

Ministry of Health
National Contact Tracing Solution (NCTS)
Focus: NCTS – Contact Tracing
Privacy Impact Assessment

Date 12 November 2020

Document creation and management

This Privacy Impact Assessment (“the Assessment”) reflects the development of the National Contact Tracing Solution (NCTS) to deliver the technology solution required to support Contact Tracing processes nationally, through the COVID-19 pandemic.

An initial Privacy Plan was prepared following the issue of an epidemic notice under the Epidemic Preparedness Act 2006, which confirmed design decisions and privacy mitigations applicable as the NCTS build commenced. This Privacy Impact Assessment reflects the NCTS in its operational state.

This Assessment will be updated if any significant changes are to occur to the NCTS that will impact on the privacy risks and mitigations identified in this document.

This document will be made publicly available on the Ministry of Health website.

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

- The Office of the Privacy Commissioner
- NCTS Technical Director
- NCTS Manager Technical Initiatives
- NCTS Senior Project Manager
- NITC Clinical Lead for Contact Tracing
- Ministry IT Security Manager

Document Approval

| | Name/Title | Sign-off date |
|--|---|---------------|
| Approved by Senior Responsible officer | Sue Gordon (Deputy Chief Executive COVID-19 Health System Response) | |
| Approved by Business Owner | Astrid Koornneef (Group Manager, COVID-19 Contact Tracing) | |
| Approved by Chief Privacy Officer | Phil Knipe (Chief Legal Advisor) | |

Disclaimer

This Assessment has been prepared to assist the Ministry of Health (“the Ministry”) to review the purposes for which information collected via the NCTS can be used, and the privacy safeguards that are required to manage those purposes. It is not necessary or appropriate to focus on every possible privacy risk (such as the specific details of how security will be applied to the NCTS) but rather the focus is to be on the most critical points of the NCTS.

Every effort has been made to ensure that the information contained in this report is reliable and up to date. No inspection of the NCTS operation or its solution software has taken place and performance representations are as reported to the author with no independent verification of the same.

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

Contents

| | |
|--|-----------|
| SECTION ONE – EXECUTIVE SUMMARY | 5 |
| PRIVACY FOCUS | 5 |
| BACKGROUND | 6 |
| FUNCTION CREEP | 6 |
| CLARITY OF PURPOSE | 7 |
| INFORMATION COLLECTION PROCESSES | 7 |
| ACCESS AND SECURITY | 8 |
| RETENTION | 8 |
| GOVERNANCE | 9 |
| ACTION POINTS | 9 |
| FUTURE PRIVACY IMPACT ASSESSMENT ACTIVITY | 10 |
| SECTION TWO – OPERATIONAL DETAILS | 12 |
| BACKGROUND | 12 |
| OBJECTIVES | 13 |
| INFORMATION COLLECTED AND INFORMATION FLOWS | 13 |
| USE OF INFORMATION: | 16 |
| RETENTION OF NCTS INFORMATION | 17 |
| NCTS SECURITY | 19 |
| GOVERNANCE | 20 |
| SECTION THREE - PRIVACY ANALYSIS | 22 |
| APPENDIX ONE – CONTACT TRACING – THE SYSTEM SUPPORTED BY THE NCTS | 38 |
| APPENDIX TWO – THE NCTS DATABASE FACILITY | 47 |
| APPENDIX THREE – THE TELEPHONY SERVICES ASSOCIATED WITH NCTS | 57 |
| APPENDIX FOUR – THE FINDING SERVICE | 60 |
| APPENDIX FIVE - CCTA INTERACTIONS WITH NCTS | 70 |
| APPENDIX SIX – THE DAILY CHECK-IN | 74 |
| APPENDIX SEVEN – DRAFT INFORMATION AND PRIVACY STATEMENTS | 79 |
| APPENDIX EIGHT - GLOSSARY | 86 |

Section One – Executive Summary

1. The Ministry of Health (the Ministry) has created a National Contact Tracing Solution (the NCTS), to greatly increase the capacity and reliability of Contact Tracing activity, and to support existing regional expertise. The Ministry is satisfied that the NCTS will meet the national information and reporting challenges for contact tracing posed by COVID-19, and will retain a strong focus on security of the information and protecting individual privacy.
2. 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.
3. 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 diseases¹. 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 alone². Further detail about Contact Tracing can be found in Appendix One.
4. It was swiftly identified by the Ministry of Health (the Ministry) that comprehensive national level information was required. The Public Health Units contained skilled professionals, but they were working on a regional basis, had varying capacity to report at speed on responses to COVID-19 and were facing an unprecedented state of emergency.
5. The Ministry was able to rapidly configure the NCTS using the same foundation architecture as the National Screening Solution³, leveraging key elements of the end-to-end architecture and functional solution. This approach has allowed the Ministry to rapidly realise a solution that was able to support the initial critical demand for contact tracing for COVID-19 through a pro-active delegation model. Under this model Public Health Units (PHUs) can delegate Contact Tracing tasks to other PHUs and the Ministry National Investigation and Tracing Centre (NITC) for completion (primarily close contact calling and the 'finder' service for hard to locate Cases and Close Contacts).

Privacy focus

6. The purpose of this Assessment is to review the process of collection, storage, use and sharing of personal and contact information associated with the core NCTS environment. This Assessment will summarise the privacy mitigations and note any relevant new risks and their management. The Ministry will publish this Assessment on its website to

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

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

³ The National Screening Solution (the NSS) is the platform currently supporting the National Bowel Screening Programme. This platform had been subject to extensive Privacy Impact Assessment activity, and security had featured strongly in the design and development. It had successfully achieved 'go live' status immediately prior to the development of NCTS commencing.

provide reassurance to the New Zealand public that the NCTS provides a secure and appropriate solution to the Contact Tracing processes to help in the national response to COVID-19.

Background

7. The original NCTS project related directly to the support of national Contact Tracing activity. This has been provided via the Contract Tracing application supported on the NCTS platform.
8. Due to the secure environment and capability provided by the NCTS platform, this platform is now home to a number of 'collections'. These applications supported by the NCTS platform include:
 - 8.1. NCTS – Contact Tracing – this contains the national electronic database to support contact tracers to keep accurate and secure records of all contact tracing activity. This is the subject of this Privacy Impact Assessment, and this collection has been the key driver of security and management of all NCTS collections.
 - 8.2. NCTS - Border Register – this contains the record of management for COVID-19 as it relates to travellers arriving in New Zealand, and as they are managed through the Managed Isolation and Quarantine Facilities.
 - 8.3. NCTS - Border Staff Testing – this contains the management record for testing of border workforce groups, and is in development.
 - 8.4. NCTS - Managed Isolation Exemptions process – this contains the management record for determining exemptions to the Border MIQF⁴.
9. The Border Register, Border Staff Testing and the Managed Isolation Exemptions Process collections will all be addressed in their own Privacy Impact Assessments.

Function Creep

10. As the NCTS has been developed, it has become widely recognised as a valuable centralised resource with rich detail. This has led to requests from multiple agencies, and internally, for access to the various datasets as roles expand and new measures to control the spread of COVID-19 are rolled out. The greatest privacy challenge for the NCTS will be managing these requests to ensure that the core purposes of the NCTS 'collections' are maintained.
11. This is particularly important as public trust in the activities in the various government agencies is key to a successful response to the virus. People must feel that they can have trust in the systems being used so they remain willing to contribute to, and participate in, the virus response to the fullest extent.
12. The NCTS management of these challenges is an ongoing, and key, focus for the NCTS team. Some features already in place include:

⁴ Managed Isolation and Quarantine Facilities

- 12.1. dividing the collections into the four categories which support discrete projects as noted in paragraph 8.
- 12.2. the creation of strong technical controls to prevent access between collections, and further controls within collections to only the information necessary for the role being performed.
- 12.3. commencing the development of audit and access authorisation review programmes, and
- 12.4. strengthening governance roles and processes.

Clarity of purpose

13. Multiple components intersect with the NCTS in the delivery of Contact Tracing related services. It is essential that all components work to a common, clearly articulated purpose, related to the COVID-19 pandemic. This is both to maintain public trust, and also to ensure compliance with Privacy Act and Health Act requirements.
14. It was determined that this Privacy Impact Assessment would endeavour to analyse all contributing components to the Contact Tracing processes⁵, so that the Ministry could have confidence that clarity of purpose would be maintained.

Information Collection Processes

15. Public facing components⁶ associated with the NCTS (where information is collected electronically directly from Consumers) are expected to have Privacy Statements available to the Consumer as part of their initial registration process.
16. It is recommended that an information sheet, and possibly a Frequently Asked Questions section be created for the NCTS⁷. This would be placed on the Ministry COVID-19 section of the website so that any individual wishing to find out what happens to Contact Tracing information will be able to review that information. It is intended that this Privacy Impact Assessment (once finalised) will also be placed on the website.
17. Much of the personal information necessary for Contact Tracing is obtained under Part 3A of the Health Act (Management of Infectious Disease), subpart 5 (Contact Tracing).
 - 17.1. The approach is to first seek cooperation from individuals, and only use compulsion provisions under the Health Act if necessary. This is particularly important when working directly with individual Cases to identify Close Contacts, as it will enhance public trust, in working towards a common goal – rather than appearing punitive. A more open dialogue is likely to be created,

⁵ Although the work of the Contact Tracers working at the Public Health Units is included in this assessment from the perspective of their interactions with the NCTS, the work within their District Health Board role and interaction with Consumers is not directly addressed in this Privacy Impact Assessment as being outside scope. This is distinct from the Contact Tracers working within the NITC, who will conduct both overflow work for the PHU Contact Tracers, and the finders service.

⁶ The CCTA and the QR Code application and poster generation processes each have Privacy Statements that can be accessed as part of the registration processes. A Privacy Impact Assessment has been completed for each of these components. There will also be a Privacy Statement incorporated as part of the Daily Check-In web interface to be added to the NCTS (draft attached in Appendix Seven).

⁷ Draft attached in Appendix Seven.

potentially generating more useful information if people can be engaged to participate willingly in the Contact Tracing process.

- 17.2. In the interests of creating public trust with third party organisations, however, Contract Tracers may need to remain alert to situations where a third party is being requested to release personal information about another individual. This could include, for example, a request to identify customers who attended an event on a specific date (if the Contact Tracer has identified a risk that other unknown individuals may have been exposed to COVID-19 at that event). That third-party may want the comfort of legislative protection (for example a request under s92ZZF of the Health Act) if they are to release that personal information.
 - 17.3. These variables have been included in the training materials for NITC Contact Tracers (including the surge workforce).
18. The 'Finders' service that is part of the National Contact Tracing Service performs key investigation activities to identify individuals and their contact details when the PHU or NITC have been unable to do so promptly. More detail is described in Appendix 4. It is essential that this service is able to continue to legitimately access the necessary information to prevent the spread of COVID-19.
 19. The Ministry of Health has worked with the Office of the Privacy Commissioner to identify options for maintaining appropriate flows of information. Final decisions on authorisation for collection of the 'Finders' information will be resolved in the near future. It is anticipated this will continue to involve the Office of the Privacy Commissioner to ensure both appropriate authorisation, and processes, are implemented. Legislative updates are being considered to the Health Act 1956, in Subpart 5 of Part 3A (Management of infectious diseases).

Access and Security

20. A full Certification and Accreditation process has been proceeding in parallel with NCTS development due to the extreme time pressures applicable in the pandemic situation. The NCTS has been operating under an Interim Approval To Operate, and independent security reviews have been completed as NCTS development has progressed. Any risks or weaknesses identified during development have been added to the NCTS Risk Management Action Plan maintained by the Ministry, and managed for prompt resolution. The final Certification and Accreditation process for the NCTS including the Border Register and Exemptions process is due for completion by 30 October 2020.

Retention

21. It is recommended that a full policy be developed for the NCTS (including clinical input) to finalise retention timeframes for different information types. This policy will include all identifiable information collected, and use of non-identifiable information, specifically:
 - 21.1. NCTS health records retained as part of the Contact Tracing services (including Daily Check-In for Cases);

- 21.2. Contact information, including the information obtained directly from individuals by Contact Tracers, information submitted by individuals via the CCTA and information discovered by the Finders service.
- 21.3. Location information submitted by Consumers via the CCTA App, including information subsequently identified as an Exposure Event by Contact Tracers;
- 21.4. De-identified data; and
- 21.5. Statistical information and audit logs.

Governance

- 22. Governance Group oversight, and Steering Group processes are being finalised and implemented to manage the NCTS operations into the future. Of key importance is the governance role to manage against the potential for function creep. The COVID-19 Response: Technology Governance Group will perform the overall governance function, and the COVID-19 Response: Technology Steering Group will manage operational matters.
- 23. In the interim the established Ministry Data Governance Group has been providing assistance if required in reviewing applications for access to the NCTS (via a documented process). This will directly assist with ‘function creep’ oversight.

Action Points

- 24. The Ministry retains a NCTS Risk Management Action Plan to manage and monitor risks and mitigations. It is to add the following issues into this plan for action and resolution (dates for completion are approximate):

| Action | Planned Date for completion |
|---|---|
| Incorporate standard Terms of Use for all NCTS Users (as part of original authorisation process, and then repeating three-monthly on change of password) | (Actioned) |
| Prepare and publish on the Ministry COVID-19 website an information sheet and FAQ about NCTS (link to NCTS PIA to be added once finalised). This information will be explicit about all intended uses for the NCTS information. Prepare and incorporate a Privacy Statement for the web-based Daily Check-in process | End October 2020 (draft copies as per Appendix Seven) |
| Define and finalise process for monitoring and reviewing access by Users. | Initial implementation end of end October 2020 (ongoing – to be continuously reviewed) |
| Implement policies for NCTS, including: <ul style="list-style-type: none"> • Retention of Information Policy • Use of Mobile Device Policy | End October 2020 |
| Terms of Reference for COVID-19 Response: Technology Governance Group (the Governance Group) to be reviewed to ensure that relevant | End of October 2020 |

| | |
|--|----------------------|
| oversight can be provided for the core NCTS. This will include the features identified in clause 25 of Section Two. Operational Governance is in place. | |
| Appoint an NCTS service management role(s), with regular reporting responsibilities to the Governance Group. This role will have responsibility for the following activities: <ul style="list-style-type: none"> • Compliance with Retention of Information Policy (once finalised). • Monitoring audit logs and reviewing compliance with processes (with consequences for non-compliance). • Referral of Code of Conduct breaches to the employer of the individual User; and • Oversight of provision of appropriate training to Users (with updates as required when new functionality or new issues arise). | End of November 2020 |
| Implement improved contact tracing data governance processes | End of October 2020 |
| Finalise Certification and Accreditation process for all NCTS components | 30 October 2020 |
| Develop standard Application Process for requests to access NCTS (or information thereon) outside established NCTS role controls | (Actioned) |
| Finalise Application Process for management of NCTS data management layer within Snowflake, the Ministry operated cloud data platform to support data management, warehousing, analytic and sharing requirements. | (Actioned) |
| Progress consideration of legislative updates to Part 3A subpart 5 of the Health Act <ul style="list-style-type: none"> • Complete discussions with Office of the Privacy Commissioner • Consider preparation of draft 'standard' to cover regular information requests by Contact Tracers and release of information by government agencies and specific organisations • Identify if appropriate opportunity in legislative agenda to address amendments | Ongoing |
| The Ministry to determine if necessary, and if so, apply to the Chief Archivist for specific authority in relation to COVID-19 information and the expectations for deletion at the end of the pandemic (as per Public Records Act). | December 2020 |

Future Privacy Impact Assessment Activity

25. In the event of future developments of significance to the NCTS Contact Tracing, Privacy Impact Assessment update activity will be undertaken. This will be designed to assist with those developments to enable mitigation activity to be incorporated into those future design components.

