Ministry of Health
COVID-19 Contact Tracing Application

Privacy Impact Assessment
Includes: Release 1 (20 May 2020)
    Release 2 (10 June 2020)
    Release 3 (29 July 2020) and
    Release 4 (3 September 2020)
    Release 4.2 (9 September 2020)

Date 9 September 2020
Confidentiality

This Privacy Impact Assessment (“the Assessment”) will be an evolving document that will record the impacts related to the latest release developments, immediately prior to implementation of such releases. This document will be regularly updated. The current version of this document will be made publicly available, commencing with initial release of the NZ COVID Tracer mobile app.

- The first Privacy Impact Assessment was in respect of Release 1.
- The second Privacy Impact Assessment covered both Release 1 and Release 2.
- The third Privacy Impact Assessment covered Release 1 to Release 3 inclusive.
- This is the fourth Privacy Impact Assessment and addresses Release 4 in addition to those matters addressed in the third Privacy Impact Assessment.

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:

- Sector Portfolio Manager, Digital Portfolio Team, Ministry of Health
- Manager, Data Governance, Data & Digital, Ministry of Health
- Project Manager, COVID-19 Contact Tracing App, Data & Digital, Ministry of Health
- General Manager, Emerging Health Technology and Innovation, 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 purposes for which information collected via the NZ COVID Tracer mobile app 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.

Summary of Intent

This Assessment represents the current state of the way the NZ COVID Tracer mobile app will operate, and expectations for future releases.
# Contents

## SECTION ONE – EXECUTIVE SUMMARY
- Clarity of Purpose
- Information Collection Processes
- Access and Security
- Future Privacy Impact Assessment Activity

## SECTION TWO – OPERATIONAL DETAILS
- Background
- Information Collected and User Information Flows
- Data Flows
- Use of Information: Data Storage, Retention and Access
- CCTA Security
- Governance

## SECTION THREE - PRIVACY ANALYSIS

## SECTION FOUR - INTENDED FUTURE USE CASES

## APPENDIX ONE – CONTACT TRACING – THE SYSTEM SUPPORTED BY THE CCTA

## APPENDIX TWO – THE DETAIL OF RELEASE 1 OPERATIONS

## APPENDIX THREE – THE DETAIL OF RELEASE 2 OPERATIONS

## APPENDIX FOUR – THE DETAIL OF RELEASE 3 OPERATIONS

## APPENDIX FIVE – THE DETAILS OF RELEASE 4 OPERATIONS

## APPENDIX SIX – THE DETAILS OF RELEASE 4.2

## APPENDIX SEVEN - GLOSSARY
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\(^2\). Further detail about Contact Tracing can be found in Appendix One.

3. The Ministry has identified an opportunity to support national Contact Tracing processes by use of an application for supported iOS and Android smart phones (the NZ COVID Tracer mobile app – the App), a Web Application (Website), and a Data Platform (Platform). These are collectively referred to as the COVID-19 Contact Tracing Application (the CCTA).

4. Individuals who choose to use any component of the CCTA are referred to as “Consumers” in this Assessment. The CCTA will enable Consumers to keep their own record of places they have been, and activities they have undertaken. This will assist them to rapidly respond to Contact Tracers about where they have been, who they have been in contact with and the type of activity that has occurred. Contact Tracers will then be able to more quickly identify Close Contacts and Casual Contacts, and assess the risk of exposure to the virus.

5. The Office of the Privacy Commissioner has been consulted and is satisfied that the privacy implications of this release and their mitigations have been appropriately recorded in this PIA.

   **Privacy focus**

6. 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 minimise any potential privacy risks in its development of the CCTA. Consumer trust is essential if use of the CCTA is to become widespread. The Ministry intends to earn and respect that trust.

7. 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

---

\(^1\) 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://science.sciencemag.org/content/early/2020/04/09/science.abb6936)  
the CCTA to ensure that relevant risks are identified and mitigated. This has involved ongoing consultation with the Office of the Privacy Commissioner and others to ensure that the CCTA retains a strong privacy focus.

8. This Assessment is to be a ‘living’ document that will be updated as the CCTA development progresses, with the intent that updates be published either ahead of or alongside future releases. This will enable the Ministry to maintain transparency about the CCTA with Consumers, who may choose to opt-out if they do not wish to participate in future releases.

**Background**

9. 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.

10. 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.

11. Additional key uses for technology are:

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

11.2. 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

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

12. The Ministry has therefore commissioned, and is operating, the CCTA to enable the New Zealand public to opt in to support Contact Tracing processes for the purposes of the COVID-19 pandemic response.

13. As other apps enter the New Zealand marketplace, the Ministry is developing standards that will enable those other apps to participate in support of the public health Contact Tracing processes, provided that the other apps can meet the necessary security and privacy standards.

**COVID-19 Contact Tracing Application (the CCTA)**

14. Development of the CCTA is progressing in stages, and new functions will be released as they are developed. This Assessment addresses Releases 1 to 4 inclusive.

15. Components of Release 1 are summarised below. Additional detail of the CCTA operations involved in Release 1 can be found in Appendix Two.
### Release identifier | Content of Release | Date of release
---|---|---

| Release 1 | **Contact Details**: Website available to enable Consumers to opt in and submit their own contact details. The only compulsory detail is an email address. Full name, date of birth, gender, phone number, address are all optional details, and will assist with identification and contact if provided. Ethnicity is also optional and is being collected where available to help the Ministry monitor one element of equity of access for Consumers. These details will be available to contact tracers to look-up within the NCTS when that person tests positive with COVID-19 or is a potential Close Contact of that person. | 19 May 2020 |

NZ COVID Tracer mobile apps for iOS and Android
- **Contact Details**: Consumers can opt in and submit their own contact details via the mobile App
- **Location recording**: Consumers can ‘check-in’ to Locations by scanning a QR code (location recording). This will record the Location visited, the date and the time of the scan. This record will remain on the Consumer’s device as a digital diary if that Consumer is contacted by a contact tracer. The information does not leave the Consumer’s device in Release 1.

16. Components of Release 2 are summarised below. Additional detail of the Release 2 CCTA operations can be found in Appendix Three.

| Release identifier | Content of Release | Date of release |
---|---|---

- Notification of potential Exposure Event
- Location ‘data upload’ capability
- Haptic features for scanning
<table>
<thead>
<tr>
<th>Release 2</th>
<th>NZ COVID Tracer mobile apps for iOS and Android</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>Notification of Exposure Event</em>: Contact Tracers are able to, at their discretion, publish an Exposure Event of Interest (EEOI) to subscribed App Consumers to notify them of a potential exposure to COVID-19.</td>
</tr>
<tr>
<td></td>
<td>• This process will trigger a ‘match’ if the Consumer’s device holds appropriate Location data associated with a specific date and time period generated by scanning a compatible QR code. The App will then advise the Consumer of relevant information about how the individual can manage their health, and testing options where appropriate.</td>
</tr>
<tr>
<td></td>
<td>• The Consumer may choose not to use this feature (it requires opt in for iOS, and opt out for Android, due to the nature of the respective operating systems).</td>
</tr>
<tr>
<td></td>
<td>10 June 2020</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NZ COVID Tracer mobile apps for iOS and Android:</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Location data upload capability</em>: Consumers who have:</td>
</tr>
<tr>
<td>• recorded Location information (the places the Consumer has been and scanned a QR code); and</td>
</tr>
<tr>
<td>• are contacted by a Contact Tracer as they have tested positive, or are a probable case</td>
</tr>
<tr>
<td>will be able to authorise the App to release the current Location data held on their device to the NCTS for access by the contact tracer, if they choose to do so.</td>
</tr>
</tbody>
</table>
NZ COVID Tracer mobile apps for iOS and Android:

*Haptic features:* A vibration function will be added to enable confirmation for a Consumer when a Location scan has been successfully completed. This feature is not addressed further in this Assessment but will be available to all App users to improve the accessibility of the solution.

17. Components of Release 3 are summarised below. Additional detail of the Release 3 CCTA operations can be found in Appendix Four.

<table>
<thead>
<tr>
<th>Release identifier</th>
<th>Content of Release for NZ COVID Tracer mobile apps for iOS and Android:</th>
<th>Intended date of release</th>
</tr>
</thead>
</table>
| Release 3          | *Manual Digital Diary Entries:* Consumers can manually add entries to their Digital Diary, to record activities, or places they have been, where a QR-code poster was not on display. A Digital Diary entry can include free text entry by the Consumer. This may record the name of a location or activity (and address details), and the date/time of the visit. The Consumer is also able to jot down notes about the visit to jog their memory.  
  - Manual Digital Diary entries are stored on the Consumer’s device in the same way as “scanned” Locations.  
  - If the Consumer authorises the release of their Digital Diary, at the request of a contact tracer, both scanned Locations and manual entries will also be included in the Digital Diary release.  
  *Support for password managers:* To help a Consumer choose and remember a secure password, the native “password manager” functionality support will be enabled on the Consumer’s own device.  
  - The Consumer is required to opt-in to use this functionality | 29 July 2020 |
If the Consumer does opt in, credentials (email address and password) will be stored securely using the built-in password manager on the Consumer’s device.

The App will be able to operate on additional operating systems in Release 3 – Android 6 and iOS 11.

18. Components of Release 4 are summarised below. Additional detail of the Release 4 CCTA operations can be found in Appendix Five.

<table>
<thead>
<tr>
<th>Release identifier</th>
<th>Content of Release for NZ COVID Tracer mobile apps for iOS and Android:</th>
<th>Intended date of release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4</td>
<td>Ability to manually record a Consumer’s own National Health Index (NHI) number</td>
<td>3 September 2020</td>
</tr>
<tr>
<td>Release 4</td>
<td>Ability to edit Digital Diary entries</td>
<td></td>
</tr>
<tr>
<td>Release 4</td>
<td>Ability to Manually Record NHI: Consumers will be given the option to manually add their NHI to the details they have recorded on their device. This will enable them to use their device screen to display (if they choose) their NHI, and name and date of birth on the ‘My NHI Details’ screen.</td>
<td></td>
</tr>
<tr>
<td>Release 4</td>
<td>This is designed to enable Consumers to swiftly and privately show their details to testing staff if they attend community-based testing facilities.</td>
<td></td>
</tr>
<tr>
<td>Release 4</td>
<td>The NHI will not be verified on the Consumer device and is to be used for information only. The NHI would still need to be verified by any health professional interacting with the individual.</td>
<td></td>
</tr>
<tr>
<td>Release 4</td>
<td>The NHI details added into the ‘My NHI Details’ process will not be added to either the contact details on the CCTA platform nor to the Digital Diary Upload information. The name and date of birth would be added to the contact details (if not previously entered).</td>
<td></td>
</tr>
</tbody>
</table>
19. Components of Release 4.2 are summarised below. Additional detail of the Release 4.2 CCTA operations can be found in Appendix Six.

