered necessary to meet the Contact Tracing purposes, and time and Location criteria. Additional fields would not be able to be collected.

Interactions with the NCTS

- *Exposure Event Notification*

7. The NCTS will have a feature (a button for 'Escalate Exposure Event') to enable a Contact Tracer to indicate that an Exposure Event may have created Close Contacts and therefore be appropriate for Notification via the CTIP.
    - The Notification content will be defined by the Contact Tracers when the Notification is created.
    - This will require individual review and clinical sign off before the Notification is released to the CTIP, for publication to Consumers as a Contact Alert (via either Digital Diary applications or via Register processes of a CTIP Partner).
    - The EEOI Notification will pass through the CTIP APIs to the CTIP Partner solution, and on to the Consumer via the use cases out lined in Appendix Three.

- *Uploaded Information*

8. The NCTS will receive and store information uploaded via the CTIP Digital Diary and Register APIs. The processes for upload are detailed in Appendices Four and Five.
9. This information will be linked to the relevant NCTS Case record (the person who has tested positive) and where relevant, an Exposure Event associated with that Case. This will involve the Contact Tracers checking the uploaded information and verifying it before adding it to a Close Contact or Exposure Event entry.

Statistical and Analytical Information

10. All Activity and logging is captured in CloudWatch and CloudTrail which will be streamed directly into AWS ElasticSearch Service to enable API Monitoring and Alerting.
11. A non-identifying analytics event may be recorded to help the Ministry measure the number of Notifications.
12. The Ministry will use server logs to provide usage and performance reporting of the CTIP. This includes monitoring for the number of exposure notifications delivered, diary uploads processed, and visitor register uploads processed.
13. No personal information will be recorded in server logs.

Appendix Two – CTIP Partner Certification Process

1. Prior to authorisation for a Vendor to become a CTIP Partner (to authorise use of the CTIP by the relevant Vendor Solution) each Vendor will need to demonstrate that it can meet the requirements of the Certification Process.

2. This Certification Process is currently under development by the Ministry, but will include at least the following elements for the initial three CTIP Partners:

    - Contractual terms entered containing minimum Ministry mandated information technology and security terms. This will also provide for cancellation of the CTIP Partner status if specified events occur;

    - The CTIP Product Certification and Authorisation[18] process has been conducted by a third-party security provider. Connectivity of the Vendor Solution to the CTIP product will be reviewed for each CTIP Partner.

    - Contact details for each CTIP Partner must be available for Contact Tracers and a process in place to provide the opportunity to make prompt and direct contact with the Vendor or a Location Manager (as appropriate) for Contact Tracing related matters.

3. Each Vendor will be required to demonstrate that it can meet Privacy Act / Health Information Privacy Code requirements including:

    - An appropriate information Collection Process.

        - Each Vendor must establish that its published Privacy Statement – and the collection process / sign up terms - will adequately inform Consumers in accordance with collection processes required by the Privacy Principles of the Privacy Act (or Health Information Privacy Code if applicable)[19]. The Ministry and the initial CTIP Partners may work together with a view to developing standardised collection information that can be made available to subsequent Vendor applicants.

        - Each Vendor must identify any information it may hold in relation to a child or young person and confirm how it will comply with Rule 4 (fair and not intruding to an unreasonable extent on the personal affairs of that child or young person)[20].

    - The Vendor Solution Register upload process must follow a specific request from Contact Tracer. During the Certification Process the Ministry must analyse the information held by the Vendor Solution and identify if the Location Manager will be able to identify the name and address of contacts of the 'case' as required by section 92ZZF, and fits within one of the four roles set out in s92ZZF. Alternatively, it

[18] This is the standard, and comprehensive security review process conducted by the Ministry to identify compliance with the Ministry requirements

[19] This will include in particular the proposed use of the information, whether the supply of the information is voluntary (or mandatory for any aspect of a Register upload), reference to the potential recipient of the information (NCTS) and the process for access to and correction of information.