Additional Privacy Impact activity to be undertaken

26. The health response at the Border (to assist with management of international arrivals and testing), is being supported by the NCTS, with specific components for each major workstream. During the design and development privacy issues are being addressed to identify and mitigate relevant privacy challenges. The Office of the Privacy

Commissioner will be advised of the progress of these developments and will be requested to assist in review of Privacy Impact Assessment activity.

- 26.1. NCTS Border Register – this contains the record of management for COVID-19 as it relates to travellers arriving in New Zealand
 - 26.2. NCTS Border Staff Testing – this contains the management record for testing of border workforce groups
 - 26.3. NCTS Managed Isolation Exemptions process – this contains the management record for determining exemptions to the Border MIQF.
27. Future technology initiatives that may interact with, or support the NCTS will also be subject to specific privacy review activity, and direct engagement will be undertaken with the Office of the Privacy Commissioner as those opportunities evolve.

Section Two – Operational Details

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 2002⁸.
2. A National Contact Tracing Solution (NCTS) has been established by the Ministry of Health to provide secure, consistent and accurate management of Cases nationally. This is in line with recommendations in the [Rapid Audit of Contact Tracing for COVID-19 in New Zealand](#)⁹ that '*The Ministry of Health should develop a system that monitors the case-isolation and contact tracing process from end-to-end in the NCCS¹⁰ and PHUs*'.
3. The ESR provides COVID-19 test results securely into the NCTS to enable the Contact Tracing processes to be initiated in respect of all affected individuals. The users of the NCTS include PHU and NITC staff to perform related Contact Tracing services.
 - 3.1. The PHUs are the Public Health Units (operated regionally by the District Health Boards) whose members perform Contact Tracing services, particularly the initial engagement with individuals to advise of test results and conduct first interviews.
 - 3.2. The NITC is the National Investigation and Tracing Centre within the Ministry of Health also provides Contact Tracing activities, and finding services for Close Contacts who cannot be promptly located.
4. The NCTS supports a number of processes associated with Contact Tracing. The Appendices contain more details of each of the following processes and their interaction with the NCTS:
 - 4.1. Appendix One: Contact Tracing Processes (this includes the legislative framework that applies to Contact Tracing)
 - 4.2. Appendix Two: The NCTS database facility features
 - 4.3. Appendix Three: The Telephony Service
 - 4.4. Appendix Four: The Finders Service
 - 4.5. Appendix Five: COVID-19 Contact Tracing Application (the CCTA)
 - 4.6. Appendix Six: The Daily Check-In

⁸ On 30 January 2020 'novel coronavirus capable of causing severe respiratory illness' was listed under the Health Act schedule as a notifiable infectious disease. On 25 March 2020 an epidemic notice came into force under the Epidemic Preparedness Act 2006.

⁹ Dr Ayesha Verrall, University of Otago, 10 April 2020 – the 2 May 2020 indicator review can also be found [here](#) [The Final Report on the Contact Tracing System by the Contact Tracing Assurance Committee \(16 July 2020\)](#) can also be found [here](#)

¹⁰ Now the NITC for National Investigation and Tracing Centre

5. This Section summarises the NCTS interactions, features and security. It shows the information collected and managed as a whole and how it will be used, stored and accessed.

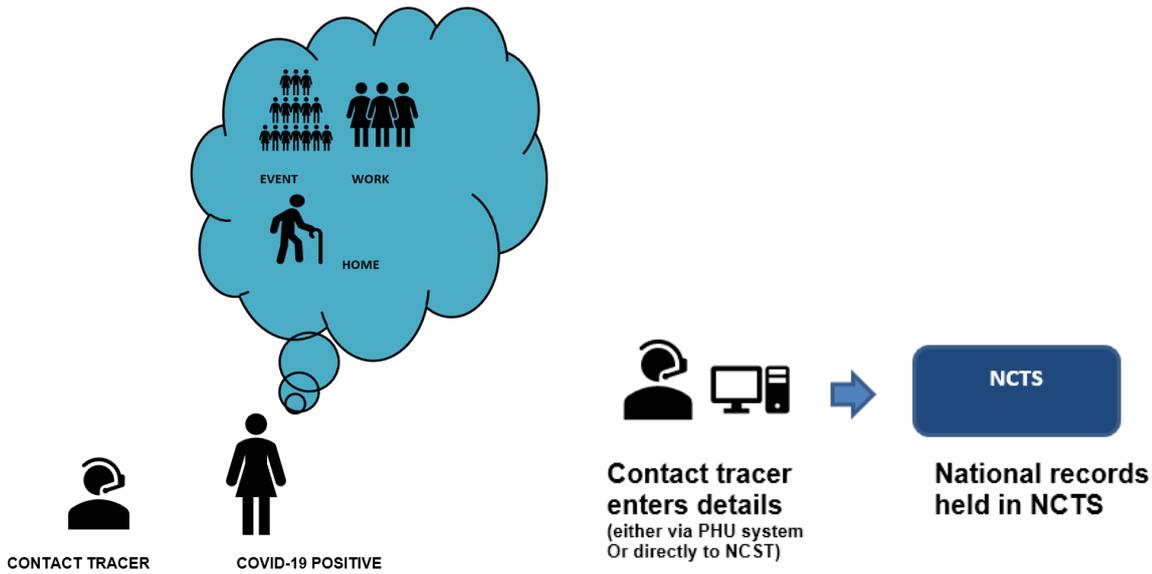
Objectives

6. Identified objectives for the NCTS include a technological Contact Tracing solution that:
 - 6.1. provides a safe, robust and timely implementation of the NCTS that supports the end-to-end Contact Tracing pathway for COVID-19;
 - 6.2. is capable of supporting contact tracing for COVID-19 nationally across all PHUs. This is to ensure that information and process are consistently recorded, managed and monitored, and a central coordination of contact tracing can be achieved and scaled to support PHUs where local demand exceeds available capacity.
 - 6.3. supports an end-to-end pathway, with fit-for-purpose functionality and integrations. This is to ensure a reliable national distribution of clinical and operational information to be accessible to authorised users who are part of the Contact Tracing process
 - 6.4. establishes and integrates technology services that will enable the rapid scaling of call centre operations for COVID-19 contact tracing, should that be required.
 - 6.5. provides a robust and timely mechanism through which all data necessary to support the monitoring process across all aspects of COVID-19 contact tracing is available in a timely manner.

Information Collected and Information Flows

Contact Tracing – confirmed Cases

7. All COVID-19 test results (both confirmed and negative) on individual Consumers are reported from ESR to the NCTS. ESR performs public health surveillance of infectious disease on behalf of the Ministry of Health. Test results are recorded against Covid-19 Case records and Close Contact follow-up Case records in the NCTS. Test results on the follow-up Case records for Close Contacts identify compliance against the assigned management plan. All test results are recorded within the NCTS data management layer to support national monitoring services for COVID-19. PHUs receive test results from ESR, they can also access them through the NCTS.
8. The PHU Contact Tracer will contact each person (Case) who is either a confirmed or probable Case of COVID-19 and advise them of the test result, and provide the necessary clinical information. The Contact Tracer will then arrange a subsequent time to call the individual back and work through any potential Close Contacts (from the individual's home and work environments) and any potential Locations where an Exposure Event might have occurred.



9. To maintain secure national records all PHUs will enter information directly into the NCTS (the last PHU has become fully operational on the NCTS by the end of July 2020). As the NCTS is to provide a 'fail-safe' process, recording events on a pathway flowing from a confirmed result, information is recorded from the outset of a confirmed test result (or an identified probable Case even if the test result is not positive at that time).
10. Only information required to support the safe and effective execution of contact tracing for COVID-19 is to be collected. The fields of data about a confirmed or probable Case are designed by clinicians and based on the public health Case report form which identifies information necessary for contact tracing.¹¹
11. Information flows into the NCTS include:

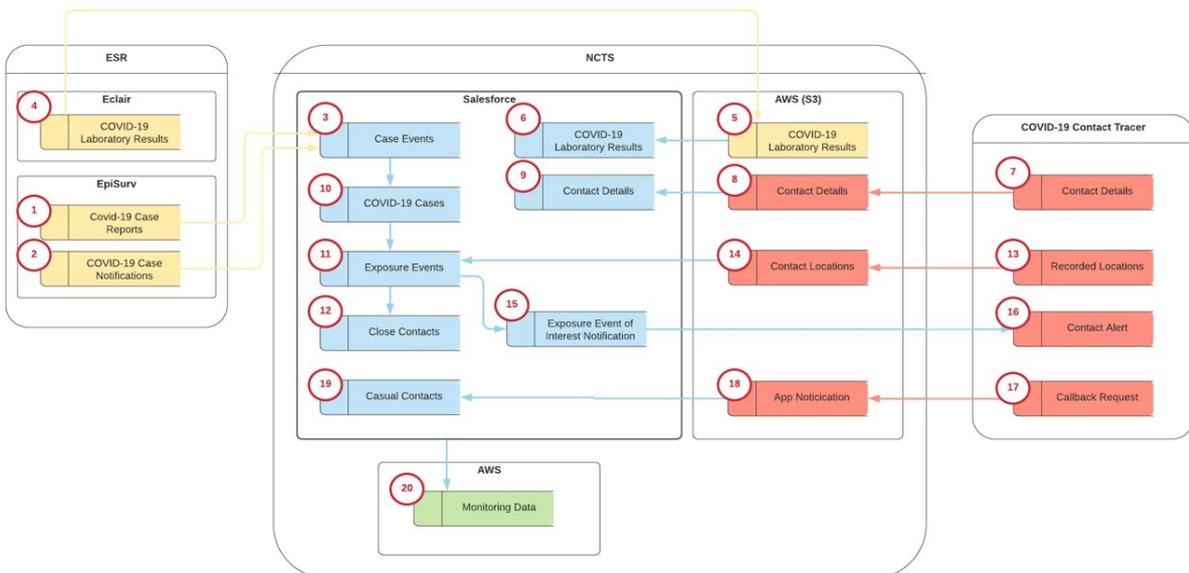
| Information field | NCTS Source | Purpose for Collection (as part of Contact Tracing process) |
|--|---|--|
| COVID-19 test result (includes name and NHI) of a 'Case' and other test outcomes | ESR | To identify confirmed Cases, and negative ¹² results for COVID-19, and manage related reporting for all test results nationally |
| Identity and contact details of Close Contacts of each 'Case', and Exposure Events (Locations where Close Contact with the Case may have occurred) | PHU or NITC authorised users who obtain those details directly from the Case or Close Contact | To identify Close Contacts |

¹¹ The various HISO standards created for the COVID-19 Contact Tracing scenarios can be located [here](#)

¹² A probable Case is a symptomatic Close Contact. It will be identified because a Contact Tracer is following up the Case.

| | | |
|--|---|---|
| Case and Close Contact identification (name, date of birth, gender) and contact details (contact phone or email details if available, residential address) | National Health Index (NHI), National Enrolment Service (NES) | To confirm identity and contact Cases and Close Contacts |
| Close Contact, contact details (if not available from above processes) | Consumer App (CCTA) | To contact Close Contact |
| Location information | Consumer App (CCTA) and MBIE NZBN GLN scanned Location | To identify potential Exposure Events a Case may have attended. The CCTA Upload (if the Consumer chooses to use this process) will send scanned Locations to the NCTS. The NCTS can match those scanned Locations against the NZBN database to identify the relevant business identity and contact details. |
| Contact details of Close Contact if unable to be located from previous options | External sources as further described in Appendix Four for the Finders services within the NITC. | To identify and / or contact the Close Contact |
| Daily Check-in Details | From individuals (on a clinically mandated template, via web interface) or In response to a telephony service caller via an equivalent phone script. | To monitor Cases and Close Contacts through self-isolation periods |

12. The following diagram demonstrates the dataflows associated with the NCTS (the full details to support the diagram are located in Appendix One – Annex One):



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

- 13.1. Related to an individual who has a confirmed or probable Case of COVID-19;
- 13.2. Related to an individual who is identified as a Close Contact (and the status of some Close Contacts may change to confirmed or probable Case over time); or
- 13.3. Related to an individual who is determined not to be a Close Contact after inquiry.

Use of Information:

14. The information is to be limited to uses associated with the public health response to the COVID-19 pandemic. This will include:

- 14.1. Management of the infectious disease COVID-19¹³ in accordance with Part 3A of the Health Act;
- 14.2. To meet the purposes for Contact Tracing as identified in Part 3A Subpart 5 of the Health Act 1956:
 - To identify confirmed and probable Cases to enable Case management (to identify the source of the infectious disease or suspected infectious disease – s92ZY(a));
 - To identify and contact Close Contacts (to make the contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary – s92ZY(b)); and
 - To limit the transmission of the infectious disease or suspected infectious disease (s92ZY(c)).
- 14.3. Reporting and analysis to support these management objectives, and appropriate research if authorised by the Ministry of Health.

15. As all DHB PHU units are now contributing the contact tracing information directly into the NCTS (rather than into their own regional record keeping systems) this enables a national real time view of workflows (how quickly Close Contacts are being identified and contacted for example). In the August 2020 Auckland outbreak it was possible to identify when additional support was required and enable a proportion of activities to be allocated to other specialist regional public health services throughout the country, with all activities managed securely within the NCTS.

16. The Ministry has identified its Snowflake platform as a secure location where authorised DHB personnel can access and analyse relevant information held by the NCTS.