<table>
<thead>
<tr>
<th>Release identifier</th>
<th>Content of Release for NZ COVID Tracer mobile apps for iOS and Android:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Call back request following a Contact Alert notification (when determined by Contact Tracers that the Location is high risk of unknown contacts)</td>
</tr>
<tr>
<td></td>
<td>Extension of Digital Diary retention period to 60 days</td>
</tr>
<tr>
<td></td>
<td>Quick scan for a logged out user and default screen changed to Record a Visit.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Call back request</strong>: If an authorised Contact Tracer determines that there is an Exposure Event of Interest that would benefit from additional follow-up of notified Consumers, a ‘Call Back’ option may be included in the Contact Alert Notification.</td>
</tr>
<tr>
<td></td>
<td><em>The Consumer will be given the option to confirm their details and receive a Call Back (a call from Contact Tracers).</em></td>
</tr>
<tr>
<td></td>
<td><em>This will enable the Consumer to complete their contact details so that they can be submitted to the NCTS to enable the Contact Tracer to make contact (as the Consumer is otherwise unknown to the Contact Tracer).</em></td>
</tr>
<tr>
<td></td>
<td>**<strong>Digital Diary</strong>: Extension of retention period. The Contact Tracing clinical team signalled the ability to look back at retained information for additional incubation periods would be useful to assist in the identification of source cases. An extension of the period for data retention before automatic deletion from the Digital Diary is now set at 60 days rather than 31 days.</td>
</tr>
<tr>
<td></td>
<td><strong>Quick scan</strong>: If a user is logged out by the App they are still able to scan using the camera (this</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>9 September 2020</strong></td>
</tr>
</tbody>
</table>

*Entry Edit Ability:* As previously signalled in Release 3, the manual edit function for the Digital Diary has now been enabled for Release 4.
will not apply to a user who deliberately logs off). The default screen for a logged-in user will change from the dashboard setting to ‘Record a Visit’ for Consumer convenience.

Clarity of purpose

20. A simple Privacy Statement is displayed to Consumers as part of the CCTA registration process. This is linked to a more detailed Privacy and Security Statement for those who wish to view that more detailed information.

20.1. These Privacy Notice Materials have been created with the intent that all Consumers can obtain a full understanding of how their information will be used if they choose to participate.

20.2. The original versions of these statements were updated immediately after Release 1 to incorporate feedback from academics and Consumers to ensure additional detail was added into the Privacy Statement to provide further clarity about where contact details and Location information are held. The Statements were updated to address the additional functions available as part of Releases 2 and 3, and will be updated again as part of Release 4, as appropriate.

21. Authorised users of the information (Contact Tracers) will be informed about expectations for use, and limitations on use of this personal information. This will be consistent with their existing legislative responsibilities under the Health Act to manage this information appropriately.

Information Collection Processes

22. The Privacy Notice Materials, including the Privacy Statement and the Privacy and Security Statement, are designed to be compliant with rule 3 of the Health Information Privacy Code. The Privacy Notice Materials are available to Consumers at the first contact with the CCTA, and will form part of the Terms of Use, prior to the Consumer submitting any information.

23. CCTA Consumers will be notified in advance of any material changes being implemented to the Purpose Statement or other Privacy Notice Materials via their registered email address or in-App message. This will indicate new features and also what has changed from a privacy perspective (if anything). There will also be an opportunity within the App to review the updated privacy statement on the device screen when a new feature is added that requires an opt in / opt out choice. This will enable ongoing Consumer choice about participation.

24. Consumers have the choice of opting-in to use the CCTA, and if they do, will retain the choice of the extent to which they wish to contribute information.
25. This includes:

25.1. when recording their contact details for upload to the Ministry (other than the email address required for registration) they may choose what contact and identification details they include;

25.2. whether or not to use the location features, and Consumers may choose which participating Locations that they wish to scan or add to their Digital Diary;

25.3. whether or not to use the manual entry Digital Diary features, and what to include in their Digital Diary; from Release 4 manual Digital Diary entries can also be edited or deleted.

25.4. whether to add their NHI, name and date of birth details to the ‘My NHI Details’ screen, and then whether to display that if presenting for COVID-19 testing;

25.5. whether to electronically share recorded Digital Diary entries if contacted by a Contact Tracer (both Locations and manual entries will be uploaded if the Consumer chooses to forward these Digital Diary records to the Contact Tracer); and

25.6. whether to opt in (or opt out depending on the operating system) to receiving Exposure Event Notifications; and

25.7. responding to a Contact Alert Notification including a Call Back request.

26. Links will be provided to a web-based explanation in the Privacy and Security Statement which will contain more detail for those individuals who wish to know more (a layered privacy notice). The Privacy and Security Statement will also link to the current version of this Assessment.

Access and Security

27. The CCTA implements robust security and authorisation controls to prevent unauthorised access to information, and follows leading practices for encrypting data at rest and in transit. Access to information requires authentication.

28. Prior to each substantive release, the CCTA and supporting web services will be independently security assessed by an All of Government approved supplier. Findings from the reviews will be remediated where appropriate. Future releases of the solution will also be independently assessed to the same standards.

Future Privacy Impact Assessment Activity

29. The CCTA has been developed in parallel with completion of this Assessment. The Office of the Privacy Commissioner and Government Chief Privacy Officer have provided independent advice and assessment to the project team during this process, which the project team has endeavoured to incorporate into the CCTA application.
Section Two – Operational Details

Background

The Ministry approach to the CCTA development

1. The Ministry is developing the CCTA to support national Contact Tracing activity. Decisions made on Release features for the CCTA are driven by a focus on privacy and choice for individuals, alongside identified requirements for Contact Tracing.

2. The Ministry has taken an approach informed by the work done for the development of the proposed national Health Information Platform. This work was informed by the development of the social sector Data Protection and Use Policy. The intent with this is for the Ministry to be transparent with the use of the data, in order to maintain and grow social licence. The Ministry has applied these principles in the following manner:

- The information collected will be voluntarily provided by the Consumer (on an opt in basis)
- The information collected will only be used for the COVID-19 Pandemic Public Health Response (limited use)
- Any information relating to the Consumer’s visited Locations will remain on their device unless they decide to use the CCTA’s electronic upload facility after a request from a Contact Tracer. This voluntary process does not remove the requirement under section 92ZZC(3) of the Health Act for a person who has COVID-19, or is a probable case, to provide information about the circumstances in which they may have contracted or transmitted the virus.
- The visited Location records on the Consumer’s device will expire on a rolling 60-day period. This is on recommendation of the Contact Tracing team following the Auckland outbreak. It is consistent with four incubation periods of the virus – which amounts to 56 days.

3. The approach the Ministry has taken is to try and make it as easy as possible for Consumers to sign up and provide their information, while providing sufficient security controls for Consumers to manage their information. Consumers will choose to visit the website or download the App through hearing about it from a number of sources. If they choose to sign up, they will see the Privacy Statement and have access to the Terms of Use prior to registering.

4. Contact Tracers will be able to use App generated information from Consumers to support the national case management of positive cases and Close Contacts. Case management is recorded on the NCTS. All points of contact with the NCTS are described in this Section Two of this Assessment.

3 https://dpup.swa.govt.nz/
Information Collected and User Information Flows

5. The Ministry has identified three key sets of information the CCTA will collect:

- **Personal, contact and demographic information** – Consumers providing this information about themselves will allow Contact Tracers to contact the correct person more quickly and easily. Demographic details (including via ethnicity information, if Consumers choose to provide it) will also assist the Ministry to understand its performance and to produce a solution that is more equitable. The individual may also record their NHI number on their device in case they require it to establish their health identity quickly.

- **Visited Locations** and Digital Diary entries – this information will be provided by Consumers about Locations they have visited (by scanned QR Code) or by manual Digital Diary entry for places visited or activities in which the Consumer has been involved. This easy access by Consumers to their past movement and activity information will allow Contact Tracers to more quickly assess information relating to Locations where the COVID-19 infected (or probable case) Consumer may have encountered Close Contacts, thus reducing the risk of transmission to others.
  
  - A Consumer must choose to scan a QR code or manually record a visit in their Digital Diary on each occasion or no information will be collected. This Digital Diary information is held on the Consumer’s device.
  
  - A Consumer, who has tested positive or is a probable case, may also make a decision to upload that information (when requested by a Contact Tracer). Release 3 will enable all Digital Diary entries to also be uploaded at this same time (there will not be a choice to upload only scanned Locations or only manual entries – the choice will be to upload all information or not upload).

  ▪ Uploaded Locations and Diary Entries will be useful to the Contact Tracer as they will be able to review the Locations and Digital Diary details, and discuss them further with the Consumer.

  ▪ This discussion will enable the Contact Tracer to identify any Location, date and time were there may have been a risk of transmission to other individuals (Exposure Events).

- **Anonymous Statistical and Performance Information** – this information will be collected from Consumer’s interactions with the CCTA, and from its performance on devices, to help the Ministry to understand the stability and effectiveness of the CCTA, and develop equitable solutions.

6. Appendices Two to Five inclusive contain additional discussion of the information collected in respect of each release.

Data Flows

7. The following diagram demonstrates the dataflows associated with the CCTA:
Use of Information: Data Storage, Retention and Access

8. Consumer access to personal information is limited to information about that specific Consumer only. No Consumer is able to see information about any other Consumer.

9. Select staff and individuals in a production support role have access to the CCTA Platform (the data storage system that holds Consumer personal contact information). This access is only used for the purposes of maintaining the correct function of the production application. This access is logged and audited, and written authorisation is required before viewing of any personal information is permitted.

Contact details

10. Consumer contact details are securely stored by the CCTA AWS platform. This data store is able to be queried (view only access) by Contact Tracers who:

- have authorised access to the NCTS, and
- who need to find contact information of confirmed or probable Close Contacts of a person with a confirmed or probable case of COVID-19.

11. This secure NCTS / CCTA interface will only be used if the Contact Tracer needs to locate the individual Consumer and did not already have access to their current contact details.

- Any access will be logged into the NCTS audit records. This audit trail will record which Contact Tracer used their view access to an individual Consumer’s contact details.
• The contact information will only be entered into NCTS once it has been verified by the Contact Tracer through making contact with the Consumer, both to confirm they have identified the right person and that the contact detail is accurate. Other information will be obtained directly from the individual Consumer by discussions with the Contact Tracer.