[20] Clarity would need to be provided about how the upload would be managed in relation to children and young persons if their information may be included in an upload, for example Snapper Green and Snapper School ID cards, or a child using a Snapper Red card. This should be clarified during the Certification Process to determine any appropriate restrictions on the information or the manner in which it is managed. There is provision in the Health Act at s92ZZC(5) for how Contact Tracers may require a parent or guardian to respond for the person under 16 years of age

will be identified whether the Contact Tracers will make their request under the exception to the Health Information Privacy Code) where there is a serious threat to public health or safety exception. The relevant Location Manager(s) who may authorise the upload with the one time password provided by the Contact Tracer, will also be identified.

- Upload Process:
    - The Vendor must demonstrate that any upload process will be appropriately authorised by the relevant Consumers. Digital Diary upload must always be authorised by Consumer choice, and Register uploads must be able to demonstrate appropriate authorisation[21].
    - The Vendor must confirm only necessary information fields will be uploaded as part of the Digital Diary or Register upload process (as per datasets specified by the Ministry). It is important that each Vendor can demonstrate only 'necessary' information will be submitted for NCTS collection i.e. information related to the identified risk of exposure to a third party, and only during that period of potential exposure.
    - The Vendor must confirm that time frames for information uploaded will not exceed:
        - the previous 60 days for Digital Diary uploads (being the clinically determined period appropriate to signal the previous four cycles of COVID-19); and
        - the specified time and date window specified by Contact Tracers for Register uploads (which will align to the potential risk of an Exposure Event).

4. The Vendor must also demonstrate a process for access for Consumers to information held about them, and the ability to request correction (a Consumer edit feature within any Digital Diary is strongly recommended).

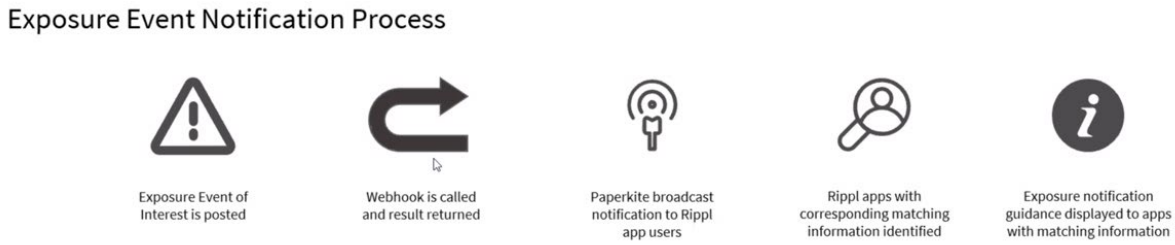
[21] Both in terms of the relevant authority request (section 92ZZF or the serious threat exception) and the process for the Location Manger authorisation signaled with the one-time password

Appendix Three– Use Case 1: Exposure Event Notification

1. This Notification use case relates to targeted messaging to potential Consumer contacts who may have been at the same place around the same time as a person who has tested positive (but not who that person was, nor the location / time in question).
2. If a Contact Tracer, through their investigation, determines a recorded Location (GLN) may be an Exposure Event, that recorded Location is added to the NCTS Case record. The Location could have been identified via the COVID Tracer App upload process, or via a CTIP upload process, but also in standard Contact Tracing unrelated to the App, where a compatible GLN Location is identified during discussions with a Case.
3. Contact Tracers have identified that the NCTS Notification process of alerting potential 'casual contacts' of an Exposure Event where they were present is useful to the Contact Tracing processes. Contact Tracers will be able to determine which Exposure Events are appropriate to send a Notification, and the message to be included (if any specific messaging is determined important). The Contact Tracers will determine the appropriate level of information to disclose based on the risk, and circumstances of the Exposure Event.
4. Appropriate resources are included on a weblink contained in the Contact Alert Notification about the symptoms to look for, and what to do in the event the Consumer needs further assistance (including Healthline contact details). Consumers receiving a standard (or lower risk) Contact Alert will be requested to monitor their wellbeing and call Healthline if they have any concerns.
5. The CTIP will not be able to identify which Consumers have received a Notification. Consumers are not required to identify themselves to Contact Tracers, nor to self-isolate. There is no ability for CTIP to independently track a Consumer's movements. Each Consumer will therefore be put on notice to monitor any potential health changes.
6. Consumers are not compelled to respond or take any particular action. They are instead able to monitor their own health and have a list of resources available if they become symptomatic.