¹³ On 30 January 2020 'novel coronavirus capable of causing severe respiratory illness' was listed under the Health Act schedule as a notifiable infectious disease.

- 16.1. Snowflake is a secure environment, based on its AWS platform, with analytical tools that will enable national and regional planning, oversight and measurement of outcomes and resource deployment.
 - 16.2. This authorisation would permit access to the NCTS data management layer¹⁴ and to the analytical tools within Snowflake, which the DHBs may not have available within their own information technology systems. Only very limited numbers of DHB and Ministry analysts would be authorised to access the relevant NCTS dataset (the data management layer), and regional restrictions may be applied to identifiable information.
 - 16.3. The Snowflake PIA requires the completion of a Data Assessment Process (the SDA Process) prior to incorporation of any datasets. This is reviewed by the Ministry Data Governance Group prior to any access being granted.
 - 16.4. It is expected that this process will record the limits on user access (both in number and role of users), subsequent management of information (if removed from the Snowflake environment) and obligations regarding retention of information.
17. The Ministry is continuing work to further develop its NCTS and contact tracing data governance framework.

Retention of NCTS information

18. Different time frames will apply to different aspects of the information. In summary, retention expectations are:
- 18.1. Information will be managed in accordance with the Public Records Act 2005, and any applicable Retention and Disposal Schedule. It is expected that the Ministry will apply to the Chief Archivist for specific authority in relation to COVID-19 information and the expectations for deletion at the end of the pandemic.
 - 18.2. Any health record will be managed securely and retained in accordance with the Health (Retention of Health Information) Regulations 1996. Clinicians will be involved in setting a policy to mark out the boundaries of which information fields and person records will constitute the health record, and this will be used to form the retention policy for the NCTS.
 - 18.3. Any identifiable information that does not become part of the health record of an individual will be securely and promptly destroyed after the pandemic is over, or earlier where appropriate (where its purpose has been served).
 - 18.4. A summary of the retention of records requirements are set out below.

| |
|--|
| Information to be deleted within six months of collection: data that is not used as part of active Contract Tracing |
|--|

¹⁴ Where all data is collected, consolidated and curated into a single place within NCTS environment

| |
|---|
| Digital Diary details uploaded from the App (the Location and manual diary entry information in the secure S3 bucket on the NCTS boundary) that is not incorporated into a NCTS Case file. |
| Survey responses from the Daily Check-In for all Close Contacts who have not developed any symptoms. If they remained asymptomatic it is not considered a health record (although a record will be retained on the NCTS confirming the individual did complete the Daily Check-In process). |
| Any 'test' dataset developed during contact tracing readiness training and analysis (this would involve information from volunteer individuals who assist in test scenarios to simulate confirmed COVID Cases and Close Contacts, and who may disclose personal information or invented information during that process). |
| Retained for the duration of the pandemic (until the COVID-19 Public Health Response Act 2020 is repealed) |
| Contact details submitted via the App (not held on the NCTS). |
| Confirmation of completion of Daily Check-in by asymptomatic Cases. |
| Information provided under the Customs Information Disclosure Agreement that has not been incorporated into a health record or anonymised |
| Retained for two years post creation of the record |
| Any tracking and auditing information of User access within the NCTS. |
| Retained as a 'health record' for minimum of 10 years |
| Case records for confirmed Cases that are a record of the disease (these are not clinical treatment records but are considered health records). These records will include the individual Case name, identification and contact details, NHI, test result, Daily Check-in records (record of the disease), Exposure Events and Close Contacts. |
| These records will also be retained for a probable Case that becomes symptomatic. |
| It will be important to also retain a master record of the disease, which may need to be separately held after the end of the pandemic (this may need to be used for future immunisation, or location of those individuals known to have been infected if it is identified there may be additional health treatment repercussions in future). |
| Research and planning |
| Non-identifiable (or de-identified) information may be retained, to be used for purposes related to the public health response to COVID for as long as that information remains relevant for those purposes. Ideally a non-identifiable dataset for epidemiological data will be retained, which would include Case, exposure event and close contact information to enable effective management of infectious disease as contemplated by the Health Act Part 3A. |
| NCTS Components – including the Border Register, Border Staff Testing and Border Isolation Exemptions Process |
| The Privacy Impact Assessments for each of these components will directly address any specific data retention requirements for each collection, and these will be included in the NCTS Retention Policy. |

19. It is strongly recommended that a full policy be created to set the retention timeframes, and that the Governance for the NCTS monitor for compliance with the policy.

NCTS Security

20. In summary:

- 20.1. The NCTS is made up of a number of components, including:
- integration and Amazon Web Service (AWS) capability;
 - Salesforce Service Cloud (Service Cloud). This 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, Health Connect provides additional configuration;
 - Office 365 office productivity tools to allow and support the Contact Tracing role for the NITC users (messaging and meetings only).

20.2. The Salesforce Service Cloud instance is served from AWS Cloud infrastructure based in Sydney, Australia.

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

21. The Ministry is to finalise its standard Certification and Accreditation process by the end of October 2020 (including documenting standard operating procedures and incident response procedures).

22. The NCTS has been, and continues to be, independently security reviewed by an All of Government approved supplier as part of the Certification and Accreditation process. Findings from the reviews are addressed and managed as part of ongoing development (and managed by the Ministry in accordance with its risk register). Ongoing development of the NCTS will be independently assessed to the same standards and is required to meet the security requirements for central government.

23. Some of the technical security features on the NCTS include:

23.1. Data stored within AWS is encrypted in transit and at rest.

23.2. Multifactor authentication for all users using cloud NCTS cloud applications

23.3. Role based access controls and audit logging of all access

23.4. Monitoring and alerting for abnormal activities and security incidents on NCTS cloud applications

23.5. Transaction security polices applied preventing bulk data downloads

23.6. System access using Ministry devices are required to meet government security standards

24. In addition, there are operational security mitigations and policies. These include standard operating procedures such as:
- 24.1. Administration of the National Investigation and Tracing Centre and supporting teams to handle sensitive information in a secure manner, and documented standard operating procedures.
 - 24.2. All Users to confirm Terms of Use at time of being granted first access (and again at each ninety day password renewal).
 - 24.3. Timely offboarding of exiting users and unused accounts.
 - 24.4. Controlling allocation of access rights to those who meet suitability and training criteria (reference also nomination process for contact tracers under s92ZZA of the Health Act).

Governance

25. Governance of the programme includes entities to manage and maintain oversight of information arising from the NCTS processes:
- 25.1. During the configuration and implementation phase the governance team has included the COVID-19 Public Health Response Governance Group and the Population Health Technology Steering Committee, with stakeholder representation including clinical and Public Health Units.
 - 25.2. As the NCTS has moved from development into operational 'business as usual' management, oversight and Internal Quality Assurance (QA) will be provided via the COVID-19 Response: Technology Governance Group, with input from the National Investigation and Tracing Centre.
26. The COVID-19 Public Health Response Governance Group will continue to act in the interim as the governance group (the Governance Group) and the Population Health Technology Steering Committee can assist with operational / clinical input.
- 26.1. The Governance Group will provide leadership and strategic direction for the NCTS. It is suggested that this Group have the following attributes from a Privacy perspective:
 - the ability to manage the overall direction of the NCTS.
 - a pathway for involved parties to approach the governance entity to determine high level NCTS queries.
 - the ability to develop and / or approve Policies to provide guidance for operation of the NCTS.
 - oversight to provide protection from 'function creep' over time, by retaining an overall focus on the privacy interests of parties and the original stated objectives of the NCTS.

- Audit planning functions – even if delegated. The Governance Group could set appropriate parameters for operation of the system and determine who will have the ability to intervene if non-compliance with requirements occurs.

26.2. The Steering Group will oversee the operational aspects of the implementation and ongoing management. It is recommended that a strong and experienced core of members be retained to ensure that knowledge and experience is not lost in the changeover of personnel.

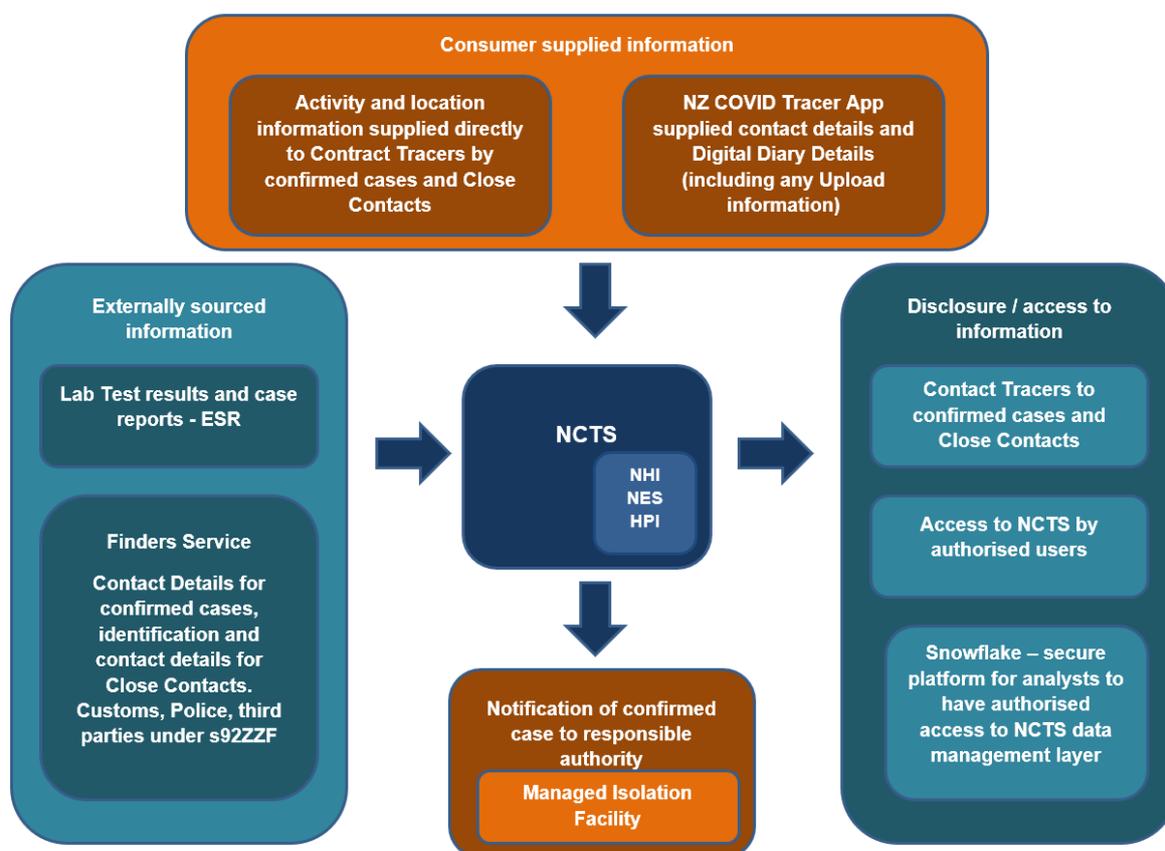
27. It is recommended that the Terms of Reference for each group are reviewed to ensure an appropriate and specific focus is included for the issues identified above.

Section Three - Privacy Analysis

The purpose of this Assessment is to review the NCTS processes for the COVID-19 pandemic response. This includes the collection, storage, use and sharing of personal and health information.

The NCTS is the IT solution that will define and support the contact tracing pathways. As noted in Appendices One to Six, there are a number of processes involved in the contact tracing response to the pandemic, all of them interacting with the NCTS technology solution¹⁵.

The summarised dataflows for the NCTS Contact Tracing component are as follows:



There is significant potential for the NCTS to improve accuracy and completeness of the contact tracing response on a national basis, thereby contributing to the maintenance of health and safety of individuals living in New Zealand. It is not, however, without privacy challenges. These need to be carefully managed to ensure that confidence and trust in the NCTS, and the associated contact tracing processes, will be created and maintained. Without trust in the contact tracing system, the willingness of individuals to acknowledge when they are experiencing COVID-19 related symptoms, or the participation by regional Public Health Units could be compromised.

¹⁵ There has also been a Privacy Impact Assessment completed (which is being regularly updated) for the CCTA. This can be found [here](#).

The Ministry has conducted its analysis under the Health Information Privacy Code (the HIPC) as the information is ultimately about individuals who are a confirmed or probable Case of COVID-19, or Close Contact of a Case.

Under clause 4(1)(e) of the HIPC it is considered that the NCTS could include information about an *'individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual'*. The Ministry has therefore chosen to analyse the high standards associated with health information in the HIPC for the purposes of this Privacy Impact Assessment.

Health information and personal information will be collected about each participant who progresses along the Contact Tracing pathway.

- The Public Health Units and Daily Check-In processes are integrated with the NCTS, and this does incorporate some clinical elements in monitoring care of Consumers.
- The main health treatment record of a COVID-19 Case will however remain with the clinicians treating the individual. The NCTS will only be recording health record elements integral to its contact tracing pathways, for the NCTS related purposes only, and will not be sharing that information with those clinicians treating the individuals.

A significant risk in this project is 'function creep'. Management of this risk will contribute significantly to maintaining trust in the NCTS operations. A clear purpose statement, backed by operational controls to support limits on use, and access, are essential. Strong governance, and management, will also support these objectives. There is a confidentiality requirement in section 92ZZG(2) of the Privacy Act. This provides *'...information provided or obtained by a contact tracer under this Part may not be used or disclosed by anyone except for the effective management of infectious disease...'*

Another key risk area is security of the NCTS. The NCTS has been able to leverage off the successful NSS go live in its development (the NSS had completed the C&A process). The NCTS project has obtained expert advice throughout the design and build process. The need to ensure the NCTS design and operation are secure and minimise the opportunity for user error or misuse was identified early in the design process. Strong security and tightly controlled user operation of the NCTS will ensure development and maintenance of trust in the NCTS by both potential participants and the health provider community.

- The NCTS has been able to take advantage of the NSS design privacy and security features to minimise the risk of breach of privacy, and any impact if a breach occurs. Quality assurance has been performed by third parties to achieve the best technical solutions that can be identified and incorporated.
- The information collected will be stored in the 'cloud'. It will be available to users working remotely who have a role in the contact tracing processes.
- Ongoing training of Users and implementation of a comprehensive monitoring programme will be key to successful use of the NCTS platform for the duration of the pandemic, and will help to minimise the potential impact of User error.
- The NCTS pathway is designed to have numerous 'failsafe' options incorporated to make sure people keep being progressing within identified timeframes, to help achieve and report on the KPIs identified for contact tracing.