Digital Diary - Location details and manual entries

12. If a CCTA Consumer (who is a confirmed or probable case) is requested by a Contact Tracer to inform them of the Locations they have been to, or the people that they have been in contact with, the Consumer may choose to use the CCTA’s electronic release facility to upload the Digital Diary they have recorded. This will include scanned Locations recorded on their device, and their manual Digital Diary entries (the Upload Information).

13. If the Consumer chooses to electronically release the Upload Information, that information will be held in a secure store within the NCTS Salesforce boundary.

• The Upload Information can be accessed by the Contact Tracer through Salesforce (NCTS) which retrieves the data relating to that case from the data store.

• Any access will be logged into the NCTS audit records. This audit trail will record which Contact Tracer used their view access to an individual Consumer’s Upload Information.

• Where a scanned Location or manual Digital Diary location that has been submitted by the Consumer is identified as an Exposure Event, an Exposure Event entry will be created within the NCTS. This Exposure Event and the associated Contact Location will be retained as part of the NCTS case record.

• Digital Diary manual entries that identify potential Close Contacts will be followed up through NCTS contact tracing processes.

• Form this Upload Information Locations that are not identified as Exposure Events, or manual entries not identified as relevant for Contact Tracing of Close Contacts will be retained for six months before being securely destroyed.

Exposure Event Notification

14. If a Contact Tracer, through their investigation, determines a recorded Location may be an Exposure Event, that recorded Location is added to the NCTS case record. This will apply to Locations identified that have been submitted via the App, and also in standard Contact Tracing unrelated to the App.

15. Contact Tracers have identified that the App can assist to provide notification of potential ‘casual contact’ with an individual who has since tested positive. If an Exposure Event is determined to have created a risk of infection of Close Contacts, and that Location has a GLN, a clinical decision will be made as to whether it will benefit the Contact Tracing process to send Notification via the App, in addition to the other methods available for identifying Close Contacts.

16. 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 CCTA.
• This Exposure Event will then be considered by Ministry clinicians to determine whether Close Contacts are likely to have been created and the App is an appropriate method of advising of that Exposure Event.
  
  o Only a limited number of authorised Contact Tracers will be able to use the interface in NCTS to create an Exposure Event of Interest (EEOI) for Notification (an EEOIN).
  
  o The EEOI Notification content will be defined by the Contact Tracers when the Notification is created. The Contact Tracers will determine the appropriate level of information to disclose based on the risk, and circumstances of the Exposure Event.
  
  o This will require individual review and clinical sign off before the EEOIN is released to the CCTA, for publication to Consumers as a Contact Alert.
  
  o This clinical intervention is to maintain national consistency in the Notification process, and ensure that consistent clinical criteria are applied. It is important to maintain a balance between alerting individuals to a potential exposure, against the anxiety generated by over Notification of Contact Alerts. The clinical oversight and final decision making on sending the Notification is designed to weigh that balance in decision-making.
  
  o The addition of the Call Back feature, and the ability for Contact Tracers to add a specific message in a Contact Alert, will assist the management of the higher risk Exposure Events from those that are lower risk (as the lower risk Contact Alerts will not receive the Call Back option).

17. Notification of an EEOI is available to Consumers who subscribe to the alert Notifications, and who have a matching date, time and Location (scanned GLN) on their device.

• Upon a successful match of an Exposure Event on a Consumer’s device, the Consumer is provided with a Contact Alert Notification that they may have been in contact with COVID-19 (including any content that may have been approved by the authorised Contact Tracer).

• Each Consumer will therefore be put on notice to monitor any potential health changes. If the Contact Tracer considers additional information is necessary, that information could be included in the Notification message. If the Contact Tracer considers it a higher risk event, a Call Back option may be initiated.

• 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.

• The Consumer will not be identified by the Contact Alert receipt, and no information about the Consumer’s identity will be passed to Contact Tracers. Only if a Call Back option is offered, and accepted by the Consumer, will the Consumer choose to send their name and contact phone number as part of the Call Back request. If the Consumer chooses to accept the ‘offer’ to receive a Call Back from a Contact Tracer a code (linking to the case record of the person who gave rise to the Exposure
Event) will be available to the Contact Tracer as part of the Call Back response. The Contact Tracer can then have a direct discussion with the Consumer about their personal situation.

- At no time is information about the person who tested positive to COVID-19 available to other Consumers.

18. 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.

19. A non-identifying analytics event may be recorded to help the Ministry measure the number of Notifications.

Security and Retention on NCTS

20. Full details of the data access and controls in place for NCTS will be covered in a separate Privacy Impact Assessment for the NCTS. In summary:

- 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.

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

- 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.

21. Information that originates from the App that is sent to the NCTS by one of the processes identified above will be securely stored under the following retention requirements:

- Any identifiable information collected will only be used for public health purposes related to COVID-19.

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

- Digital Diary data uploaded will be located in a secure location within the NCTS Salesforce platform but will not be transferred into a NCTS case record unless a Contact Tracer determines it is relevant to an Exposure Event. Any information, including Location Information, not transferred will be securely deleted on a regular basis (within six months of submission).

- 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.
• Information retention policies will be fully detailed in the NCTS Privacy Impact Assessment, but in summary:
  o Any identifiable information that does not become part of the NCTS case record of an individual will be securely and promptly destroyed after the pandemic is over (such as information linked only to a Close Contact).
  o Any information incorporated into an individual NCTS case record will be managed securely and retained in accordance with the Health (Retention of Health Information) Regulations 1996. Consideration is being given in the NCTS retention policy development as to what parts of this NCTS case record may be able to be securely destroyed earlier. The NCTS will engage with the Office of the Privacy Commissioner and the Chief Archivist before finalising its retention policy and specifically address this issue.
  o Non identifiable (or de-identified) information may be used for purposes related to the public health response to COVID (which may include planning for future potential events or research).

Statistical Information

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

CCTA Security

23. Prior to each major release, the CCTA and supporting web services will undergo an independent security review by an All of Government approved supplier. Findings from the review will be remediated where appropriate. Future releases of the solution will also be independently assessed to the same standards.

24. The CCTA, including Consumer’s personal information and anonymised information, is hosted and stored using Amazon Web Services (AWS) 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.

25. The Website found at tracing.covid19.govt.nz is stored and served using Netlify, a specialist web hosting service designed to host static web applications. Only pre-compiled static web assets, including HTML, CSS, and JavaScript are served from Netlify. Consumer’s personal information, and other data collected by the CCTA, is not sent to Netlify servers.

26. Data stored within AWS is encrypted. The Ministry controls access to the encryption keys and the data.

27. The source code and high-level architecture for initial design of the solution have been reviewed by the Government Communications Security Bureau’s National Cyber Security Centre and an independent All of Government security supplier and designed in collaboration with Amazon Web Services. The National Cyber Security Centre continues to be involved in the architecture reviews.
28. The Specific Agreement with the Service Provider for provision of the CCTA contains standard Ministry Information Technology clauses designed to require compliance with relevant New Zealand security and privacy obligations in development of the CCTA.

Governance

29. 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:

- The Data Governance Group at the Ministry for COVID-19.
- The Senior Responsible Officer for Data and Digital's COVID-19 response
- 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.
- The NCTS governance team.
Section Three - Privacy Analysis

The purpose of this Assessment is to review the process of collection, storage, use and sharing of personal and contact information for the purposes of the COVID-19 pandemic response against the 12 Rules in the Health Information Privacy Code (HIPC).

This application will collect personal and contact information for health purposes. It will be a health agency (the Ministry of Health) collecting, storing, using and where appropriate sharing the information collected (with other health agencies, but only as required for the purposes of the COVID-19 pandemic response).

The App has been changing incrementally through a series of Releases. The Release in which an initial change occurred, or feature was added, may be referenced in the Analysis below. All subsequent Releases will continue to incorporate that change or feature unless otherwise stated.

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.

<table>
<thead>
<tr>
<th>Health Information Privacy Code Rules</th>
<th>Solution Details and commentary</th>
<th>Key Controls</th>
<th>Residual risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1 Purpose of collection of health information - Only collect health information if you really need it</td>
<td>The purpose of collecting this information is to assist with Contact Tracing activities as part of the COVID-19 pandemic response. The App is intended to address two problems: 1. Consumer Contact Details: New Zealanders who have changed their contact details since they were last updated in the NHI or NES services or people in New Zealand with no contact details in those services. The impact of this lack of information is that Contact Tracers find it more difficult to contact the person concerned, delaying the process of testing and/or self-isolation for potential Close Contacts. 2. Close Contacts and Locations: People have difficulty remembering where</td>
<td>Purpose Collection of this demographic, contact and Location information is for the lawful purposes of the COVID-19 pandemic response to assist in the public health response. This involves Contact Tracing to locate Close Contacts of COVID-19 positive individuals, and includes associated activities. This may include: • reviewing up to date contact details; or • enabling prompt identity verification to expedite community testing of Consumers (with NHI and details available on Consumer device screens) if the Consumer chooses to use this option; • enabling Call Back contact to be requested by a Consumer who has received a Contact Alert, if the Consumer chooses to request that contact; • discussing Locations where an Exposure Event may have occurred (if the individual has chosen to opt in to the Location-related choices); or</td>
<td>Low</td>
</tr>
</tbody>
</table>
they have been and who they have had “close contact” with, particularly over the period of interest (up to 60 days). This means Consumers and therefore Contact Tracers may not be able to identify all of those who need to be tested, and/or isolated. The App Digital Diary feature will enable both scanning of QR Location codes and also manual entry of relevant details by the Consumer.

The type of information being contemplated for collection under the CCTA is aligned with that addressed under Part 3A of the Health Act, subpart 5 – Contact Tracing. This CCTA 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.

The additional functionality provided in Releases 2 and 3 are also aligned with the Contact Tracing options and will remain voluntary.

- Notifications of Exposure Events will occur only if enabled (for iOS) or not disabled (for Android).
- The Upload option for Digital Diary details (both Location information and manual Digital Diary entries) will occur only if the Consumer chooses to Upload this information when asked by a Contact Tracer.

The Release 4 option enabling a Consumer to choose to add their NHI and use it at the time of seeking a COVID-19 test, and also to receive a Call Back after receiving a Contact Alert are all still optional for the Consumer and remain voluntary.

- identifying potential Close Contacts using Digital Diary entries as a prompt.