   Notifications to Digital Diaries:

7. Messaging may be forwarded directly to Consumers who have CTIP compatible Digital Diaries (example Rippl):



8. As with the COVID Tracer App notification process, this process will enable the Consumer to be provided with a message through their device / app if they have a matching GLN for the relevant data and time.
9. The messaging will indicate to the Consumer that they have potentially been exposed to COVID-19, and general advice about what action to take in response.

Notification via a Register:

10. There may be multiple options with the CTIP Register use cases, depending on the nature of the Vendor solution. During the Certification Process each Vendor Solution, and the processes associated with any proposed Notification, will be reviewed to ensure that any unique privacy requirements are identified.

11. The Contact Tracer preference is that no notification from a centrally held Register be provided to:

    - The third party business owner associated with the Notification – the notification would relate to individuals who may have been present at that Location. The Contact Tracer expectation is that they will contact the business owner directly in the usual course of their processes - if a Case identifies they were at a Location when they were likely to be infectious. This enables the Contact Tracers to provide the relevant information about employees and their safety when they contact the business owner.

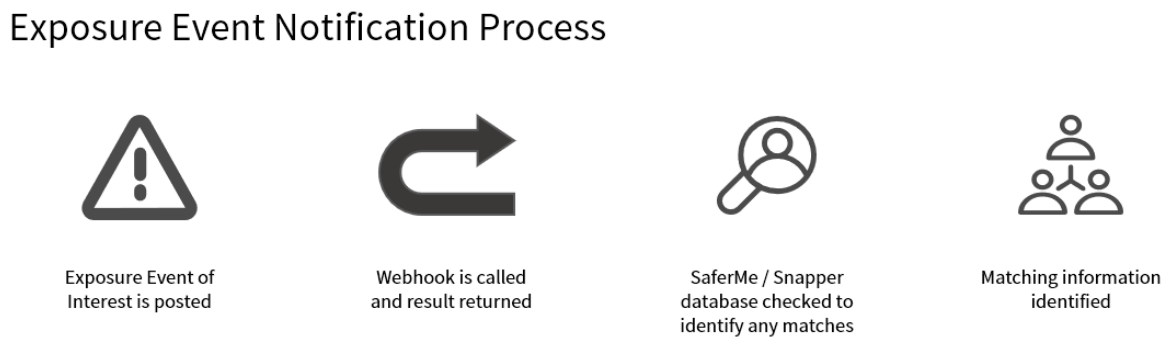
    - Consumers if email contact is the only communication method. The Contact Tracers will instead use the CTIP Partner upload process to identify lists of Consumers at a location and then contact them directly via the contact details uploaded – for example all of the passengers who recorded a transport event on a Snapper card that matches an Exposure Event, and had provided contact details to Snapper.

12. The following diagrams show the Notification will be sent to the CTIP Partner, but not sent by the CTIP Partner to the related business or Consumers.

13. The Notification process for the Register option will enable the CTIP Partner to be prepared for an upload authority to be received from a Location Manager, in the event the Contact Tracers request a Location Manager to upload the records.

14. The Contact Tracer will make contact with the Location Manager (via the s92ZZF or serious threat avenue identified during the Certification Process), and provide them with the opportunity to upload the part of their Register related to the Exposure Event. A one-time password would be provided, and the Location Manager would either enter that directly if it held the relevant Register information in its direct control, or provide OTP that to the CTIP Partner to action the upload process (further detailed in Appendix Five).

    The following process would apply to both the ‘SaferMe’ and Snapper Notification process:



Contact Tracers will control the process of identifying what Exposure Events are of sufficient risk that a Notification will be sent. The CTIP process will enable information matching that requested Exposure Event profile to be identified.

If the CTIP APIs are used to upload information the Contact Tracers will use standard questioning processes to identify what the actual risk of exposure was in the case of each individual contact identified in the uploaded information, after discussions with each contact.

Appendix Four – Use Case 2: Consumer Digital Diary Upload

1. This use case relates to individual Consumers, and the records they maintain of places they have been and people they have seen.
2. The Digital Diary information could be stored either on the Consumers mobile device (as is the case with the COVID Tracer App) or stored on a centralised database.