- The expectations associated with an electronic shared care record¹⁶ have been applied to the design of the NCTS. This has included in particular allocation of role based access controls, and recording (and monitoring) all access to the NCTS.

¹⁶ <https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/Electronic-Shared-Care-Records-Elements-of-Trust-report-1.pdf>

| Health Information Privacy Code Rules | | Solution Details and commentary | Residual risk of non-compliance with rule |
|---------------------------------------|--|--|---|
| Rule 1 | <p>Purpose of collection of health information</p> <p>Only collect health information if you really need it</p> | <p>Purpose: The information to be incorporated into the NCTS is collected for lawful purposes connected with supporting New Zealand's contact tracing response to the COVID-19 pandemic.</p> <p>As noted in section 92ZX of the Health Act 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:</p> <ol style="list-style-type: none"> Identify the source of the infectious disease or suspected infectious disease Make the contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary Limit the transmission of infectious disease or suspected infectious disease <p>Section 92J also permits directions to be given by the Medical Officer of Health to those individuals who may have been in contact with a person who has an infectious disease. It is therefore important that close contacts are comprehensively and consistently identified.</p> <p>The public health units are all now using the NCTS, rather than their own IT systems. This creates a national collection which recognises that Cases may spread between regions, and if surge assistance is required (a marked upswing in Cases in a particular region) Contact Tracers from other regions can quickly provide additional support.</p> <p>The NCTS purposes include:</p> <ul style="list-style-type: none"> national management of, and reporting on, individual Cases and their close contacts, with all of these activities will be recorded onto the NCTS. This will include: <ul style="list-style-type: none"> identification and investigation of confirmed Cases, via the testing process. contact with and management of those individuals who are a confirmed or probable Case of COVID-19, and any potential Close Contacts. This is the work conducted by the Contact Tracers and information obtained via the App processes. collection of relevant information from other individuals or organisations as authorised under the Health Act provisions or other relevant legislation. This includes the Contact Tracer and Finders staff activity. the national and local planning and management required to provide effective management of the infectious disease in accordance with s92ZZG(2) of the Health Act. This has been interpreted by the Ministry as including its internal planning, reporting and analysis activities, authorised research with appropriate ethical approval and the use of Snowflake for analytics required by the DHB PHUs and the Ministry. | Low |

| | | | |
|--------|---|---|-----|
| | | <p>It is recommended that a clear Purpose Statement be developed that can be incorporated into publicly available materials about the NCTS – Contact Tracing component. This will also provide guidance when measuring against the risk of ‘function creep’ – to ensure the intended purpose aligns.</p> <p>Necessity: Only data required to support the safe and effective execution of Contact Tracing for COVID-19 will be collected.</p> <ul style="list-style-type: none"> • <i>Information sourced directly from Consumers:</i> The fields of data to be collected by Contact Tracers have been analysed by the Ministry and PHU clinical teams to confirm the details collected are necessary. <ul style="list-style-type: none"> ○ This is based on the public health Case report form which has identified information necessary for contact tracing. ○ This also applies to the data fields in the Daily Check-in information, which are designed to elicit only relevant information to identify the symptoms of COVID-19, and to assist those Consumers who are required to isolate. ○ Information obtained via the App is limited in nature to what is necessary to assist Contact Tracing purposes, and is all voluntary, including the Digital Diary upload in a confirmed Case. • <i>Information sourced from external sources</i> <ul style="list-style-type: none"> ○ The Finders service is expected only to request information necessary to identify and locate Cases or Close Contacts, and identify the least sensitive sources first before seeking information from third parties or more sensitive sources. Information is to be verified by the Finders service before being added into the NCTS, so only necessary and relevant contact and identification information will be included. | |
| Rule 2 | <p>Source of health information</p> <p>Get it straight from the people concerned</p> | <p>There are a number of information sources which support the NCTS purposes. Not all of these are directly from the individual concerned, but the external sources are consistent with the requirements of Rule 2.</p> <p><i>Sourced from ESR:</i> All test results, Case reports and Case notifications will come from ESR (which receives all reports nationally from laboratories). Section 74AA and 74B of the Health Act require reporting of all Cases where a person ‘<i>is, has been, or may be or have been, infected with a notifiable disease</i>’.</p> <ul style="list-style-type: none"> • A direct integration/ interface with ESR enables a ‘feed’ of pre-determined information fields into the NCTS of confirmed, and negative results of the tests and the associated NHI identification / contact details into the NCTS. If necessary, probable Cases will also be identified by Contact Tracers on the NCTS, and passed to NITC for contact tracing. • In addition, it is not reasonably practicable to collect this test result information from individuals as the Ministry has no direct contact with the individuals, and it would prejudice the purposes of the collection if a full dataset were not able to be obtained with urgency. Any delay or uncertainty in the individuals who needed to be followed up by Contact Tracers could have serious consequences in terms of the ability to limit the spread of infectious disease. <p><i>Sourced from internal Ministry datasets:</i> To make contact with the Case, the Contact Tracers will make use of the Ministry held NHI and NES records to obtain current contact details (and also subsequently for Close Contact contact details if necessary). This will be managed on an individual lookup basis, when required to locate an infected Case or Close Contact.</p> <ul style="list-style-type: none"> • The use of the NHI and NES contact details is generally consistent with the provisions in the Privacy Fact Sheet at Appendix 6 of the Health Information Governance Guidelines which indicates that ‘We also collect your health information | Low |

| | | | |
|--------|---|---|---|
| | | <p>to help you...manage your own health...keep you and others safe...' When individuals enrol in a PHO they are to be provided with the Privacy Fact Sheet, and their information is then submitted via the NES. The use of the information for contact tracing purposes is consistent with managing the health of the individual and others.</p> <ul style="list-style-type: none"> In these instances, (and when necessary to review contact details in other Ministry databases) the Ministry will rely on Rule 2(2)(d) – as compliance is not reasonably practicable in the urgent circumstances of needing to prevent the spread of infectious disease – it is not practicable to attempt to obtain contact details directly from Consumers. This is particularly the Case when it is the necessary contact details that are being sought from the NHI or NES. It would also prejudice the interests of the confirmed Case, or Close Contact, if it were not possible for the Contact Tracers to promptly contact them. <p><i>Sourced directly from the Consumer:</i> Information is collected directly from confirmed Cases about their activities and the individuals they may have been in close contact with. This is consistent with legislative authorisation and consistent with original purposes for collection.</p> <ul style="list-style-type: none"> The confirmed or probable Case themselves will be asked directly for their possible close contacts. This is always initiated on a voluntary response basis, although there are legislative obligations in section 92ZZC of the Health Act if required. In requesting the confirmed Case advise who their contacts were this is information about the close contacts, which will therefore come from a party other than the individual concerned. Due to the potential to invoke legislative authorisation and the fact that compliance would prejudice the safety of the Close Contact (if the Case did not disclose the third party is at risk – Rule 2(2)(c)(iii)) it is not considered that this will breach the 'source' rule. Close Contacts, and border workers will also be asked for information directly about their health status for the purposes of the Daily Check-in The App information will be sourced directly from the Consumer with their authority (and is voluntary). <p><i>Sourced from Third Parties:</i> In those limited Cases where an individual is unable to be located, other internal Ministry databases may be searched, or other government agencies or organisations (such as businesses or educational institutions) may be requested to provide contact information. The justification for these collections is detailed in Appendix Four. In addition to the Rule 2(2)(c)(iii) exception to avoid prejudice to the safety of any individual there is also authority under s92ZZF of the Health Act for a Contact Tracer to require specified third parties to require information.</p> <p>It is strongly recommended that current considerations for amending Subpart 5 of Part 3A are pursued promptly to determine if additional clarity is required.</p> | |
| Rule 3 | <p>Collection of health information from individual</p> <p>Tell them what you're going to do with it</p> | <p>It is recommended that a general NCTS information sheet (and possibly also an FAQ) be included on the Ministry COVID website. An initial draft of such a document, and a draft Privacy Statement for the Daily Check-in is attached in Appendix Seven.</p> <ul style="list-style-type: none"> At present it is understood that there is no specific information given to Consumers at the time of laboratory testing other than that provided as part of a standard laboratory consultation. As this is prior to any direct contact with any NCTS representative the Ministry COVID-19 website (which is now a commonly known source of relevant COVID-19 Information) has now provided some relevant collection information. The initial NCTS collection of details of test results will be under statutory authority from laboratories (including ESR). | <p>Low, provided relevant information is made readily available to the public about the NCTS in a manner compliant with Rule 3</p> |

| | | | |
|--------|---|---|---|
| | | <ul style="list-style-type: none"> • A script has been devised for NCTS Contact Tracers to meet any necessary collection expectations when they contact Cases or Close Contacts and seek information from them. The script is to reflect the requirement of respect for individuals (s92C of the Health Act) and voluntary compliance where possible (s92D of the Health Act). • The collection of information from confirmed or probable Cases is, however, effectively mandated by statute. Section 92ZZC provides that individuals with 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. There are additional powers under 92ZFF to make enquiries from an employer of an individual, any educational institution the individual has attended, any business or organisation they have dealt with or organiser of any event they have attended. Contact Tracers will be trained to discuss with individuals who indicate that they are unwilling to respond what the obligations are. There are also outreach services which may assist in individual Cases to encourage contribution of information in a setting that may be more comfortable or acceptable to the Consumer. This may include specialised language or cultural assistance. If necessary, this could include meeting with the individual. <p>In the interests of transparency it is recommended that a Privacy Statement (or information sheet) for the NCTS (and its associated activities) be put on the Ministry COVID website – as this is now a well known resource for individuals to search if they have any questions about activities related to COVID events. This would need to address each of the requirements for Rule 3 – including particularly the contact point for individuals who have questions about what information is being held about them.</p> | |
| Rule 4 | <p>Manner of collection of health information</p> <p>Be considerate when you're getting it</p> | <p>The collection itself is lawful, and not unfair, with its general population health focus. Contacts with individuals are expected to be managed in accordance with legislative processes.</p> <p>All contact tracers will have previous experience from within the Public Health Unit they work with, or will be trained in accordance with Ministry instructions before being permitted to conduct tracing work so they are fully aware of their obligations.</p> <p>For a person under 16, or lacking legal capacity the Contact Tracer may require guardians or legal representatives to answer the questions (section 92ZZC(5)). This would ensure that support could be available for a young person, or other individuals who may require assistance, in the event that they were required to be involved in the Contact Tracing process.</p> <p>For a small number of Cases where a potential Close Contact may not be identifiable and only a few pieces of information are held open source social media may be used to identify links, or to confirm other information. This will be managed by the Finding Service, who will all follow standard processes and use accounts that are registered with Ministry of Health identifiers. No information from these sources is used for purposes other than contact tracing. As it is important that these individuals are identified and informed of the risk of exposure to COVID-19, so that they and their contacts can be protected, it is considered that this is not unfair or invasive in the circumstances.</p> | Low |
| Rule 5 | <p>Storage and security of health information</p> <p>Take care of it once you've got it</p> | <p>This is the key risk area and where significant work is being expended by the Ministry to manage this. The Ministry Certification and Accreditation process across the NCTS components will be completed by 30 October 2020. Ongoing security assessment has been provided by an independent provider, and the identified security mitigations progressively implemented.</p> <p><i>Operational and technical security:</i></p> | Medium, but reduced to low if necessary security features are consistently applied |

| | | | |
|--|--|--|--|
| | | <p>With any network connected and complex system such as the NCTS there will be risks of accidental or intentional information disclosure, such as an accidental misconfiguration of the system exposing data, or a determined and sophisticated attacker who is able to bypass security measures to access information they shouldn't have.</p> <p>The intended mitigation strategies rely heavily on the design and underlying platforms of the NCTS, specifically to incorporate the necessary security measures to provide protection and mitigate damage from such intrusion. This includes, for example:</p> <ul style="list-style-type: none"> • The use of established and experienced large global cloud providers who are responsible for maintaining the security of their environments. These cloud providers have extensive interests in maintaining the security of their platforms, and often go through regular extensive certification processes around security and privacy. For example: <ul style="list-style-type: none"> ○ AWS and Salesforce hold a number of security and assurance reports including ISO 27001, ISO 27017, ISO 2018, SOC 1 through 3, and more.¹⁷ ○ MuleSoft Anypoint Platform meets ISO 27001, SOC 1 and 2, and is built on the AWS platform.¹⁸ • A requirement that all information on the NCTS will be encrypted while in storage and in transit, whenever reasonably possible, which helps protect the information from unauthorised disclosure. In the event of a security breach in the provider environments, there is a technical possibility the encryption keys may be exposed as well. A useful discussion of 'balancing the risks' is contained at pages 13-14 of the Office of the Privacy Commissioner's own PIA¹⁹. It would also likely give the cloud providers the ability to decrypt and hand over information as part of a lawful request (jurisdictional issues addressed further below). The Ministry has balanced its risk with the contracted provider for the Ministry holding the AWS encryption keys on behalf of the Ministry. Salesforce holds the encryption keys for Salesforce. • Prior to the completion of the C&A process the NCTS has been operating under Interim Authority to Operate – which has approved the current security arrangements for the purposes of operating the NCTS while the final development and C&A processes is completed. • Connectivity between the NCTS and the Public Health Units systems will be via secure file transfer protocols within the NCTS solution. • Any interface with the CCTA is via secure file transfer protocols within the NCTS solution • System integrity measures such as intrusion detection, network segmentation, and logging and monitoring have been incorporated into the NCTS design. • Additional optional security and privacy components have been included as part of the design, including the Salesforce Shield²⁰ technology which provides enhanced encryption and audit logging capability to provide better protection of, and tracking of access to, confidential information held in the solution. | |
|--|--|--|--|

¹⁷ <https://aws.amazon.com/compliance/programs/> & <https://trust.salesforce.com/en/compliance/>