The Consumer contact information supplied is necessary to meet this purpose, as set out in Appendix Two paragraph 6.

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.

*Necessary*

The original Digital Diary information was to be automatically deleted after 31 days. In accordance with further clinical advice from the Contact Tracing team it has been identified that 60 days worth of Digital Diary records may provide additional valuable information to identify the source of an original infection. The time frame for automatic deletion has now been extended to 60 days as it is considered information related to the additional two incubation period is necessary to assist with Contact Tracing.

One potential challenge created by the addition of free field text entries for the Digital Diary is that individuals can put as much information as they wish (up to the character limit) and are not constrained in the information they wish to include. This means that the App features themselves do not, in this instance, limit the information fields that can be included in the recording. 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 the significant mitigation feature that the information will not leave the Consumer’s device for review by a Contact Tracer unless they choose to Upload it in response to a Contact Tracer Request.

- Part of the Contact Tracer training will be to reinforce 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).
- The Digital Diary itself will have a prompt immediately above the ‘Add entry’ screen stating ‘Describing who you were with and what you were doing can help the Contact Tracing team if you share your diary’.
- Release 4 has added an edit feature for Consumers to update or delete entries – this will enable the Consumer to review the data they have collected on the Digital Diary and modify it if necessary to remove any
information they did not wish to share (if they were requested to Upload).

**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.

| Rule 2 | Source of information | A Consumer is the voluntary source of their personal and contact information collected by the application. This is compliant with HIPC Rule 2. Information about a Location a Consumer has attended will be sourced via the App Location scan (if the Consumer chooses to release the recorded details, either by verbally advising a Contact Tracer or choosing to use the Location data upload).

The 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 information is used as a memory aid to help identify Locations, and therefore potential Close Contacts if requested under 92ZZC.

In Release 2 and Release 3 Consumers can use the App on their mobile devices to scan Locations and manually record information in their Digital Diary if they so choose. The App functionality to Upload Information is voluntary as to whether the individual forwards the electronic copy of information that has been collected on their Digital Diary. Even if the Consumer does not agree to Upload the information from their mobile device it could be used as a reminder to the Consumer in their discussions with the Contact Tracer. | The collection of information for Releases 1 to 4 inclusive is consistent with Rule 2 as the information, in every instance of collection associated with the CCTA, is collected directly from the Consumer.

The Consumer still has the choice whether to advise the Contact Tracer of visited Locations or relevant information from their manual Digital Diary entries verbally over the phone, or to release that information via the App Upload feature. This retains some control of the data with the individual. However, the Consumer’s independent obligations under clause 92ZZC(3) remain.

It is also noted that some of the manual Digital Diary entries may include information about other individuals that the Consumer has been in contact with if that information has been recorded by the Consumer. If that information were to be uploaded after a request by a Contact Tracer then potentially information will be collected about third parties, rather than directly from those third parties. In these circumstances it is not reasonably practicable to collect information from those third parties as they are unknown to the Contact Tracer. 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, under Rule 2 it is an exception to the rule if compliance would prejudice the purposes of the collection or the safety of any individual. In the case of potential Close Contacts it is considered that Rule 2 will be complied with. |

Low
**Rule 3**  
Collection of information from individual  
- Tell them what you’re going to do with it  

The Ministry will take all reasonable steps to ensure any Consumer of the CCTA is aware that:  
- information is being collected,  
- the purpose of the collection and  
- the intended use, and users of the information.  
- The expiry and destruction of the information  

The individual will also be made aware:  
- of the name and address of the collecting agency and the agency that will hold the information,  
- That the supply of the information to the CCTA is voluntary  
- When the supply of information may become mandatory under section 92ZZC of the Health Act (and any consequences of not supplying the information), noting that the CCTA is not specifically part of the mandated legislation.  

**Privacy Statement** Material has been developed by the Ministry and is available in the App, to ensure that individuals are aware of the purposes of collection and the possible recipients of the information.  

The Privacy and Security Statement reflects the Rule 3 requirements.  

It also references the Privacy Impact Assessment on the Ministry website. The first version of the Privacy Impact Assessment will be replaced with this third version prior to Release 3 being activated in the App.

**Rule 4**  
Manner of collection of information  
- Be considerate when you’re getting it  

The Ministry will not collect personal information by unlawful, unfair or unreasonably intrusive means.  

The App is designed to be opt-in for all personally identifiable information. The only requirement for creating an account is a valid email address that the Consumer has access to. All additional information collected is on a voluntary basis (other than non-identifiable statistical information).  

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.’  

It would be very difficult to prevent under 16 year olds signing up to the App as there is no verification requirement nor compulsion to submit age. Also, some individuals younger than 16 may

**User Experience (UX) Design** The approach taken by the Ministry is to use UX design processes and to collect anonymous information from Consumers in order to ensure that information is collected as efficiently as possible. Feedback will be used from App use (both analytics and email feedback – see below) to make enhancements to the way the App operates.  

**Feedback Email** The Ministry is providing a feedback email address to receive and incorporate feedback from Consumers to improve utility and equity.  

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.
travel independently from their parents and they may wish to collect Location information on their personal device. If they are identified as under 16 years old by a Contact Tracer the representative of the young person can be consulted where appropriate.

### 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 1993 and Health Information Privacy Code 1994.

  Contact details will be stored by the CCTA Platform and made available to NCTS for search purposes (read only access). All of this information is held securely in compliance with Ministry of Health standards. Measures are in place to protect Consumer information from unauthorised access.

  Consumer details will be stored either on their device (in the case of the Digital Diary scanned Locations and manual entries) or securely on the CCTA Platform based on Amazon Web Services, Sydney, Australia for the New Zealand Ministry of Health (for contact details).

  Some data directly relevant to COVID-19 positive cases, and Close Contacts will also be sent to and stored within the NCTS in individual cases. This includes contact information where this information was otherwise unknown and a Contact Tracer has checked its accuracy and relevance to a case. It will also include selected Digital Diary data if a Consumer has chosen to use the ‘upload’ function when contacted by the Contact Tracer, and the Contact Tracer has decided the specific information is relevant to the Contact Tracing processes associated with that Consumer.

  Information on NCTS will be encrypted in transit and all personally identifiable, clinical and diagnostic data is encrypted in the NCTS. The NCTS operates on Salesforce Service Cloud on a

### Review of Architecture
This has been completed using the standard Ministry process.

### Review of Security Architecture
This has been undertaken by the Government Communications Security Bureau’s National Cyber Security Centre and by an All of Government independent organisation.

### Review of Security Implementation
The Ministry has used an All of Government supplier that is independent and has experience working in the health system.

#### Access Controls
Access to the CCTA Platform and NCTS by specific Ministry staff and suppliers is permitted for production support. This access is logged and audited.

Consumer access to App information held on their device or stored information held about them is by email address and password. Consumers are also able to enable two-factor authentication for additional protection. A ‘password manager’ functionality will also be enabled on the App to enable the email address and password to be stored securely on the Consumer device. This will be an opt-in choice for the Consumer if they wish to use it.

Any interactions involving the interfaces with NCTS for review of CCTA contact details or Locations will be managed securely within the AWS Platform for the CCTA, and the security features applied to the NCTS.
secure AWS platform based in Sydney.

This CCTA application has been through a number of independent security reviews:

- Source code and high-level architecture review from the Government Communication and Security Bureau’s National Cyber Security Centre
- security review of cloud environments that the application is deployed to by a company contracted to government
- security review of the application source code and penetration testing by another company contracted to government

The Ministry continues to have new features and significant updates independently security reviewed before deployment into production.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Access to personal information</th>
<th>Views of personal details provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>People can see their health information if they want to</td>
<td>The Consumer will be able to see their own personally identifiable contact information they have supplied in the user interface. any other information the Consumer has recorded on their mobile device via the App (Digital Diary entries, being Location scans or manual entries) will be visible on the device for 60 days from the date of recording. Only contact details or data the Consumer chooses to Upload will be held by the Ministry. This information will be available via access request to NCTS/Ministry.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Correction of information</th>
<th>Personal details provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>They can correct it if it's wrong</td>
<td>The Consumer will be able to see and modify or remove personal, identifiable contact information supplied in the user interface. For any Uploaded information that is then entered on the NCTS standard Ministry policies will apply about access to and correction of information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Accuracy etc. of information to be checked before use</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Make sure health information is correct before you use it</td>
<td>There are some potential accuracy challenges caused by the manner of information collection (including the lack of verification requirements, and choice of options with the privacy enhancing features of the CCTA).</td>
</tr>
</tbody>
</table>

Low

Low

Medium
Contact Tracer is not otherwise able to find contact details for a Consumer. The Contact Tracer will check these details directly with the Consumer prior to entering any of them into the NCTS record for the case.

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. The CCTA will have no control over the accuracy / completeness of the data Uploaded.

The additional Release 4 ‘edit’ feature for the Digital Diary will enable the Consumer to correct their information if required. If, for example, they have selected an incorrect date for a manual entry they will be able to amend that by selecting the edit button in the manual entry screen. A scanned entry may also have an additional note added to provide context to the entry.

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 before further use.

Noting the importance of the NHI as a unique identifier in the health system, the ability for a Consumer to add their own NHI details into their device creates a potential accuracy challenge. Inaccuracy could arise if a Consumer adds details that are not an NHI number (they may mistakenly assign an alternative series of figures that are unrelated to the NHI) or they may not accurately enter the details (for example transpose figures).

In mitigation of this risk:

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:

**Personal details provided** The Consumer will be able to see and modify or remove personal, identifiable information supplied in the user interface. Release 4 has implemented the editing option, enabling individuals to change / delete information added into the Digital Diary. This will enhance the opportunity for the Consumer to maintain accurate Digital Diary Records.

**Contact Tracer Review** will be used to ensure the information is accurate and matches to the correct person before use (where possible – if contact details are incorrect the Consumer may not be identifiable until the Consumer has been located by other means). This statement applies both to information provided by Consumers about themselves and to information they may provide about Locations.

**NHI Use:** As the NHI is a unique identifier within the health system it is essential that it is correctly assigned to the right individual. If the wrong NHI was added to a test, and a positive result was returned, it may be initially assigned to the wrong individual.

Community Based Assessment Centres will be required to use standard channels available to health professionals to check the NHI against the Consumer offered version. Name, and date of birth and contact details are also collected as part of the testing process, so even if an NHI was incorrectly recorded on a laboratory test form those other details would enable identification of the correct individual.