Upload Process

3. The Digital Diary information is managed by the individual and they will maintain control over whether or not to consent to the recorded information being shared for contact tracing purposes.
4. The Contact Tracer will contact a Case, and if they indicate they have a CTIP compatible Digital Diary, will invite them to upload it.
5. If the Consumer agrees to upload the Digital Diary details they are given a one-time password (OTP) over the phone. This OTP will authenticate the upload request and allow the date to be linked to the correct case in the NCTS.
6. The upload process will be as follows (example for Rippl):

7. There is no ability for CTIP to independently track a Consumer's movements, nor will the CTIP Partner be permitted to upload the Digital Diary without appropriate authorisation by the Consumer (driven by the OTP provided by the Contact Tracer).

Appendix Five – Use Case 3: Register Upload

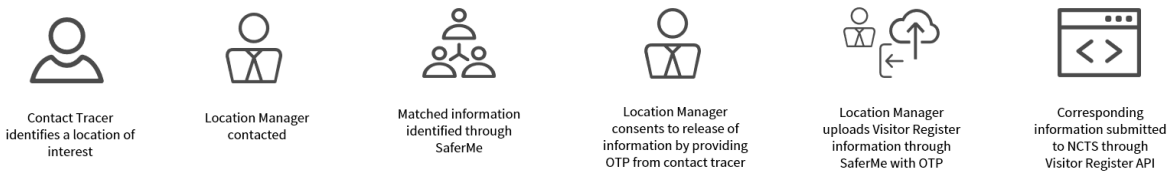
1. This use case relates to the Consumers who electronically 'check-in' to a location, or where Consumers can be matched electronically to a Location. The records are stored in a central database. This could include, for example:
    - a store recording information about visitors (an electronic version of a paper register)
    - an employer track of employees within a large workplace; or
    - a transport service which maintains records of travellers on that service (such as a bus).
2. As part of a case investigation a Contact Tracer will investigate Locations of possible Exposure Events. They will make phone calls to responsible people at affected Locations for more information (usually a Location Manager). This could include, for example, requesting a copy of a visitor register for a particular time period if one is available[22], or a request for details of passengers on a specific bus route. The information will be limited to the timeframes or locations necessary to identify potential contacts who may have been exposed to COVID-19.
3. The Contact Tracer will directly contact the party holding the information, and, under section 92ZZF (or the serious threat exception) request information relevant to the Exposure Event be provided.
4. It is to be part of the Certification Process that each CTIP Partner establish that the use of the information they will supply to CTIP, when necessary, will meet the requirements of the relevant information collection processes (as identified in the Certification Process), to ensure that Consumers they represent are fully informed about the potential use of their information
5. Using a GLN and time range relevant to the Exposure Event in question the CTIP Partner can search the Register records for matching records, or the Vendor Solution can be configured to identify the relevant information necessary to meet the criteria identified as necessary by the Contact Tracers.
6. The party with the direct relationship to the Consumer group who was present at the Exposure Event (who could be the Location Manager CTIP Partner – if the information holdings are centrally held) will be responsible for enacting the upload process. This will be by use of the 6 digit one-time-password provided over the phone by the Contact Tracers, to send the relevant data to Contact Tracers electronically.
7. Examples of Register Upload Process:

[22] Section 92ZZF authorises Contact Tracers to request information about names and addresses of a contact from any business or other organisation that the individual has dealt with if they are known to a person. If this provision does not apply then the request will be made under the serious threat to public health or safety exception.

Safer Me

SaferMe

Visitor Register Upload Process

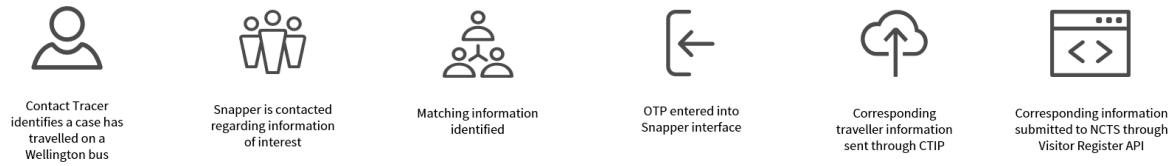


- The organisation may upload relevant contact and Location information in response a Contact Tracer request; or
- a system to system request may be created advising the Exposure Event ‘window’.