¹⁸ <https://www.mulesoft.com/trust-center>

¹⁹ <https://www.privacy.org.nz/assets/Files/OPC-cloud-PIA.pdf>

²⁰ <https://www.salesforce.com/au/products/platform/products/shield/>

| | | | |
|--|--|--|--|
| | | <ul style="list-style-type: none"> • User accountability is incorporated, logging who accessed what and when. <ul style="list-style-type: none"> ○ The NCTS is designed to limit access to authorised Users by role based access, and uses authentication and authorisation (with unique User name and password, and additionally multi-factor authentication where reasonably possible). The system will automatically capture who accessed what and when. A matrix has been developed during the configuration phase that contains the roles and related access controls that will be apply during the operation of the NCTS. ○ The NCTS itself will limit access, for example, to those Cases within a users queue for attendance, or unique to the PHU region, and for finders to those Cases assigned. ○ Monitoring of all access will also be undertaken, with enforcement where appropriate. <p><i>Operational Security – Users</i></p> <p>While some of the security risks can be minimised or even eliminated with the use of appropriate technology, there remain risks associated with human impact that cannot be completely removed. It is noted that there are a range of potential risks of unauthorised access /disclosure, created by Users, including:</p> <ul style="list-style-type: none"> • Accidental disclosure (for example, leaving a computer logged in when absent from the computer, or printed data in a location where unauthorised individuals can access it). The intended mitigation strategy is to: <ul style="list-style-type: none"> ○ require Users (or their contracted managers) to confirm / sign terms of use; ○ provide basic training to Users; and ○ the timely offboarding of users no longer working on NCTS²¹. • Insider curiosity (a person with access privileges reviewing more than they are entitled to see) or internal data breach (someone with some limited access rights taking advantage of system knowledge to view more records/ detail than authorised). The intended mitigation strategy is to appoint a management role(s) with reporting to the Governance Group, with oversight of the following mitigations: <ul style="list-style-type: none"> ○ system controls implemented within NCTS with access and event tracking. ○ use of audit logs and review processes (with consequences for non-compliance) to discourage non-compliant behaviour and also increase the likelihood that non-compliant behaviour will be identified when it occurs. This is an area that the NCTS will retain an ongoing focus on. The NCTS already records all User access. There will be ongoing monitoring to reduce risk of inappropriate access and additional controls to ensure the protection of information. Monitoring is to be undertaken as a regular and standard activity, as well as the enhancing the ability to track any specific issues raised to identify all access to records where a concern has arisen. Monitoring of these reports will be the responsibility of the management role (role to be appointed by end of November 2020). | |
|--|--|--|--|

²¹ A training package is provided to those with RBAC rights to the NCTS as a condition of access being granted. Noting also that free training that can be undertaken directly from the website of the Office of the Privacy Commissioner – e-learning Health 101 <https://privacy.org.nz/further-resources/online-privacy-training-free/>

| | | | |
|--------|--|--|-----|
| | | <ul style="list-style-type: none"> ○ reference of code of conduct breaches to the employer of the individual User (all Users are expected to be employed or contracted in some capacity by a government related agency – including District Health Boards). The surge workforce and Healthline staff are to be managed in accordance with the contracts they hold with the Ministry. ○ monitoring Users requirements to confirm Terms of Use as part of the access credential process, prior to being able to access the NCTS. This recommendation has been implemented and standard Terms of Use (as set out in Appendix Two Annex Two) are now a standard confirmation screen as part of the access credential sign up process; and ○ Oversee provision of appropriate training to Users (with updates as required when new functionality or new issues arise). <p><i>Information to be held off-shore</i></p> <p>A jurisdictional review was completed for the NSS. The NCTS relies on its similar architecture to proceed with the NCTS on the basis that the jurisdictional review is effectively identical. The AWS hosting (storage and transmission) components of the NCTS AWS services will be implemented using dedicated Ministry Accounts and use a Virtual Private Cloud (VPC) in the prescribed Sydney Region (ap-southeast 2) – with the VPC creating a <i>'private isolated section of the AWS Cloud where the customer can launch AWS resources in a virtual network that the customer defines'</i>²² Similarly data held within Salesforce Service Cloud will be managed within a dedicated instance of Salesforce within the Salesforce Private Cloud in the Sydney Region (ap-southeast-2).</p> <p>The Privacy Impact Assessment²³ from the Office of the Privacy Commissioner provides some general points to consider for cloud based information solutions. The OPC has concluded (for the information it is responsible for) that <i>'taking into account government policy, the law and a risk-based approach, the Microsoft cloud solution remains the preferred and prudent option...Microsoft offers industry leading data security, and better data security than we can currently deliver...we are comfortable that the regulatory framework in Australia is adequate and provides an equivalent level of protection...The storage of our data on an offshore cloud solution involves a theoretical risk that an overseas government or law enforcement agency could make a request for our data. However, the likelihood of this occurring is extremely low...The combination of assurances, contractual provisions, independent audits and certifications, and the applicability of local and overseas privacy regulations will effectively ensure that we have meaningful control over our data while it is stored in the cloud...'</i></p> <p>The Ministry is satisfied that the decision to host the NCTS on the same platform as the NSS is an appropriate choice and provides the necessary security.</p> | |
| Rule 6 | <p>Access to personal health information</p> <p>People can see their health information if they want to</p> | <p>The right of an individual to seek access to their personal information and request correction where appropriate is not affected by the Programme.</p> <p>The NITC will have the ability to retrieve and amend information relating to an individual if requested.</p> | Low |

²² Page 9 of the 'AWS – Using AWS in the Context of New Zealand Privacy Considerations May 2018'
https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf

²³ Privacy Impact Assessment on the use of Microsoft cloud services 23 October 2018

| | | | |
|---------------|---|---|-------------------|
| <p>Rule 7</p> | <p>Correction of health information</p> <p>They can correct it if it's wrong</p> | <p>Corrections can be made to NCTS information to update if new / corrected details are appropriate. Any changes made will be auditable.</p> <p>The Ministry's Data Access Policy sets out a procedure for individuals applying to access their own information. It states:</p> <p style="padding-left: 40px;">Under the Privacy Act 1993 you are able to request a copy of any data held about you. Should you wish to do this, please email information@moh.govt.nz with the specific information you would like as well as your contact details and we will be in touch. Before releasing personal information we need to confirm your identity. We do this by asking you a standard set of questions²⁴.</p> <p>It is considered that this policy, which is followed by those staff responding to the request, meets the provisions of the HIPC. Accordingly, it is considered that the risk of rules 6 and 7 being breached by operation of the NCTS is low.</p> | |
| <p>Rule 8</p> | <p>Accuracy etc. of health information to be checked before use</p> <p>Make sure health information is correct before you use it</p> | <p>The NCTS is not a clinical treatment database, but it will contain some elements of a Consumers health management (including the Daily Check-in for confirmed and probable Cases). Accuracy is therefore an important feature, and these records will be treated as part of the Consumers health record.</p> <p>It is expected that the original test results will come from an authoritative source (the laboratory).</p> <p>There will be challenges with identification and contact details in some instances, but on balance the use of the NCTS is expected to significantly improve accuracy over the previous manual and nationally fragmented Contact Tracing activities:</p> <ul style="list-style-type: none"> • Address / contact details will be checked against the NHI / NES information held within Ministry databases as being considered to have the most up to date contact details readily available to the Ministry. All data will be indexed by NHI where available. This will minimise the risk of Consumer information being allocated to the wrong person and ensure that the right things are happening for the right people. • If necessary, the Finding Services (as per Appendix Four) will assist with checking accuracy of contact and identification details as required. • Incorrect advice may be received from individuals about who their contacts were (either wrongly identified people, or not all people who were in contact are remembered or known etc). This will be managed as much as possible by the phone contact with the Contact Tracer to follow up ambiguities or errors where identified. <ul style="list-style-type: none"> ○ It is acknowledged that people could be incorrectly identified, and that is why the involvement of personal contact from Contact Tracers is designed to minimise the opportunity of this happening by communicating directly with the person concerned and checking details with them. ○ Contact and Location details will be checked with individuals when the Contact Tracers have been able to make contact with them. <p>The electronic database record is expected to reduce some of the opportunities for error on the manual spreadsheet operations, but will still rely on manual input from Contact Tracers. The use of electronic pathway and reporting features will enable management of</p> | <p>Low</p> |

²⁴ <http://www.health.govt.nz/publication/current-data-access-policy>

| | | | |
|---------|---|---|--|
| | | Cases on pre-determined pathways and will minimise the opportunity for failure to complete Contact Tracing follow up or clusters within an appropriate time frame. | |
| Rule 9 | <p>Retention of health information</p> <p>Get rid of it when you're done with it</p> | <p>The retention policy will be finalised in the near future. The expressed intent is that information will generally not be retained in an identifiable format beyond the end of the pandemic, subject to any health record requirements. At this point in time there will not be any deletion of information from the system until that policy is finalised. The current expectations are as follows:</p> <ul style="list-style-type: none"> • Compliance with the Public Records Act 2005 and related Disposal authorities (currently being investigated in terms of specific COVID-19 related activity) • Determination of the aspects of the NCTS information might be considered part of an individual's 'health record' and the applicability of the retention time frames under the Health (Retention of Health Information) Regulations 1996. This will currently relate to any Consumer record where a confirmed or probable Case has been recorded, or Daily Check-In information for a symptomatic individual has been recorded. Non-symptomatic Daily Check-in details do not need to be retained, although a record that the Daily Check-in has / has not been completed will be retained. • One centralised and highly secure record of individuals who have tested positive for COVID-19 is expected to be maintained after the end of the pandemic to ensure that if any future health needs are identified in relation to COVID-19 those individuals will be able to be identified. • Destruction of unnecessary information on set time scales (for example any App provided information that is not recorded within the NCTS as having some validity – either submitted contact details or Digital Diary information - will be routinely destroyed on set rolling time frames). • If the information is not part of the health 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). • In terms of the NCTS Border Register the original datasets supplied by MBIE and Customs will both be deleted once no longer required to resolve any transfer errors arising (estimated destruction within 24 hours of receipt). The Customs Information Disclosure Agreement requires information provided by Customs that is not part of a health record to be deleted or anonymised within 20 working days of the date on which the COVID-19 Public Health Response Act 2020 is repealed. The MBIE Agreement requires information transferred into the Border Register be managed in accordance with the relevant NCTS retention policy. | Low |
| Rule 10 | <p>Limits on use of health information</p> <p>Use it for the purpose you got it</p> | <p>The information collected is to be used only for contact tracing, and directly related, purposes in the COVID-19 situation (such as analysis, reporting and planning nationally and regionally).</p> <p>This will essentially be a limited data set – of those confirmed or probable Cases of COVID-19 and any potential Close Contacts.</p> <p>It will be important to manage any risk of function creep. Strong data governance must be provided to retain oversight of any potential use of the NCTS information to ensure that use remains consistent with purpose. It is recommended that the Privacy Information made available (on the Ministry website) will be explicit about all intended uses for the NCTS information, and that the Governance Group monitor to ensure those identified uses are complied with.</p> | Low provided appropriate governance is in place |

| | | | |
|---------|--|---|------------|
| | | <p>If there is any research intent at this point that is consistent with COVID-19 purposes it is suggested that also be incorporated into the Privacy Statement. It is recommended that the SDA process controls for Snowflake also address this research point and make any necessary restrictions on future use by authorised users.</p> <p>Statistical and research reporting from the information held by NCTS in a non-identifiable format will not breach Rule 10.</p> <p>Secondary purposes such as service improvements, teaching, research and audit must be well-publicised and use anonymised or pseudonymised data wherever possible. Any new secondary purposes should only be adopted with proper consultation and with careful consideration of the potential risk to public trust in the NCTS. Guidance can be found in Appendix Thirteen of the Health Information Governance Guidelines describing the methods of reducing risk of consumer identification.</p> | |
| Rule 11 | <p>Limits on disclosure of health information</p> <p>Only disclose it if you have good reason</p> | <p>This provision does not obligate the agency to disclose any information, but allows it to make a disclosure if the principle applies. Disclosures will be limited to purposes associated with contact tracing and the COVID-19 response.</p> <ul style="list-style-type: none"> • Initial contact is made by the Public Health Unit (PHU), they contact the patient to let them know their test result is confirmed (or suspected). This is a health professional talking to the patient. This involves disclosure of a positive test to an individual and would be covered by rule 11(1)(a)(i) – disclosure to the individual concerned. The PHU or a GP is also responsible for notifying negative test results. The NCTS will be able to use fully verified details (email or letter) to advise of negative results in future. • Once Close Contact information is obtained, there may be general disclosure from the Contact Tracer of relevant matters to the Close Contact (the focus is on the Exposure Event rather than the confirmed or probable Case). • All contact tracers will be trained and will work from a script to minimise the possibility of disclosing inappropriate information about a person who has tested positive to Close Contacts, or any other person that they need to obtain information from. Disclosure to any potential contact will be in accordance with section 92ZZ of the Health Act: | Low |

| | | | |
|--|--|---|--|
| | | <p>92ZZ What contact tracing involves</p> <p>Contact tracing, in respect of an individual with an infectious disease or suspected of having an infectious disease, involves—</p> <ol style="list-style-type: none"> (a) ascertaining the identity of each of the individual’s contacts; and (b) communicating with each contact, so far as this is practicable and appropriate; and (c) ascertaining the circumstances in which the infectious disease or suspected infectious disease may have been transmitted to or by the contact; and (d) providing information and advice to the contact about the risks that the contact faces because of his or her exposure to the infectious disease or suspected infectious disease, including, where appropriate, advice about— <ol style="list-style-type: none"> (i) medical examinations for the infectious disease or suspected infectious disease; and (ii) the risk that the contact may have transmitted the infectious disease or suspected infectious disease to others; and (iii) the risk that the contact may pose to others; and (iv) appropriate exclusion, treatment, and prophylaxis; and (e) obtaining information about the contacts of that contact, including information required under section 92ZZC in relation to those other contacts. <ul style="list-style-type: none"> • It is important to note that section 92ZZG provides a duty of confidentiality on each contact tracer, (and others) particularly about the individual who may have transmitted the infectious disease or exposed the contact to risk of infection: <p>92ZZG Duty of confidentiality</p> <ol style="list-style-type: none"> (1) A contact tracer who approaches a contact under this Part or approaches a person under section 92ZZF must not, as far as practicable, disclose to the contact or that other person the identity of the individual who may have— <ol style="list-style-type: none"> (a) transmitted the infectious disease to the contact; or (b) exposed the contact to the risk of contracting the infectious disease. (2) Despite anything in the Privacy Act 1993, information provided or obtained by a contact tracer under this Part may not be used or disclosed by anyone except for the effective management of infectious diseases, but nothing in this section limits the right of an individual to access or disclose information about him or her under that Act or any other Act. <ul style="list-style-type: none"> • Each ‘disclosure’ arising from access by authorised users is limited by role to be consistent with the purposes associated with Contact Tracing. The NCTS Contact Tracing application is established for the purposes of supporting the contact tracing activities associated with COVID-19. Authorised user access for the purposes of Contact Tracing and effective management of infectious disease is consistent with Rule 11(1)(c) – it is one of the purposes in connection with which the information was obtained. It is also consistent with the duty of confidentiality in clause 92ZZF(2) of the Health Act: <i>‘information provided or obtained by a contact tracer under this Part may not be used or disclosed by anyone except for</i> | |
|--|--|---|--|