**Quick Scan when logged out:** If a user is logged out by the App they are still able to scan using the camera, with the Record a Visit button, They will therefore be able to maintain their Digital Diary until they are able to log in again. As the log out is often discovered when a Consumer is attempting to scan a Location, and Consumers do not always have the password immediately available to log in, this quick scan Record a Visit feature will enable the user to maintain a continuous record. This option will not be available if a user deliberately logs off (as they have made the choice to do so), nor when there are multiple Consumers with Digital Diary access (to avoid the scan being recorded to the wrong account).
- no treatment would be provided to an individual based solely on their self-recorded NHI. All test takers (such as Community Based Assessment Centres) would still be required to verify the NHI on standard health provider pathways prior to assigning an NHI to the relevant test.
- The Ministry will be sending a communication to Community Based Assessment Centres to advise them of the App My NHI Details screen and that they need to continue to complete their standard checks to verify the person’s identity.
- A ‘how to’ guide is being developed for CBAC staff on how to either tell people, ‘this is your NHI, add it to the App’, or ‘do you have your NHI in your app? Then let me check that is correct’.
- The App screen itself will explain to a Consumer how to identify their NHI.

The Ministry does not have full control over allocation and use of the QR codes. 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 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 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.

A 'Call Back' function will also be added to the Contact Alert Notification process where an authorised Contact Tracer identifies a high risk of exposure to unknown individuals at a Location. This will enable individuals to have direct contact with the Contact Tracing related services to address any concerns the Consumer may have, and connect them directly with a Contact Tracer to analyse the actual risk they are a Close Contact and may need to be self-isolating and monitored.

Release 2 will not include any 'sign out' time from a Location but this may be considered for future releases (noting also that a Consumer may forget to use it and not sign out).

Release 3 has the option in the manual Digital Diary entry for date entries, which can be set by the Consumer for the present or the past (but not more than a day into the future). This also does not have a 'sign out' time field, but a Consumer could add one in the notes section if they wished.

<table>
<thead>
<tr>
<th>Rule 9</th>
<th>Retention of information</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Get rid of it when you’re done with it</td>
<td></td>
</tr>
</tbody>
</table>

Consumer contact information is held on the CCTA AWS Platform for the duration of the pandemic and deleted thereafter.

Digital Diary information (on visited Locations and manual entries) recorded by a Consumer will be stored on their device and will expire on a rolling 60-day basis. This has been expanded from the original 31 day period as Contact Tracers have indicated.

Data Governance This group will be responsible for ensuring that personal contact details and any other data is deleted at the end of the pandemic.

Database Configuration There is a standard feature that will delete Digital Diary information on the Consumer's device after 60 days.

Low
value of being able to look back further for contacts during an outbreak situation to assist with identifying the source case. The additional time includes up to four incubation periods. Consumers retain the option to delete entries if they wish, or to not Upload information when requested, and provide details only for a shorter period.

The NHI (if the Consumer chooses to record it in their device) will remain on the phone until the Consumer deletes it or the App is deleted from the device. It is not uploaded by the Consumer.

A Consumer may have an interaction with the NCTS:

- A Contact Tracer may locate a Consumer using the contact details they have provided through the App.
- Information relating to Locations or Close Contacts of a positive case, if relevant and provided as part of a Digital Diary data Upload, may be entered into the Consumer’s NCTS case record.

If that 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 will be stored in accordance with the Health (Retention of Information Retention) Regulations 1996.4

If the information is not part of the NCTS case record, then any identifiable information supplied to the NCTS via the App 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 a potential Exposure

---

Event by a Contact Tracer will not be entered into the NCTS (and will be deleted on a regular basis – currently planned as a 6 month rolling deletion). This will also apply to any manual Digital Diary information that is not found to be relevant to the Consumer’s case.

<table>
<thead>
<tr>
<th>Rule 10</th>
<th>Limits on use of information</th>
</tr>
</thead>
</table>
| - Use it for the purpose you got it | Consumer information obtained via the CCTA will only be used for the purposes of the COVID-19 pandemic response. The Privacy Statement provides: Any personal information you share through NZ COVID Tracer will be used only for public health purposes related to contact tracing, during the COVID-19 pandemic response. The information will not be shared with other government agencies except where the agency is directly involved in the COVID-19 public health response. Consumers opt in to the collection of their identifying and contact information by signing up for the CCTA. Consumer choices within the App include:
- To opt in to register with the App
- Which contact and identification details to provide;
- Whether to add their NHI (and whether to show it to any third party);
- What Location data to scan;
- What information to manually include in the Digital Diary;
- Whether to upload Digital Diary information if requested by a Contact Tracer.
- Whether to receive Notifications.
It can reasonably be assumed if a Consumer has opted in to any of these features (or opted not to opt out for Android Notification features), then the Consumer is in agreement with the proposed

| Data Governance | The Data Governance Group will provide oversight of the use of the data to ensure that use matches the purpose | Low |
| Rule | Limits on disclosure of information | Consumer information will be disclosed by the Ministry of Health only for use by the public health system in relation to the COVID-19 pandemic response, for purposes related to Contact Tracing. This is consistent with the Privacy and Security statement. The data collected via the App will not be shared with other Government agencies unless they are directly involved in assisting with the COVID-19 Contact Tracing activities as identified in the Privacy and Security Statement. If relevant to a Consumer who has tested positive for (or is a probable case of) COVID-19, information disclosed to a Contact Tracer 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 CCTA. | Data Governance | The Data Governance Group will provide oversight of the use of the data to ensure that use matches the purpose. Access controls | 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. |
| Rule | Unique identifiers | A unique identifier will identify each Consumer in the database. The purpose of this is to ensure that the personal details provided are only able to be seen by the Consumer. This is also required in order for the database to function and to allow this to be provided to Contact Tracers. This unique identifier used by the CCTA is not connected to the NHI or any other identifier in use in the health system and is purely for the purposes described. The individual will be able to choose to add their own NHI to the App records on their own device, and show it on the My NHI Details screen if they wish. | | | |
Section Four - Intended Future Use Cases

1. The Ministry is committed to exploring best options for privacy protections and ensuring these have been fully canvassed before implementing any new features.

2. Other matters that may form part of the further developments would be fully assessed in a future Privacy Impact Assessment, and include:
   - Improved access to scanning and manual diary entry
   - Equity and accessibility features, including additional language support
   - Interoperability potential with other Apps meeting Ministry standard requirements
   - Bluetooth contact tracing, including possible integration with Apple/Google exposure notification frameworks
   - Surveillance symptom reporting across a wide population
Appendix One – Contact Tracing – the system supported by the CCTA

Background

1. In New Zealand, the COVID-19 pandemic was considered sufficiently serious to impose a nationwide state of emergency under the Civil Defence Emergency Management Act 2002.\(^5\)

2. The Ministry’s elimination strategy is a sustained approach to ‘keep it out, find it and stamp it out’. It does this through: controlling entry at the border with routine quarantine or managed isolation for 14 days; disease surveillance; physical distancing and hygiene measures; testing for and tracing all potential cases; isolating cases and their Close Contacts; and broader public health controls depending on the Alert Level we are in.

3. Contact tracing is one of the pillars of the public health response to this infectious disease pandemic along with border control measures, testing, case identification and case isolation/quarantine. The purpose of Contact Tracing is to obtain information about the contacts of persons with infectious diseases or suspected of having infectious diseases in order to:

   3.1. Identify the source of the infectious disease or suspected infectious disease

   3.2. Make contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary

   3.3. Limit the transmission of infectious disease or suspected infectious disease\(^6\)

4. The Health Act 1956 provides a statutory regime for Contact Tracing. The CCTA is not directly provided for under these statutory provisions, but some of the information collected via the CCTA is aligned with the information used by Contact Tracers:

   4.1. Section 92ZY of the Health Act provides that the purpose of Contact Tracing is to obtain information about the contacts of persons with infectious diseases or suspected of having infectious diseases in order to:

      4.1.1. Identify the source of the infectious disease or suspected infectious disease

      4.1.2. Make contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary

      4.1.3. Limit the transmission of infectious disease or suspected infectious disease

---


\(^6\) Section 92ZX of the Health Act 1956
4.2. Section 92ZZC provides that individuals with an infectious disease, or suspected of having an infectious disease, may be required to provide the name, age, sex, address and contact details of any contact.

5. Once a person is identified as having tested positive for COVID-19, or is a probable case of COVID-19, Contact Tracing will commence to identify Close Contacts. This supports the ‘find it and stamp it out’ component of the Ministry elimination strategy.

5.1. Trained Contact Tracers will contact the infected person directly to ask questions, in line with their responsibilities under subpart 5 of Part 3A of the Health Act. Contact Tracers need to identify Close Contacts promptly to reduce the risk that the infection may spread further, and to ensure people get the best advice as quickly as possible. Close Contacts are those individuals at higher risk of being infected.

5.2. Contact tracing includes a phone call from a Contact Tracer to the Close Contact to provide advice on self-isolation and checking on health and wellbeing. It is therefore important that the Contact Tracer can promptly identify Close Contacts and quickly make contact with them.

5.3. The infected person does not always know the identity of individuals who may be Close Contacts, for example they might have attended an event or a workplace with others they did not know. Alternatively, they might know who the individual is, but not how to contact them. Sometimes it may be difficult to contact an infected person or a Close Contact if, for example, they are travelling.

6. The Ministry has access to the National Health Index (NHI) and the National Enrolment Service (NES). These services allow the Ministry to identify and locate a majority of New Zealanders for Contact Tracing purposes, and are being used as part of the NCTS process. However, a number of limitations have been identified, including:

*Incorrect contact details of Consumers and Close Contacts*

6.1. Consumers who have changed their contact details since they were last updated in the NHI or NES services, or who may not be residing at their usual address. The impact of this is that Contact Tracers may find it more difficult to contact the person concerned, delaying the process of managing their self-isolation, and Close Contact identification, or they may not be able to locate them at all.

6.2. If the infected person or a Close Contact has independently submitted their contact information via the CCTA, then these contact details can be accessed by a Contact Tracer if they had not been able to locate them promptly via the standard processes.
Inability to identify Close Contacts

6.3. Consumers have difficulty remembering where they have been and who they have had ‘close contact’ with, particularly over the period of interest (this could, on occasion, be up to 60 days if the source contact has been difficult to identify). This means Consumers and therefore Contact Tracers may not be able to identify all of those who need to be tested, and/or isolated. This is even more of an issue when New Zealand is at lower Alert Levels, as Consumers will be more mobile.

6.4. The use of the CCTA to keep a record of their visits to participating Locations that display an appropriate QR code, or notation on the Digital Diary feature, to be maintained by each Consumer on their own device, may assist them as a memory prompt.