Snapper

Snapper

Visitor Register Upload Process



Appendix Six - Glossary

The following are definitions used in this Assessment:

Terms	Description, relationship and business rules
AWS	Amazon Web Services
Case	A case of a person who has had a positive laboratory test for COVID-19. Case definition of COVID-19 infection can be found here
CCTA	Contact Tracing processes by use of a Mobile Application for supported iOS and Android smart phones (the NZ COVID Tracer mobile app), a Web Application (Website), and a Data Product (Product) collectively referred to as the COVID-19 Contact Tracing Application.
Certification Process	The process that a Vendor must satisfy before being able to become an authorised CTIP partner. Initial details of this process are described in Appendix Two.
Close Contact	This is any person who has been exposed to a suspect, confirmed or probable case of COVID-19 during the Case's infectious period without appropriate personal protective equipment. The contact is more fully detailed on the Ministry website here: https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-novel-coronavirus-health-advice-general-public/contact-tracing-covid-19
Consumer	A user who participates in a Vendor Solution, or whose information is collected onto a Vendor Solution.
Contact Alert	The app feature that will alert the Consumer that a Notification has been received by their device signalling that they may have been in contact with a case of COVID-19.
Contact Tracer	An individual who is authorised to fulfil the role of contact tracer in accordance with section 92ZZA of the Health Act, and includes those assisting with finding and location services. All Contact Tracers are subject to an obligation of confidentiality.
Contact Tracing	This is the process used to find people who may have been exposed to an infectious disease. If a person is identified as a Close Contact of someone with COVID-19 they can expected to be contacted by a Contact Tracer, generally by telephone, from the National Close Contact Service operated by the Ministry of Health.
CTIP	Contact Tracing Integration Product
CTIP Partner	A Vendor authorised to connect the Vendor Solution to the CTIP on completion of the CTIP Partner Certification Process

Terms	Description, relationship and business rules
Digital Diary	The information a Consumer chooses to record via their mobile device about their interactions and activities, including places they have visited or people they have been in contact with. This includes the scanned Location information. The Diary may be held on the Consumers own device or could be held centrally by the CTIP Partner. Any upload authorisation must be generated directly by the Consumer.
EEOI	Exposure Event of Interest
EEOIN	Exposure Event of Interest Notification
Exposure Event	A Location, and associated date and time range where there is potential for a potential Close Contact to have been exposed to COVID-19. This will be determined by a Contact Tracer.
GLN	Global Location Number. A unique identification of a specific location (which will include a specific branch of an organisation)
Location	The GLN recorded on the Consumer's mobile device, which includes a date and time of scan, or a Location where a Register is held (this can include for example, a place or a method of transport).
Location Manager	The person in charge of a Location where a Vendor Solution is collecting information, who has functional control of that information and is able to authorise release of that information.
NCTS	The National Contact Tracing Solution is the secure technology solution to support national Contact Tracing activities.
NCTS case record	The NHI linked record that is stored on the NCTS which relates to an individual Consumer who is a positive or probable case.
NHI	The National Health Index number is the unique identifier assigned to every person who uses health and disability support services in New Zealand.
Notification	The notification to CTIP Partner Consumer devices or Registers which have an Exposure Event matching a Location recorded on that Consumer's device.
OTP	One time password
Privacy Statement	A privacy 'collection' statement to be used by any CTIP Partner, which must be compliant with the Principle 3 collection process required under the Privacy Act.
Register	The Register maintained by a CTIP Partner recording the Consumers who have visited a specific place (or Location).

Terms	Description, relationship and business rules
Upload Information	The Digital Diary information that a Consumer has recorded on their device and chooses to upload to the NCTS on request by a Contact Tracer. This will include scanned Location information and also manual entries. Upload or Uploading means the process of transfer of that Digital Diary information.
Vendor	The owner of a technology solution recording and managing information about the movements and / or contacts of Consumers that is compatible with the CTIP processes.
Vendor Solution	A potentially CTIP compatible technology solution