| | | | |
|---------|---------------------------|--|--|
| | | <p><i>the effective management of infectious disease</i>'. Authorised users of the Contact Tracing application are limited to those who are involved in the effective management of infectious disease.</p> <ul style="list-style-type: none"> • There are external contractors who will assist with overflow capacity for Close Contact tracing, and, in the next NCTS release access will be limited to only the assigned Cases for that contractor. These contractors will fit within the provisions of section 3(4) of the Privacy Act 1993, and so the information will be deemed to be held by the Ministry, so is in itself an access by an authorised user as described above. • A positive result arising from a test within a Managed Isolation Facility will be managed by Contact Tracers in terms of notifying the individual of the result, and also informing the relevant authority of the result in order to ensure appropriate health care and management of that Case are handled appropriately. The management of the person within the facility is part of the All of Government response, only the contact tracing component is managed via the NCTS Contact Tracing application. • Operational reporting (for planning resourcing needs and responsiveness time frames) is available to a PHU within the NCTS, as it would be if it had retained the relevant contact tracing information within its own IT system rather than participating in the NCTS. <ul style="list-style-type: none"> ○ The difference is that this NCTS provided information will be a national rather than regional dataset. The access to this information will be controlled by Role Based Access Controls. This provides a national viewpoint which has proven to be a critical tool in the management of COVID-19. PHUs can securely share information as required (with all access tracked) and the integrity of the information can be maintained. • The secure Ministry Snowflake database may be made available for analysis and reporting purposes to authorised users. Snowflake has role-based access controls that can be controlled at a detailed level of granularity. <ul style="list-style-type: none"> ○ The Snowflake Data Assessment Process will be completed prior to access being granted (as set out in the Snowflake PIA). This will be in conjunction with the clinical and information governance representatives of the NCTS to ensure that matters such as limits on access, what level of identifiable data is to be available and any limitations on future record retention are determined and implemented. It is expected that very limited numbers of individuals in each region, and from within the Ministry, will be granted access rights to these national level records for bulk analysis of information, and regional controls are likely to be applied. • Care will need to be taken by the NITC finders service in any disclosures made to third parties to attempt to obtain relevant contact information. Processes identified in Appendix Four are to be followed. It is recommended that consideration be given to a 'standard' or memorandum to be drafted and used as guidance on the procedures to be consistently applied to ensure compliance with the external third parties (currently Customs and Police). This would address the obligations of each party in terms of information exchanged, secure methods of making the exchange and the obligations of parties in respect of destruction of the information. This process is already underway. • It is also recommended that amendments to Subpart 5 of Part 3A of the Health Act be pursued for clarity about which entities may be requested to provide information, and in what circumstances. | |
| Rule 12 | Unique identifiers | The NHI may be used to assist in correct identification of individuals (particularly in relation to an individual with a confirmed or suspected Case to avoid persons with a similar or identical name being mistakenly identified) and to link to other Ministry databases | |

| | | | |
|--|---|--|--|
| | <p>Only assign unique identifiers where permitted</p> | <p>with potential contact information for that same purpose. It will also enable the status of the individual to be entered on their NCTS health record (and if necessary engage with their health provider if requested – this is not a standard part of the NCTS process).</p> <p>No NHI information is to be shared with any agency that is not itself approved to assign the NHI under Schedule 2 of the HIPC.</p> <p>Each test result holds an ESR assigned number to uniquely identify that test. They are recorded within the NCTS, but not used as a unique identifier in their own right.</p> | |
|--|---|--|--|

Appendix One – Contact Tracing – the system supported by the NCTS

Background

1. Contact tracing is one of the pillars of the public health response to this infectious disease pandemic. The pillars include border control measures, testing, Case identification and Case isolation.
2. The purpose of Contact Tracing is to obtain information about the contacts of persons with infectious diseases or probable Cases in order to:
 - 2.1. Identify the source of the infectious disease or suspected infectious disease
 - 2.2. Make contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary
 - 2.3. Limit the transmission of infectious disease or suspected infectious disease²⁵
3. A crucial part of the process involves locating and contacting both the Case and their Close Contacts. Once a person is identified as a probable or confirmed 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.
4. The current metric is for the time between notification of a confirmed Case result to tracing a Close Contact and advising of isolation requirement at 80% of Cases within 48 hours.
 - 4.1. This enables appropriate advice and instructions to be provided to Close Contacts, in the interests of public health and safety as well as the interests of the specific individuals involved.
 - 4.2. Examples of this information can be found in the fact sheets [here](#). Notably this includes advice about self-isolation for a 14-day period from date of last contact with the confirmed or probable Case.
 - 4.3. The Case, and Close Contacts, are monitored for symptoms during the relevant infection period (or potential incubation period of 14 days since last contact). This is generally by daily phone monitoring (or potentially via App or web interface if that is appropriate).
 - 4.4. There may also (rarely) be intervention if non-compliance is identified, such as breaches of self-isolation.
 - 4.5. Individual Cases end when the original Case, and all potential Close Contacts who became infected, are ‘recovered’.

²⁵ Section 92ZX of the Health Act 1956

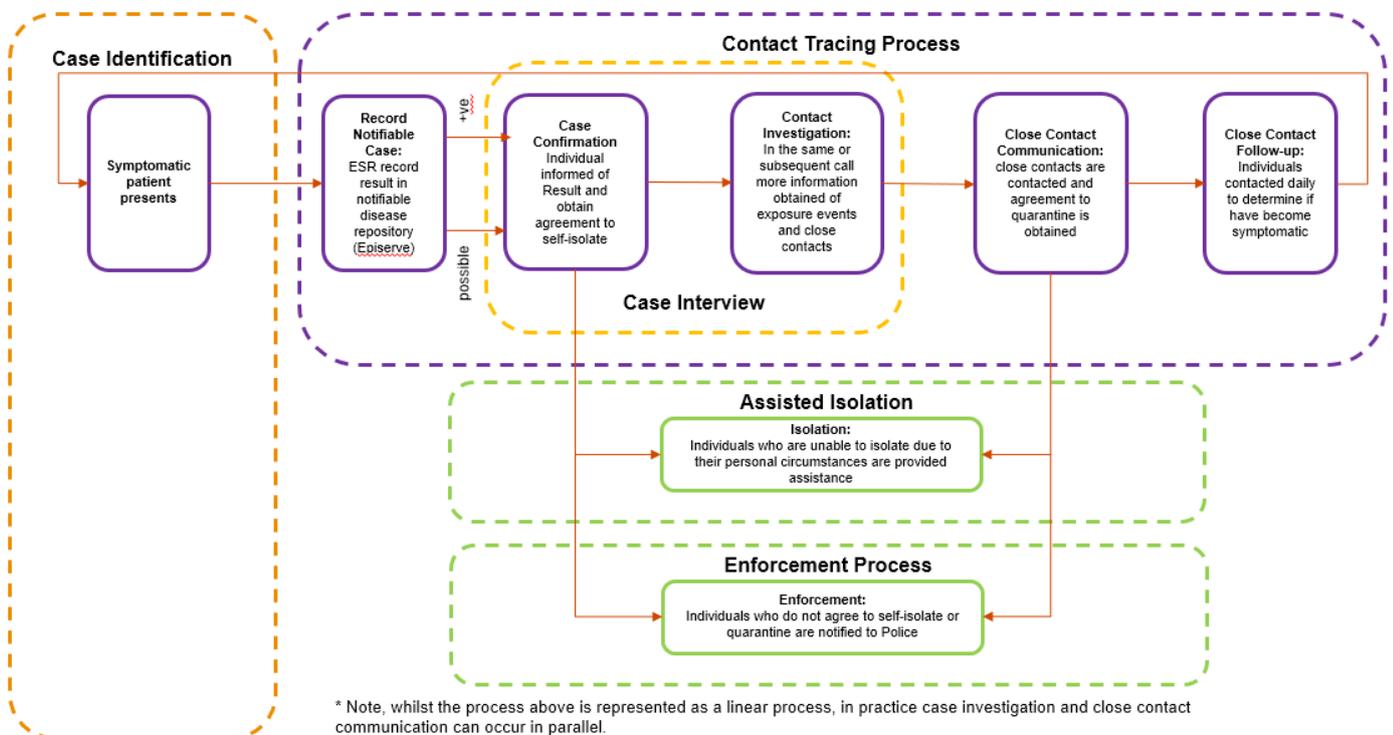
- The Ministry of Health website advises individuals [‘getting tested’](#) that *‘We will collect only as much information as we need to, so that we can let you know about your test result and to help us report on COVID-19 testing. We will only share your test result with your doctor if you ask us to and give us their contact details...If necessary, information about a positive test result may also be shared with emergency service in your area to help them in their response, but it will not be used for immigration-related or enforcement purposes’.*

The Health Act 1956 – the contact tracing provisions

- Management of infectious disease in New Zealand is subject to Part 3A of the Health Act. Subpart 5 of Part 3A governs specific contact tracing activity. This is the key source of authorisation for collecting, using and disclosing information about Cases, and their Close Contacts.
- 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.
- The Ministry website provides additional details about [Contact Tracing for COVID-19](#). This includes the current definitions of Close Contacts and Casual Contacts.

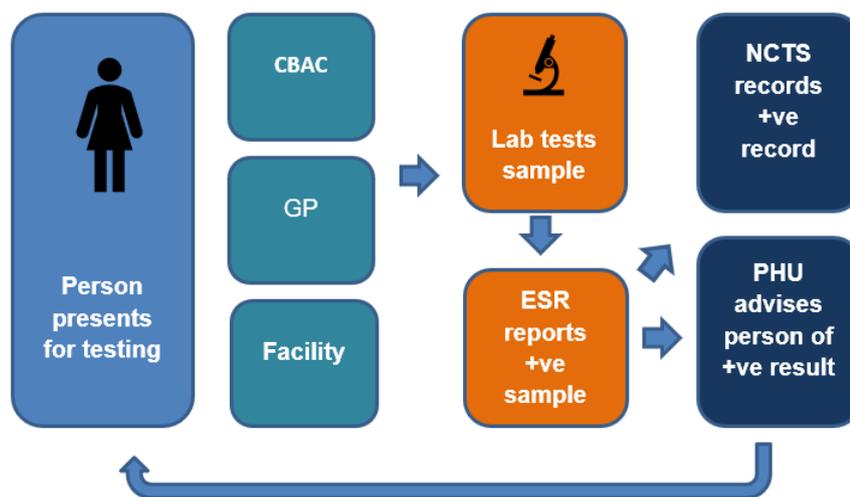
NCTS management of the Contact Tracing Process

- The general NCTS contact tracing process is outlined in the diagram below²⁶:



²⁶ ‘Finders’ service and borders not included in this diagram

10. Further details of the NCTS process flows for the Contact Tracing process are set out in Appendix One – Annex One.
11. The management of a 'Case' (a person who is a confirmed or probable Case of COVID-19) involves a process. This starts with a confirmed or probable Case of COVID-19 (the 'Case'), and progresses through a number of 'Contact Tracing' components to identify those who may have been exposed to COVID-19.
12. The initial confirmed test result is sent from the laboratory to ESR²⁷, as it performs public health surveillance of infectious disease on behalf of the Ministry of Health.
13. ESR forwards the information to the NCTS and to the relevant Public Health Unit (for the region in which the person is residing).

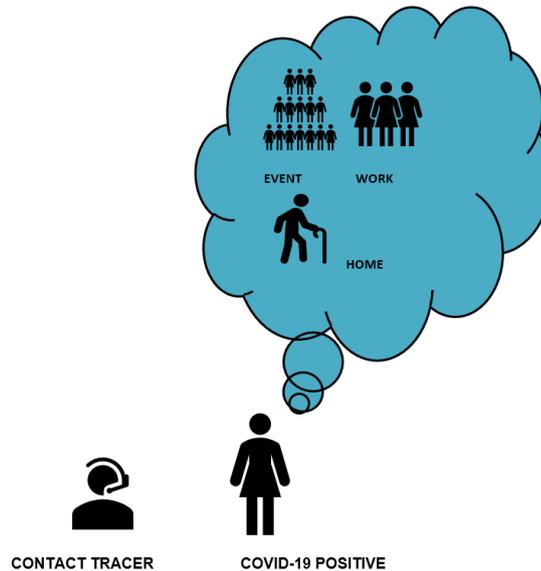


14. The Contact Tracing process involves the Contact Tracer engaging directly with the positive Case.
 - 14.1. It starts with 'Call 1' (the primary call) where the trained clinician (usually a Public Health Unit member who will be a nurse, doctor or health protection officer) contacts the individual, usually by phone, to inform them of the positive test result (or probable Case).
 - During this call relevant clinical advice is provided about what the individual needs to do in terms of keeping themselves and others safe.
 - A further time is made for the Contact Tracer to call the individual back to discuss potential Close Contacts.
 - 14.2. Call 2 (the 'interview' call) is when the Contact Tracer (commonly called the 'Case investigator) will call the Case (or probable Case) to review with them

²⁷ ESR can also perform diagnostic tests.

who they may have been in contact with, and where they have been, in the period during which they were likely to have been infectious.