7. The Ministry has identified the CCTA as being able to support some aspects of Contact Tracing. This includes the potential to enable faster contact with Consumers who may be Close Contacts by providing access to up to date contact information, and also by enabling Digital Diary recording, and Notification of applicable Exposure Events.
Appendix Two – the detail of Release 1 Operations

1. This section explains the features of Release 1 including:
   - personal contact and demographic details
   - visited Locations and
   - anonymous statistical information.

**Personal contact and demographic details**

*Sign-up process*

2. Consumers are able to sign up to the Website or App using an email address of their choosing. They will be asked to confirm (via a code sent to that registered email address) that they control this address. This email and password will prevent unauthorised users from accessing the information the Consumer provides.

3. A second layer of protection will allow the use of a Time-Based One Time Passcode (TOTP) in order to further protect the account from unauthorised use (commonly described as “multi-factor”).

4. Consumers can subsequently choose to add their name and current phone number.

5. A component of the CCTA is to gather limited personal and contact information including a Consumer’s phone number, email address, address details, gender and ethnicity. All of the information provided by the Consumer to the Ministry of Health is done so voluntarily. This information is used to:
   - Increase the speed and the reliability with which a Consumer is contacted in the case of having a positive test result or being a Close Contact.
   - Help ensure that the overall service that is delivered by the Ministry is accessible to all parts of New Zealand.

6. Consumers will also be able to add and update this personal demographic information to assist in identifying the correct individual, and their relevant contacts. The Consumer identification and demographic information to be collected has been determined to be necessary for the purpose of the public health response to the COVID-19 pandemic in New Zealand as follows (noting that only the email address is compulsory to participate in the App):

<table>
<thead>
<tr>
<th>Data</th>
<th>Compulsory</th>
<th>Purpose / necessity</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>No</td>
<td>To identify the individual</td>
</tr>
<tr>
<td>Middle Name</td>
<td>No</td>
<td>To identify the individual</td>
</tr>
<tr>
<td>Last Name</td>
<td>No</td>
<td>To identify the individual</td>
</tr>
<tr>
<td>-----------</td>
<td>----</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>No</td>
<td>To identify the individual. The year of birth may be used in aggregate reporting on usage of CCTA across the population.</td>
</tr>
<tr>
<td>Gender</td>
<td>No</td>
<td>To identify the individual. Some people share the same name. Asking for gender helps to ensure we contact the right person. Gender may be used in aggregate reporting on usage of CCTA across the population.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>No</td>
<td>To identify the individual and allow contact to be made</td>
</tr>
<tr>
<td>Current/Permanent Address</td>
<td>No</td>
<td>To identify the individual and allow contact to be made. Post code and/or Region from address may be used in aggregate reporting on usage of CCTA across the population</td>
</tr>
<tr>
<td>Email address</td>
<td>Yes</td>
<td>Required to create an account. Also used to identify the individual and allow contact to be made</td>
</tr>
<tr>
<td>Ethnicity</td>
<td>No</td>
<td>This is to allow the Ministry to understand whether the services provided (information to support faster Contact Tracing) are equitable. This will help the Ministry confirm it is serving all New Zealanders and is obtaining sufficient population coverage from an equity perspective.</td>
</tr>
</tbody>
</table>

7. Contact and demographic data will be sent to the NCTS via a secure file transfer mechanism. Contact Tracers will have access to this information as a searchable function in the NCTS, similar to those used with the NHI in the health system. This access will be subject to the existing policies and controls relating to the NCTS, and will be secure read-only access to the CCTA Platform in response to a specific request about an individual.

8. If a Consumer decides to complete the My NHI Details fields, the NHI will not be included in this contact and demographic data. If the Consumer chooses to ‘Add’ their name and date of birth on this screen, these will populate the corresponding fields in the contact and demographic data.
9. Consumers can choose to recommend the use of the CCTA to their whānau and friends by sharing a link on their Facebook and/or Twitter account.

10. Registered Consumers may also receive official updates about Contact Tracing and other relevant information from Government sources, including updates to the Privacy Statement if required.

**Sign-up Flow**

Figure 1 represents the ‘normal’ process flow of signing up to use the COVID-19 Contact Tracing App.

![Figure 1: overview of the sign-up flow](image_url)

11. All Consumers will be required to confirm their email address using a unique code sent to them via email before being allowed to log in.

12. During registration Consumers will be prompted to enter their name and a phone number. This has been identified as the highest value information type for Contact Tracers to get in touch with someone who has been identified as a Close Contact of a confirmed or probable case of COVID-19. This step is optional but recommended.
Reset Password

13. The Consumer may reset their password to continue using the CCTA.

14. Password reset requests will be authenticated using the Consumer’s email address.
Consumer’s Personal Information and Contact Details

15. The Register Details flow provides the Consumer the ability to provide relevant personal information. Contact Tracers require this information to get in touch with any person who has been named as a Close Contact of a confirmed or probable case of COVID-19.

16. Completion and confirmation of the Consumer’s details in the Register Details flow results in these details being Registered.

Consumers Current Residence Details
17. The Register Address flow provides the Consumer the opportunity to complete address details of where they are currently staying and, if they are not staying at their home address, their home address details as well. This function is not for collecting Locations the Consumer has visited.

18. This flow uses the Health Identity eSAM Address Web service to provide auto-complete address information. eSAM uses data from NZ Post, Land Information NZ, Statistics NZ, and the Ministry of Health to provide accurate and standardised address and geospatial data. Use of this service is optional, and Consumers may also enter their address manually or by selecting it on a map.

Figure 4: Register Address flow

19. If the Consumer does not know their current address, they can use the ‘location’ function on their smart device to pin and confirm their current location.
**Visited Locations**

20. QR codes displayed at the premises of participating businesses, other groups and organisations can be scanned by Consumer’s with the App⁷.

- This QR Code will contain information about the specific Location, including a Global Location Number (GLN).

- These GLN will be used to represent a Location, or sub-Location, of a business, group or organisation. They will be low cost in terms of a PDF to print out and locate in an appropriate spot (or spots) on their premises.

- These GLNs are linked to an organisation’s New Zealand Business Number (NZBN), where available. It is expected a number of businesses may find the GLN beneficial, as a visible signal that they are taking all reasonable steps to keep their customers safe.

21. The App will record the GLN and the ‘check-in time’ when the Consumer scans the QR Code. All scanning is a manual process initiated by the Consumer.

22. The Location Check-in flow has the following screen flows:

![Figure 5: Location Check-in Flow](image)

23. The App will hold Location information on the Consumer’s device for 60 days before deleting it.

---

⁷ This feature has been expanded into the use of a Digital Diary in Release 3. This is set out in more detail in Appendix Four
Anonymous Statistical and Performance Information

24. In order to provide inputs into reporting on the performance of the end-to-end contact tracing process, the Ministry uses a service (Amazon Pinpoint) to collect and analyse anonymous details about the use of the CCTA service. The data collected by Amazon Pinpoint is stored separately in the Ministry AWS environment. It is not possible for this data to be linked to personal information collected by the CCTA. The Amazon Pinpoint service collects the data outlined in the table below by default, which is automatically attached to any analytics events captured in the CCTA.

<table>
<thead>
<tr>
<th>Data</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address of the device</td>
<td>To allow the Ministry to identify opportunities to improve the service</td>
</tr>
<tr>
<td>The pages/screens accessed on the App or the Website</td>
<td>To allow the Ministry to identify opportunities to improve the service</td>
</tr>
<tr>
<td>The date and time the App was used or the Website was visited</td>
<td>To allow the Ministry to identify opportunities to improve the service</td>
</tr>
<tr>
<td>The referring site (if any) through which the Consumer clicked through to the Website</td>
<td>To allow the Ministry to identify opportunities to improve the service</td>
</tr>
<tr>
<td>The operating system (for example Windows 10, iOS, or Android) on the device used</td>
<td>To allow the Ministry to identify opportunities to improve the service</td>
</tr>
<tr>
<td>The type of web browser and/or device used (for example, iPhone 8, Internet Explorer, of Google Chrome)</td>
<td>To allow the Ministry to identify opportunities to improve the service</td>
</tr>
<tr>
<td>Other incidental information such as screen resolution and the language setting used</td>
<td>To allow the Ministry to identify opportunities to improve the service</td>
</tr>
</tbody>
</table>

25. Analytics events may also be captured at key stages of the App and Website experience. These events are used to provide reporting into the effectiveness and performance of the CCTA and the Contact Tracing end-to-end service model. Specific events include:

- When the Consumer uses the ‘scan location’ feature, an event may be recorded that a scan has taken place. No information about the Location of this scan or the identity of the Consumer will be recorded. It is not possible to use this event to reconstruct a Consumer’s movements or track where they have been. Information about recorded Locations remains on their device.

- When a matching Exposure Event of Interest is found on the Consumer device, an event may be recorded noting that a match was made and Contact Alert was
opened. This event does not record the identity of the Consumer, nor any information about the Exposure Event itself. It is not possible for the Consumer to be contacted as a result of this event being recorded.

- Events may be triggered when the Consumer navigates to different parts of the CCTA application. The information recorded in this event does not contain personally identifying information.

26. To assist the Ministry to diagnose performance and stability issues on mobile devices, the App may send data about application crashes to a service operated by Microsoft called App Center. This data contains information about the state of the App before the crash occurred and provides insight for the Ministry and its suppliers to diagnose and fix issues that occur across the range of supported devices. When a crash occurs the following data is sent from the device to App Center:

- **Install information**: An Application Secret and an Installation Identifier are sent with every request so App Center can identify the data and attach it to the Ministry account.

- **Device data**: This data includes information about the device itself, including the Operating System name and version (e.g. iOS 12, Android 7), device model and manufacturer, installed app version, carrier, screen size, and whether the device is jailbroken or not.

- **Crash and error logs data**: This data includes the ID and name of processes, threads and frames related to the crash, the exception type and message, and the device data (outlined above).

Full details on the information which App Center can collect can be found on the App Center website. Note, the Ministry does not associate a User Identifier (userId) with data collected by App Center, so crash data cannot be linked back to an individual user.

27. The CCTA uses a hosted Content Delivery Network (CDN) operated by Google to serve the font files and other static assets used to render the application. The Google Fonts API is designed to limit the collection, storage, and use of end-user data to what is needed to serve fonts efficiently. Google may record a Consumer’s IP address and other device information (as set out in their FAQ). However, personal data, recorded Locations, or other information collected in the CCTA is never shared with Google.
Appendix Three – the detail of Release 2 Operations

1. This section explains the features of Release 2 including:
   - Notification of a potential ‘Exposure event’; and
   - Location ‘data upload’ capability (with Release 3 the Upload capability will include all Digital Diary entries).

   Exposure Events

2. Contact Tracers may receive information about scanned Locations attended by a case, either by direct contact with the infected individual or using the Digital Diary Location data a Consumer chooses to upload (discussed further below). The Contact Tracer may identify any Exposure Events that are likely to have created a risk of potential exposure to any Close Contacts.

3. A specialist public health clinician will decide whether to create an Exposure Event of Interest (EEOI) for the purposes of notifying all Consumers via the CCTA. These EEOI events are generated by application of clinical expertise, not automated.
   - This will involve speaking with the Consumer to confirm appropriate timeframes and behaviour at a relevant Location to ensure that only those Locations visited by the COVID-19 positive individual where there was likely to have been Close Contact exposure are selected.
   - There are features that make activity at a Location more likely to create risk of Close Contact, for example indoor locations, and length of time at the Location. The definition of a ‘Close Contact’ on the Ministry website indicates those that are at higher risk of being infected. Just passing through a Location is not enough to assume a genuine risk.
   - It is a challenge to provide the Exposure Notification only to those Consumers who are realistically at risk (rather than over-advising risk and creating greater anxiety than necessary) balanced against missing those who could be at risk.
   - The clinician involvement in determining if an EEOI is appropriate, and setting relevant time frames, will help balance that risk. It is noted that the App Location scan information held on the device will only record the time of the scan. The expertise of the Contact Tracer and the discussion with the positive case is key in setting the appropriate time frame.
   - The Location will also need to have a GLN location registered with an official NZ COVID Tracer QR Code to be included in an EEOI, otherwise there will not be a matching Location on any other App user devices capable of receiving a Notification for a Contact Alert.
   - The general communications to Consumers at the time of a Notification are designed to alert people but not alarm them.
The Notification alert will link to a webpage with relevant information designed to provide additional details and manage expectations and anxiety for a Notification recipient.

This will include a reference to call Healthline if the individual has questions or considers that they may be experiencing symptoms.

If the EEOI is considered to be a higher risk by Contact Tracers a Call Back will also be enabled.

4. An EEOI therefore will represent a specific Location and time range, identified during the investigation of a confirmed or probable case, where there is a specific risk of transmission of COVID-19.

5. A decision by the clinician to create an EEOI will enable the relevant Location information to be prepared within the NCTS for consumption by the CCTA. The NCTS will create a Notification to be published to a register within the CCTA platform.

6. The process flow will be as identified in the diagram below:
Consequence of Notification - Contact Alert

7. The Contact Alert is delivered to Consumers through a 'silent push notification' mechanism, after the Consumer has opted in to enable push Notifications on their mobile device (or chosen not to opt out for Android devices). If a Consumer chooses not to enable push Notifications, or they choose to later disable them, they will not receive Contact Alerts.

8. When a Consumer permits push Notifications this will grant permission for the CCTA to request a 'push token' and enrol their device for push Notifications. This push token is then registered with Firebase Cloud Messaging (FCM), a push notification service operated by Google that provides a single interface to deliver push Notifications for both iOS and Android. On iOS devices a push token is obtained by requesting it from Apple Push Notification Service (APNS), before it is passed to FCM.

9. When an Exposure Event of Interest is published from NCTS, a silent push Notification will be sent to all registered devices on the CCTA through FCM. If a device is offline, the Notification may be queued for delivery later. This push Notification process will be subject to any limitations of the underlying operating systems, if for example a device were not turned on for a period of time or did not connect to the internet. This type of Notification is in widespread use and is generally considered reliable.

10. Upon receipt of an Exposure Notification, the Consumer’s mobile device will perform a check to determine if there is a matching Location stored on the device within the last 60 days.

- If multiple people have used the same device, all recorded Locations will be checked
- A match will be determined if the following conditions are true:
  
  o The GLN identifier of the EEOI matches the GLN of the recorded Location (or location selected by the clinician sending the EEOI if it was not received via the CCTA Location upload process).
  
  o The date and time range of the EEOI will be compared with the recorded Location date and time range (the check-in time on the Consumer’s device). It is up to the Contact Tracer to set appropriate time frames.

11. This comparison happens in the background of the device, and if no recorded Location matches the EEOI, the Consumer is not alerted to the process. All devices that have opted in to receive push Notifications will receive the silent push. This enables the Consumer device to "wake up" in the background to check the locally recorded data.

- If a matching GLN is found on the device within the time range, and the Consumer has not previously been alerted for this EventId (a unique identifier for the event that is used to prevent duplicate Notifications for the same event on the same device), a local notification is presented to the Consumer as a Contact Alert. This will prompt the Consumer to open the app for more information. The EventId is recorded on the
device so future notifications for the same EventId do not result in another local notification.

- If no match is found, all information from the push Notification is discarded and no further action is taken.

- If there is a match, the Contact Alert shown to the user does not disclose the location name, the time of the exposure event, or any other details specific to the event.

12. If a matching check-in is identified, a flag will be written to the local data store on the Consumer’s device. In a scenario where the device is being shared by multiple Consumers, the flag will only be attached to the Consumer(s) who recorded the matching Location. A ‘local notification’ will be shown on the device if the currently logged-in Consumer was one with a matching Location. This ‘local notification’ will prompt the Consumer to open the CCTA for more information.

13. Once the Consumer has opened the App, and logged in if they were not already, the flag from the previous step will be checked. If it is for the logged-in Consumer, a screen will be shown informing the Consumer of their potential exposure to COVID-19. This Contact Alert screen will include:

- A Call Back feature. This will only be enabled if it is a high risk EEOI (as determined by Contact Tracers).

- Appropriate advice that the person may have been in contact with COVID-19 and a link to a specific webpage.
• This webpage is designed to ensure that a recipient does not experience unnecessary concern and has an immediate ‘plan’ available for them to review. The webpage will provide advice, including that the Consumer should contact Healthline if they develop any symptoms.

  o Contact a Consumer may choose to initiate with Healthline will occur independent to the Notification process. Any call will be managed as would any other call to Healthline for assistance with a COVID-19 related matter. It is noted however that an indication that the individual felt unwell after receiving an App related Notification may be considered a clinical indicator to suggest the person gets tested.

  o Contact Tracer contact would be made to Healthline management to indicate that the Notification process had been initiated if it was likely that any increase in queries may result, to ensure appropriate resourcing was available.

• The Consumer Notification will not include any details of the Location at which they were potentially exposed. No information about the person who tested positive, or other Consumers at the same place at the same time, will be shown to the Consumer.

14. There is no compulsion for the Consumer to follow any advice given. If they do not choose to seek assistance when appropriate, the App itself will not be able to disclose their identity to any other party – including a Contact Tracer.

15. An anonymous analytics event may be captured to record that a local match (to the Location data on a device) was made, in order to provide reporting on the effectiveness of the solution and help Contact Tracers understand the scale of an Exposure Event. The data captured in this analytics event cannot be used to identify an individual, so therefore cannot be used to make contact with them.

Locations

16. Contact Tracers will be in independent contact with Locations where there has been an Exposure Event to identify if a contact tracing register was available or to obtain any necessary additional information. If the relevant business or organisation is able to identify additional potential Close Contacts the Contact Tracers will make direct contact with those individuals. The standard Contact Tracing measures would apply to avoid identifying an infected individual as far as practicable (as per section 92ZZG).

17. Measures will be taken to prevent the list of Locations with known Exposure Events from being disclosed outside the App.

  • This includes masking the GLN identifiers through a one-way hashing function. If this information was readily accessible, for example on a public website, may be used to stigmatise a business (for having a positive case), causing a potential loss of business, potentially resulting in businesses being unwilling to display a GLN QR code in future.
• It is still possible however that a Consumer receiving a Notification may be able to
independently identify the Location at which they may have been exposed. This will
be the case if the Consumer chooses to activate a Call Back if one is included in
their Contact Alert Notification, as the Contact Tracer will discuss with the Consumer
the Location and data in question to identify the actual risk that they may be a Close
Contact. There is also no restriction on the Consumer commenting publicly on the
fact that they have received a Notification related to a specific Location.
Location data upload capability

18. Under Release 2, a Consumer could elect to send their recorded Location information to the Ministry of Health for access by authorised NCTS users involved in Contact Tracing.

19. This Upload capability has been expanded by Release 3 to include the Upload of all Digital Diary information – both scanned Location details and also the manual entries further described in Appendix Four. This section has therefore been modified to reference the full ‘Digital Diary’ records

- The Upload will be at the request of a Contact Tracer if the Consumer is a positive case. The Consumer can then choose to release the 60 days’ worth of Digital Diary (Location information and manual entries) from their device to the Contact Tracer.

- If a Consumer independently tries to submit Location information without the appropriate code then the NCTS will not record it against any file, it will sit in a secure Salesforce location within the NCTS boundary. The information in this location will be securely destroyed once the information has been held there for a six-month period and remains unused.

20. To properly link uploaded Digital Diary information to the relevant NCTS case record, when the Consumer agrees to Upload it, the Consumer will be required to enter a specific code given to them by a Contact Tracer.

- When a Consumer chooses to share their Digital Diary data, a request including their name and date of birth will be provided to the Consumer. A unique code will read out to them over the phone.

- The Digital Diary entries may contain the following information:
• The GLN of a scanned Location, and the time the Consumer scanned the QR code, and ‘checked-in’ to the Location

• The details of manual entries by the Consumer (as further described in Appendix Four).

- This Contact Tracer provided code will be unique to the Consumer and will enable the Contact Tracer to access the records forwarded to the secure Salesforce location on the NCTS platform, and link them with the correct NCTS case record.

- NCTS will retrieve business information about each Location by using the GLN to query the NZBN and QR Code database, so Contact Tracers have the information necessary to continue their investigation.

- When the Contact Tracer has accessed the identified Consumer’s Digital Diary information, they will then discuss each of the uploaded Locations, and manual entries, with the Consumer to identify how long the Consumer spent at an identified location, what activity they were involved in and who they may have come into Close Contact with.

  o Only information identified by the Contact Tracer as relevant to a potential Exposure Event or Close Contact will then be incorporated by the Contact Tracer onto the Consumer’s NCTS case record.

  o Any uploaded Digital Diary information that has not been incorporated into the Consumer’s NCTS case record will remain in the secure NCTS location and be securely destroyed after six-months.