15. This Call 2 review is designed to identify where the individual may have contracted the infection, and also who may be at risk of it being passed on to them by the Case (Close Contacts²⁸). The Case investigator will be attempting to identify contacts (either Close Contacts or Casual contacts) with others and potential Exposure Events:



16. Section 92ZZC provides that individuals with 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. Generally, Cases do not need to be 'required' to provide the information as they provide it willingly to the Contact Tracers.
17. The Case will use their memory, perhaps refer to the App Digital Diary (if they have been using one), or other information available to them such as their own bank accounts, and discuss with the Contact Tracer who they may have come into contact with.
18. The Contact Tracer may need to speak with the Case, or probable Case a number of times as they work together on identifying a list of potential Close Contacts or locations of interest. The Contact Tracer will discuss with the Case matters such as how long they were at a location, what they did there, and whether they can identify the individuals who they come in contact with.
19. The Contact Tracer will apply their clinical knowledge to the information provided and determine what individuals need to be contacted as Close Contacts (or high risk casual contacts). Considerations of this risk include the proximity of the Case to others, the length of time over which that contact occurred and what activity was involved.
20. In some instances the Case may not know the contact details for individuals, or they may know a location they visited, but not who else was there. Depending on where the

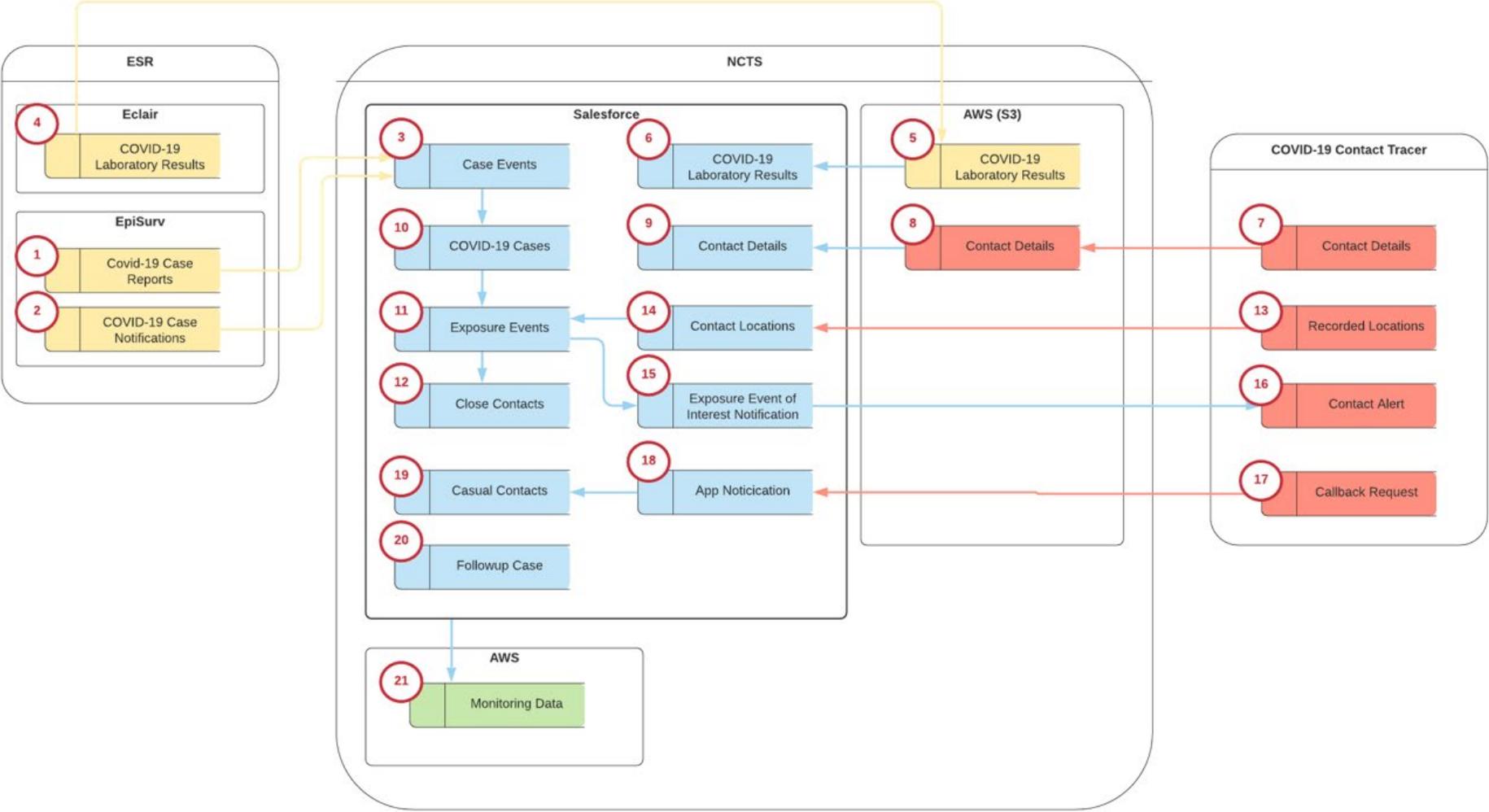
²⁸ In identifying potential Close Contacts the Case investigator will generally cover up to 48 hours before the onset of symptoms to identify those who may be at greatest risk of infection from the Case

individual has been in the relevant 'infectious' period this may be a number of individuals they know well and have contact details for. Alternatively, they may have travelled, have been to events where they do not know the other individuals who attended, or may be able to give some identity information, but not contact information.

21. In these instances, the Contact Tracer may use the provisions of subpart 5 of Part 3A of the Health Act 1956 to seek information from other sources. In the event that a Close Contact cannot be promptly located the PHU is likely to refer the matter to the National Investigation and Tracing Centre (NITC) to enable follow up by the 'Finders' service. More details on this service are contained in Appendix Four.
22. Section 92ZZF provides that a Contact Tracer may require a range of third parties to provide the Contact Tracer with the names and addresses of the contacts that are known to that person. The current provisions are set out below, but the Ministry is considering seeking amendment to these provisions for additional clarity on all parties information can be requested from:
 - (2) *The persons are—*
 - a. *the employer of the individual;*
 - b. *an educational institution attended by the individual;*
 - c. *any business or other organisation that the individual has dealt with;*
 - d. *an event co-ordinator or other person likely to have a list of persons attending an event.*
 - (3) *A person referred to in subsection (2) must provide information in response to a request made under subsection (1) despite anything in the [Privacy Act 1993](#).*
 - (4) *Despite anything in the [Privacy Act 1993](#), if a person requires another person to provide information under this section:*
 - a. *the person required to provide the information must comply with the requirement and be advised that the information must be provided for the effective management of infectious diseases; and*
 - b. *nothing in this section limits the right of an individual to access or disclose information about him or her under that Act or any other Act.'*
23. Once the Close Contacts, and their contact details, have been identified a Contact Tracer will contact those Close Contacts (this is known as Call 3). It is also possible in some instances that higher risk casual contacts may be called as part of this process (if a clinical decision is made to this effect – usually determined within the NITC).
24. Call 3 may be managed by the Contact Tracers at the PHU, the NITC or may be managed by Contact Tracer telephony services (as detailed in Appendix Three).
25. The NCTS provides support for the Contact Tracing Purposes. It records identified Cases to maintain Cases on the Contact Tracing pathway and provides 'failsafe' reporting services to signal when a Case requires further action to make sure no step in the process is overlooked. More detail can be found about the NCTS database capabilities in Appendix Two.

Appendix One – Annex One

The NCTS contact tracing dataflows are as follows:



| | |
|----|---|
| 1 | COVID-19 Cases are recorded in EpiSurv as the system of record within New Zealand for notifiable disease. The Case reports once created are sent to the NCTS to trigger contact tracing. |
| 2 | COVID-19 Case notifications are sent from ESR EpiSurv, those notifications indicate that a result has been received from the laboratory. These notifications can be used to trigger contact tracing processes where a Case has not been raised in EpiSurv. This is to expedite any urgent requirement to initiate the contact tracing process |
| 3 | Case Reports and Case Notifications are recorded as Case Events in the NCTS. Case Events are the entry point into the contact tracing process and are used to establish the Contact Tracing Case. |
| 4 | Covid-19 Laboratory results are collected from the Labs by ESR and stored in their Éclair System. This include all laboratory results (positive and negative) |
| 5 | COVID-19 test results are sent by ESR to the NCTS, these results (positive and negative) are stored in a secure S3 bucket on AWS. Results are updated periodically throughout the day. |
| 6 | The COVID-19 test results are pulled by the NCTS Salesforce App for Confirmed Case. This is required to support monitoring and failsafe requirements to ensure that a result has been recorded for every Confirmed Case of COVID-19 |
| 7 | NZ COVID Tracer App users can submit updated contact details in the App, these contact details are sent to the NCTS by the App. |
| 8 | Contact details submitted by the App are stored in a secure S3 bucket on AWS. |
| 9 | Contact details submitted by the App are available for query by NCTS Salesforce where a user (contact tracer) has identified the need to look for additional contact details. Where a contact detail for the Case exists in S3 the user will create a Contact detail for the Case within NCTS Salesforce. |
| 10 | From a Case Event (typically a Case report for a confirmed or probable Case) a COVID-19 contact tracing Case is created. |
| 11 | Once a Case has been created the investigation process will identify Exposure Events for the Case |

| | |
|----|---|
| 12 | Close Contacts will be identified for each exposure event |
| 13 | Were a Case has been identified, the person associated with the Case will be contacted as part of the investigation. Where the person is an App user they will be asked to submit their Digital Diary (including recorded Locations) to support contact tracing. |
| 14 | The Recorded Events submitted by the App user are stored as Contact Locations via a secure API. Contact Locations are only retained for a period of six months unless they have been identified as a location of interest for contact tracing and converted to an exposure event for the Case. |
| 15 | Where contact tracing has identified a “high risk” exposure event the contact tracer may create an Exposure Event of Interest, this creation will issue a notification to the App The exposure event of interest notification will identify the location and the time period to be notified. Multiple notifications can be issued for the same exposure event. |
| 16 | The Exposure Event of Interest Notification will be received as a Contact Alert by the App. App users will be notified where they have a recorded location (stored locally on their device) that matched the parameters of the Contact Alert (Exposure Event of Interest) |
| 17 | Where an App user has been alerted via a Contact Alert they will be able to issue a call back request (currently disabled in the App). |
| 18 | App Notifications (call back requests) are submitted to the NCTS via a secure API and are accessible through a managed list / queue – this functionality is available but not yet activated for the App |
| 19 | Casual contact records are created from the App notifications. Casual Contacts are people who may have been in contact with a Case but who do not meet the criteria to be classed as a Close Contact. Casual contacts will be reviewed by a contact tracer, where it is determined that a casual contact needs to be contacted they will be converted to a Close Contact for the Case |
| 20 | Cases and Close Contacts are required to complete daily check-ins. These daily check-ins are managed through a Follow Up Case within NCTS Salesforce Follow ups are conducted via phone interview or through self service survey issued by Salesforce. Persons completing a Follow-up process will be able to access the surveys from a secure link issued via email or via the consumer App (Release 3) No personal details are collected on the survey form. |

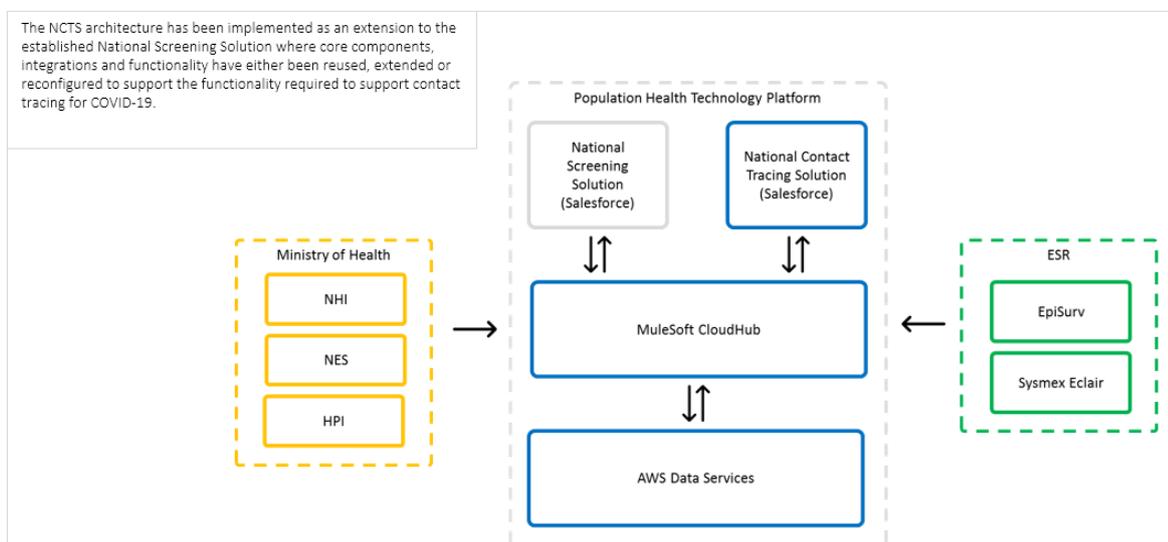
| | |
|----|--|
| | <p>Survey responses are recorded on the Follow Up Case, where a person identifies that their situation has changed (e.g. become symptomatic) this is recorded on the Case / Close Contact as required.</p> <p>Where Close Contact has been identified as symptomatic a new Case may be created for contact tracing purposes.</p> <p>Survey data is linked to but managed separately from the COVID Case, a record of all follow up activity will be retained for audit purposes but the responses are available to be deleted once they are no longer required to support Contact Tracing or monitoring.</p> |
| 21 | <p>All data within the NCTS is managed within the NCTS Data Management Layer and is available to support the Monitoring framework (reporting on key indicators for COVID-19)</p> |

Appendix Two – the NCTS Database Facility

Background – Core NCTS Environment

1. An urgent technology solution to support the end to end national contact tracing process was required. This needed to scale up at speed and cater for a remote workforce (due to then current lock down requirements). It needed to meet privacy and security concerns and be capable of managing the contact tracing pathway with safeguards to ensure all Cases were managed and contacts followed up.
2. It was determined that the National Screening Solution (NSS) core platform (based on Amazon Web Service / Mulesoft), would be used with a new Salesforce ORG (instance).
 - The NSS is the new Ministry IT solution developed for the National Bowel Screening Programme (NBSP).
 - This reuse of an existing platform meant that the Ministry were able to operate with confidence that the system was secure (noting that the Ministry is continuing to test security as the NCTS develops).
 - It also provided confidence that key privacy concerns were being addressed from a system perspective. The National Screening Solution (NSS) NBSP had successfully achieved Go Live on 24 March, and had followed extensive privacy assessment during the development stages.

NCTS Overview: Architecture



Workstream collections supported by the core NCTS environment

3. The NCTS environment has now been able to be leveraged to support four distinct workstreams required in the pandemic response. These include the NCTS Contact Tracing collection that is the subject of this Privacy Impact Assessment. In addition, the Border Register, Border Staff Testing and the Managed Isolation Exemptions Process workstreams are being supported by an NCTS collection. Each of these will be addressed in their own Privacy Impact Assessments.