21. Close Contacts are not requested to submit their information unless they subsequently become symptomatic and themselves become a probable or positive case).
Appendix Four – the detail of Release 3 operations

1. Release 3 will enhance the Digital Diary features of the App. In addition to the existing Location scan features, Consumers will now be able to add manual Digital Diary entries.

2. The Digital Diary will help individuals retain records to identify places they visit, people they have been in contact with, or activities they have undertaken such as travel on the bus to work, or attending the local school football match at a local park.

3. The Consumer will be able to choose what they enter, and how much detail they record into the Digital Diary. The limitations will be in the character limits imposed for recording (for example the character limit for notes is 255), and dates that may be entered. Dates may be entered for past activities (up to 60 days in the past) but cannot record activities in future beyond the current day of entry.

4. All of this Digital Diary information will be retained on the Consumer’s device for a period of 60 days before being automatically deleted by the App (unless deleted earlier by the Consumer).

5. Release 4 has added an edit / delete feature, so that Consumers will be able to delete or amend the manual entries made into the Digital Diary. This edit / delete feature will enable Consumers to amend records if they feel they are inaccurate, or when they no longer want to retain those records.

6. It also remains the Consumer’s choice as to whether they do Upload the Digital Diary if requested by a Contact Tracer, or retain the information on their device and use it as a memory prompt.
Content of Manual Digital Diary entries

7. It is possible that individuals may record information about third parties in their Digital Diary (presumably if they have been in contact with them), but this is consistent with the type of information that the Contact Tracers would request the Consumer to disclose as part of the Contact Tracing process. It is also important that those individuals are identified if they may be at risk of being a Close Contact, which could be a serious threat to their health and those they come in contact with. In the event that there was some sensitivity in any such records the Consumer would be able to edit their Digital Diary entries before Upload if they wished.

8. It is acknowledged that the free text choices may create a challenge for Contact Tracers to follow notations by Consumers. If a Consumer chooses to Upload their Digital Diary when requested, the content will be used by the Contact Tracer to progress their conversation with a Consumer. Only information verified with the Consumer, and relevant to the Contact Tracing process will be transferred onto the NCTS. Digital Diary information not considered relevant will remain in the NCTS secure Upload location, until deletion six months later.

Analytics Events

9. There will also be an analytics event created that a manual entry has been created, but this will not disclose which device the entry was made on (or any Consumer identity or other location details).
Appendix Five – The details of Release 4 operations

**Ability to manually record NHI**

1. Consumers will be given the option to manually add their NHI to the details they have recorded on their device. This will enable them to use the ‘My NHI Details’ screen to display (if they choose) their NHI, name and date of birth.

2. The My NHI Details screen is designed to enable Consumers to swiftly and privately show their details to testing staff if they attend community-based testing facilities (or in other appropriate settings). This was in response to Consumer request via the email support inbox, and confirmed by the COVID-19 Technology Business Design Council.

3. The My NHI Details screen could assist in the identification and testing process, by enabling the Consumer to display the necessary details on their device.
   - This could be privacy enhancing as it would enable an alternative to attempting to speak through a car window and a mask, or when other people are nearby who may overhear the identification details if spoken.
   - It may also assist in speeding up the pre-test identification processes, with a digital recording of name spelling by the Consumer, and an NHI to be checked for accuracy.

4. The NHI will not be verified on the Consumer device – but the Consumer will be told (on screen – as shown in the screen shot below) where they might find their own NHI recorded (for example on a prescription, or hospital letter).

5. The NHI will still need to be verified by any health professional interacting with the individual. A communication will be sent to the Community Based Assessment Facilities to confirm the ongoing obligation to verify the NHI, and a training package provided.

6. The NHI details added into the ‘My NHI Details’ process will not be added to either the contact details on the CCTA platform nor to the Digital Diary Upload information.

7. If the Consumer has already provided name and date of birth details as part of the registration process these details will automatically populate into the My NHI Details screen. If the name and date of birth details have not previously been provided the Consumer will have the opportunity to add them (and those details will then be included as part of the registration details).

8. The screen display is on the following page.
Add NHI

What is your NHI?
The National Health Index number (NHI number) is a unique identifier assigned to every person who uses health and disability support services in New Zealand (e.g., ZZ21234).

NHI number: Required

What is your NHI?
Where can I find my NHI?

You can usually find your NHI on:
- a prescription
- a prescription receipt
- a prescription medicine label
- a hospital letter
- an X-ray or test result

If you still can’t find your NHI, check with your general practitioner or pharmacist.

Thanks for helping stop the spread
Thank you for adding your NHI to help staff at COVID-19 testing sites. Together we can stop the spread of COVID-19.

Get your NHI ready
Have your NHI number on hand when getting tested for COVID-19.

Show my NHI details

My NHI details
NHI number: ABC1234

Full name: Kahurangi Ahataukiwa
Date of birth: 18/08/1995

Register Details

Show this screen to the staff at a COVID-19 testing site to be identified faster.

NHI number: ABC1234

NHI is kept securely on your phone.

Full name: Kahurangi Ahataukiwa
Date of birth: 18/08/1995
Appendix Six – the details of Release 4.2

Call Back Request

1. If an authorised Contact Tracer determines that there is an EEOI Location with a high risk of contacts that cannot be promptly identified, and may be Close Contacts, a ‘Call Back’ option may be included in the Contact Alert Notification. This could include, for example, a café or bar where others attended but they are not known to the case or the business at the Location.

2. The Consumer will be given the option to press the ‘Confirm details’ button (as shown below). This will present an additional screen to the Consumer to enable the Consumer to complete their contact details so that they can be submitted to the NCTS to enable the Contact Tracer to make contact with them (as the Consumer is otherwise unknown to the Contact Tracer).

3. Not all Contact Alerts will have the Call Back option – only those deemed high risk by Contact Tracers.

4. If the Consumer does select a Call Back they will be queued so that a member of the Contact Tracing team can call and speak with them.

5. If a Call Back request is made, the Contact Tracer will be able to identify which case, Location and date was involved from the Call Back request made from the Consumers device, as each EEOI will have a unique code embedded in the Call Back response. The Location and date details will not be available to the Consumer as part of the Contact Alert.

6. If the Consumer chooses not to select the Call Back it will not be possible to identify them through the App. They will however receive the brief message about monitoring for symptoms and calling Healthline as standard for all Contact Alerts.


Extension of the Digital Diary retention period to 60 days

7. The time frame for Digital Diary entries to be stored on a Consumer device has been extended from 31 to 60 days. At 60 days from creation they will be automatically deleted on a rolling basis.

8. Through the experience of the August 2020 Auckland outbreak, Contact Tracers identified the need to look back further in terms of incubation periods to identify a source case (the person the original identified case acquired the infection from). For instance, if a case is diagnosed and it is discovered they had symptoms four weeks (or two incubation periods) earlier, then it would be necessary to look back up to a further two weeks before that.

9. A Consumer is not compelled to upload their Digital Diary if they do not wish to. They can use it as a memory aid instead when speaking to Contact Tracers. They also have the option to delete entries if they choose to.

Ability to record a visit while logged out

10. Consumers are now given the option to record a visit if they have been logged out due to their authenticated session expiring. For most Consumers, they notice they have been logged out when they are attempting to scan a poster or log a manual entry. This can be frustrating and cause unnecessary delay for them to record their visit to a Location.

11. This new “quick scan” feature will allow Consumers to continue scanning provided they:
   - are the sole Consumer using the digital diary on that device,
   - have been using the app to record their visits prior to being logged out, and
   - they have not explicitly chosen the log out option.

12. When in the logged-out state they will have a “Record a Visit” button that allows them to scan a poster or create a manual entry. This will be recorded in their diary and available for review once the Consumer logs in again. It is not possible to review, edit, or delete diary entries while logged out.
## Appendix Seven - Glossary

The following are definitions used in this Assessment:

<table>
<thead>
<tr>
<th>Terms</th>
<th>Description, relationship and business rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>CCTA</td>
<td>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 Platform (Platform) collectively referred to as the COVID-19 Contact Tracing Application.</td>
</tr>
<tr>
<td>Consumer</td>
<td>A user who registers or downloads and signs up to use the NZ COVID Tracer mobile app or website</td>
</tr>
<tr>
<td>Contact Alert</td>
<td>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.</td>
</tr>
<tr>
<td>Contact Tracer</td>
<td>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.</td>
</tr>
<tr>
<td>Contact Tracing</td>
<td>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.</td>
</tr>
<tr>
<td>Digital Diary</td>
<td>The information a Consumer chooses to record on 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.</td>
</tr>
<tr>
<td>EEOI</td>
<td>Exposure Event of Interest</td>
</tr>
<tr>
<td>EEOIN</td>
<td>Exposure Event of Interest Notification</td>
</tr>
<tr>
<td>Exposure Event</td>
<td>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.</td>
</tr>
<tr>
<td>Terms</td>
<td>Description, relationship and business rules</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GLN</td>
<td>Global Location Number.</td>
</tr>
<tr>
<td>Location</td>
<td>The GLN recorded on the Consumer’s mobile device, which includes a date and time of scan.</td>
</tr>
<tr>
<td>NCTS</td>
<td>The National Contact Tracing Solution is the secure technology solution to support national Contact Tracing activities.</td>
</tr>
<tr>
<td>NCTS case record</td>
<td>The NHI linked record that is stored on the NCTS which relates to an individual Consumer who is a positive or probable case.</td>
</tr>
<tr>
<td>NHI</td>
<td>The National Health Index number is the unique identifier assigned to every person who uses health and disability support services in New Zealand.</td>
</tr>
<tr>
<td>Notification</td>
<td>The App notification to Consumer devices which have an Exposure Event matching a Location recorded on that Consumer’s device.</td>
</tr>
<tr>
<td>Privacy Notice Materials</td>
<td>Material to be prepared to inform Consumers in compliance with rule 3 of the Health Information Privacy Code 1994. This is viewable on the Privacy Statement screen on the NZ COVID Tracer mobile app. This will link to a more detailed Privacy and Security Statement. The Privacy and Security Statement will contain a link to the current Privacy Impact Assessment.</td>
</tr>
<tr>
<td>Privacy and Security Statement</td>
<td>The second part of the layered privacy notice. It is linked from the Privacy Statement available to Consumers at registration.</td>
</tr>
<tr>
<td>Privacy Statement</td>
<td>The notice available to Consumers at point of registration with the CCTA.</td>
</tr>
<tr>
<td>Upload Information</td>
<td>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.</td>
</tr>
</tbody>
</table>