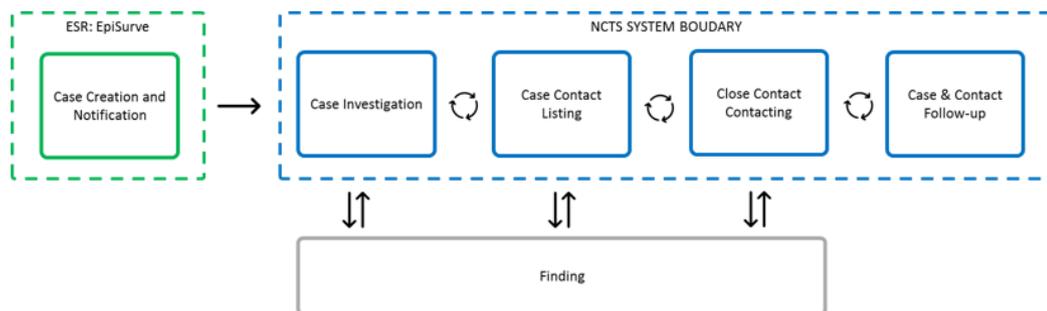
The NCTS Contact Tracing component

4. All national Case records are now held within the NCTS. All Public Health Units are now using the NCTS national system to record Cases and Contact Tracing activity.
5. Under the NCTS model (based on the NSS) integration with the National Health Index (NHI), National Enrolment Service (NES) and Health Provider Index (HPI) is in place. These are key features that enable individuals to be uniquely identified within the New Zealand Health system (NHI), current contact details to be obtained about the majority of individuals (NES) and also link to a current medical practitioner if necessary (HPI).
6. The contact tracing process is detailed in Appendix One, and the related finding service is detailed in Appendix Four. The method by which the NCTS supports these activities is summarised below:

NCTS Overview: Core Processes Supported

The diagram below provides a logical representation of the processes supported by the NCTS which can be defined as follows:

- **Case Investigation:** Once a person has been identified as a confirmed or probable case the person is contacted and contacts are identified by asking about the person's activities and the activities and roles of the people around them since onset of illness. Contacts can be anyone who has been in contact with an infected person: family members, work colleagues, friends, or health care providers.
- **Case Contact Listing:** All persons considered to have contact with the infected person are listed as contacts, efforts are made to identify every listed contact. Where contacts cannot be fully identified a request to the Finders Service will be invoked. The Finders Service will search through all available data sets and engage external agencies and third parties to collect data to help identify the close contact
- **Close Contact Contacting:** Verified Close Contacts are passed to the Close Contact Contacting service. Close Contacts are informed of their contact status, what it means, the actions that will follow, and the importance of receiving early care if they develop symptoms. Close Contacts should also be provided with information about prevention of COVID-19 and in some cases, quarantine or isolation is required for high risk contacts, either at home, or in hospital.
- **Case & Contact Follow-up:** Regular follow-up should be conducted with Cases and Close Contacts to monitor for symptoms and test for signs of infection.
- **Finding:** Through the establishment of the NCCS and NCTS it has been identified that the ability to find people quickly and consistently is one of the key issues that needs to be resolved as there is currently no consistent process locally, regionally or nationally that is followed to support finding which has resulted in inconsistent results and errors. Finding is a common problem across all health services and a paper is being developed



7. All Cases are followed on a pathway. Reporting is able to be regularly generated to make sure no Cases or Close contacts are missed. Appendix Two - Annex One contains the flow chart summarising the available NCTS Contact Tracing system monitoring.
8. A number of new components were added to the NCTS architecture. These include:
 - Amazon Connect (a cloud contact centre), which provides a soft phone solution for outbound calls. This is integrated with the Salesforce components. This can support telephony services (further described in Appendix Three).
 - Office 365 – use of the Ministry Teams service including instant messaging, audio and video calling, online meetings, mobile experiences, and web conferencing capabilities. This will not be integrated to the NCTS but will be a secure product to be used by NITC and contracted providers, using Azure AD to provide single sign on approach for the National Investigation and Tracing Centre (NITC). Staff training is

that all personally identifiable 'Case' information must be maintained in Salesforce – and no downloading of email and file attachments is permitted in Salesforce.

NCTS Contact Tracing Data Inventory

9. The NCTS data inventory includes the full details of all data fields collected onto the NCST and the interrelationships of that data²⁹.
 - This includes the personally identifiable information about each person tested for COVID-19, each Case and each Close Contact.
 - The relationships between Cases such as Close Contacts, an Exposure Event, or related Cluster³⁰.
 - The processes. Each required notification, or monitoring activity is recorded – up until a case is recorded as closed. Dates and mandated process activities are recorded. This enables progress to be monitored and fail-safe reports to be generated. This includes for example Case management and Close Contact workflows, and follow up via the Daily Check-in process (including records of decisions and call logs).
 - Audit and confirmation details are included. The DHB and contact tracers interaction are recorded as they interact with each Case or Close Contact. The context in which much of the information fields around contact details are also recorded (what date was the contact detail identified and what source did it come from – from a picklist, such as 'interview, NES, NZ COVID Tracer App, National Bowel Screening Programme, other, Police, Customs).

Security

10. The NCTS has strong security as detailed in the Rule 5 Section Three Privacy Analysis. The project was subject to an Interim Approval to Operate at the outset. The Ministry has been progressing the Certification and Accreditation process which is due for completion at the end of October 2020. This will include additional components of the NCTS (including the Border Register and the Exemptions processes).

Role based access and Terms of Use

11. The secure NCTS authorised access processes enable authorised users located throughout New Zealand to access the NCTS as required. For Contact Tracing:
 - Public Health Units (PHUs) are able to enter information directly onto the NCTS from wherever they are located, and can also delegate Contact Tracing tasks to the Ministry for completion (primarily Close Contact calling and Finders services) to meet fluctuating demand.
 - The NITC and contracted surge workforce are able to access the NCTS to complete their allocated tasks.

²⁹ Extensive Data Dictionary records are held of all data fields and their inter-relationships for the end to end processes of Case management within the NCTS. These are updated as the NCTS developments progress.

³⁰ A significant COVID-19 cluster is when there are ten or more Cases connected through transmission and who are not all part of the same household. The cluster includes both confirmed and probable Cases.

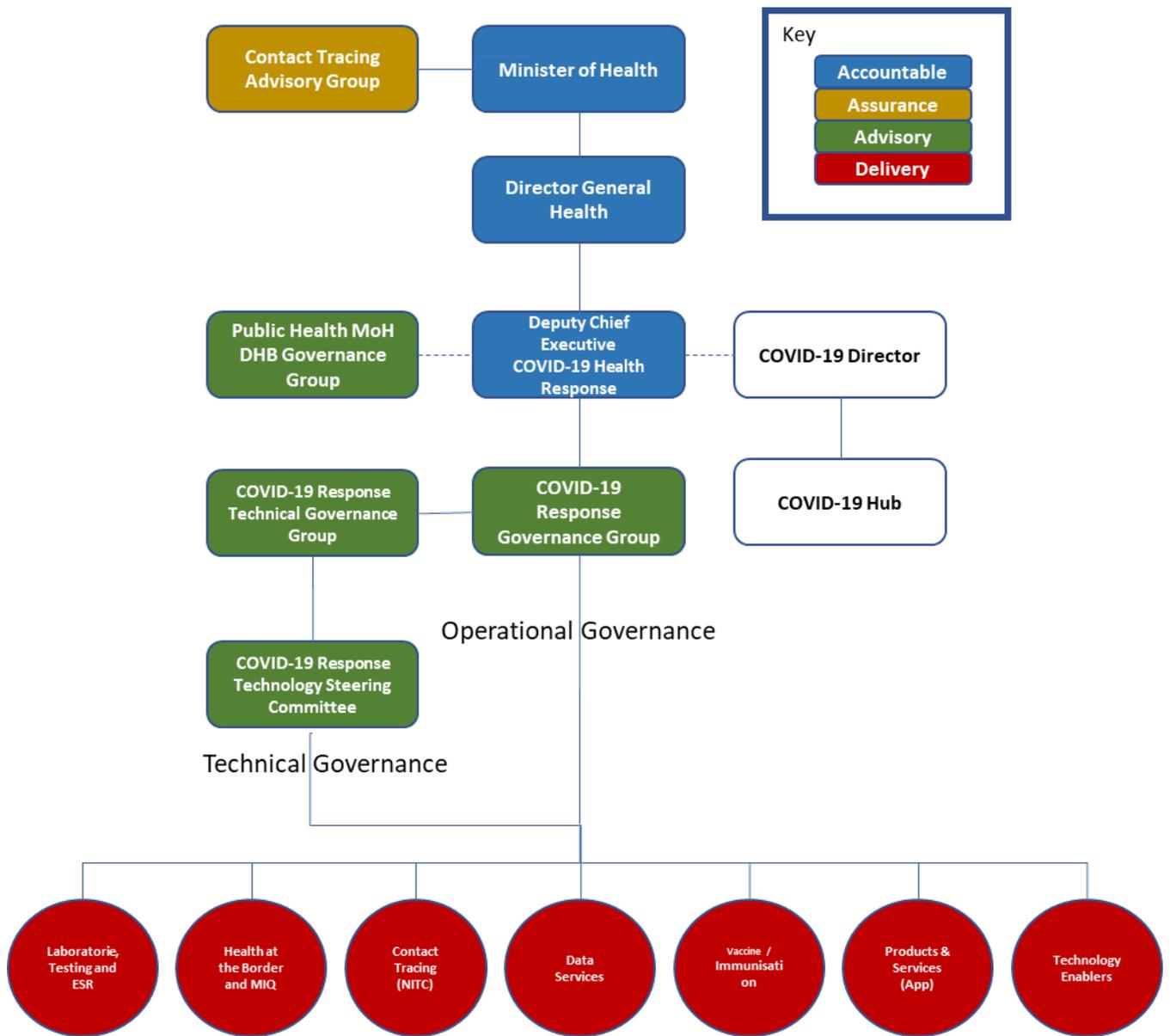
12. Role based access controls for authorised users has enabled multiple user access options to be developed, with each role based on the information it is 'necessary' for that user to perform that role.
13. The division of the NCTS information stored into the various components (Contact Tracing, Border Register, Border Staff Testing and the Managed Isolation Exemptions Process) has enabled further access limits to be applied.
14. All Users are required to electronically confirm Terms of Use prior to being granted access to the NCTS for the first time, and again on each password change (compulsory every three months).
15. The text for Terms of Use is detailed in Appendix Two – Annex Two.

NCTS Governance

16. A Data Governance Framework is in development which will record all information flows and responsibilities, and well as a comprehensive governance process.
17. The Ministry Data Governance Group is currently providing operational assistance by:
 - Overseeing the SDA Process³¹ for any access to the Ministry analytics tool, Snowflake (as it relates to any NCTS information).
 - Reviewing the process for Application for Access to the NCTS Process³².
18. Overall Governance will now be provided by the COVID-19 Response: Technology Governance Group.
19. Technology delivery is governed by way of the COVID-19 Response: Technology Steering Group.
20. The governance arrangements for the NCTS are as set out in the diagram below:

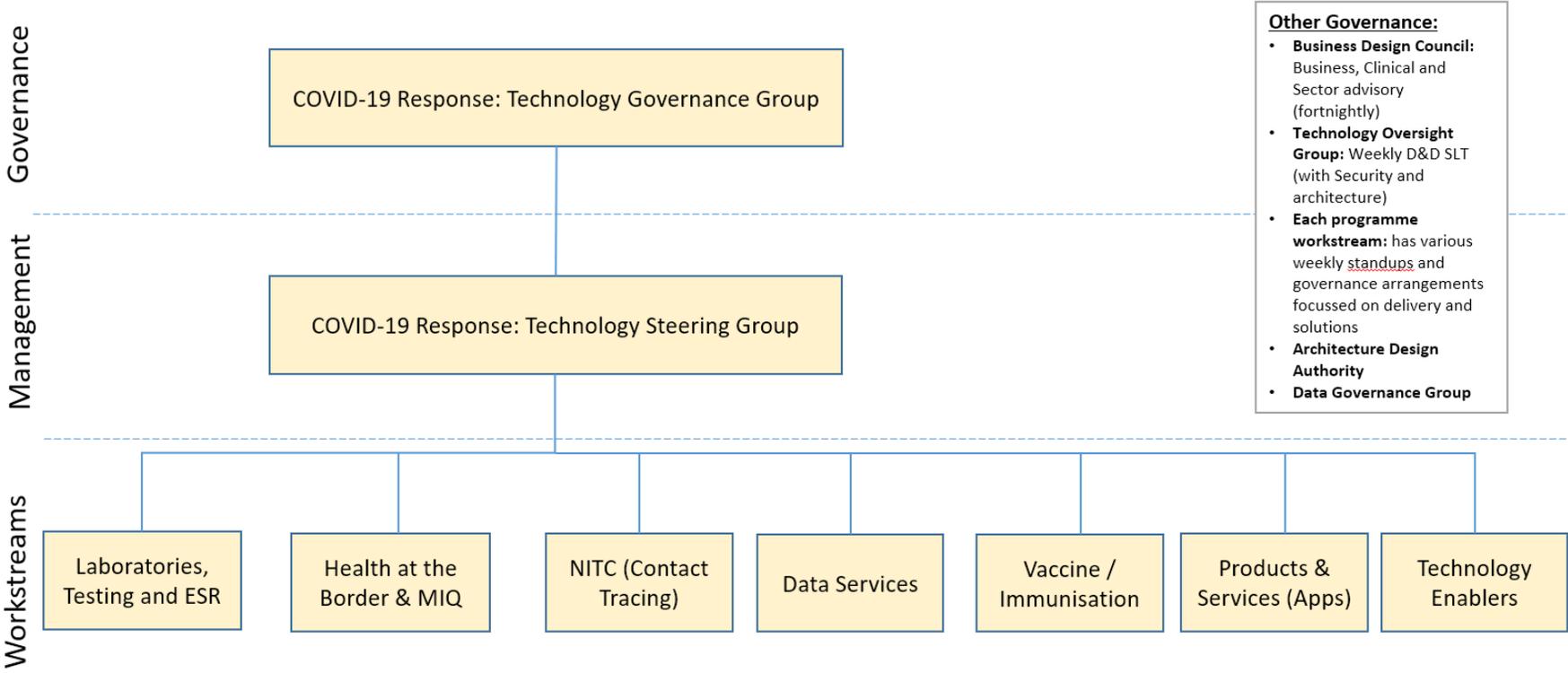
³¹ The Snowflake Data Assessment Process

³² A documented process where an NCTS access request is made that is not within existing authorised roles



COVID-19 Public Health Response Programme

Proposed Governance Overview



- Other Governance:**
- **Business Design Council:** Business, Clinical and Sector advisory (fortnightly)
 - **Technology Oversight Group:** Weekly D&D SLT (with Security and architecture)
 - **Each programme workstream:** has various weekly standups and governance arrangements focussed on delivery and solutions
 - **Architecture Design Authority**
 - **Data Governance Group**



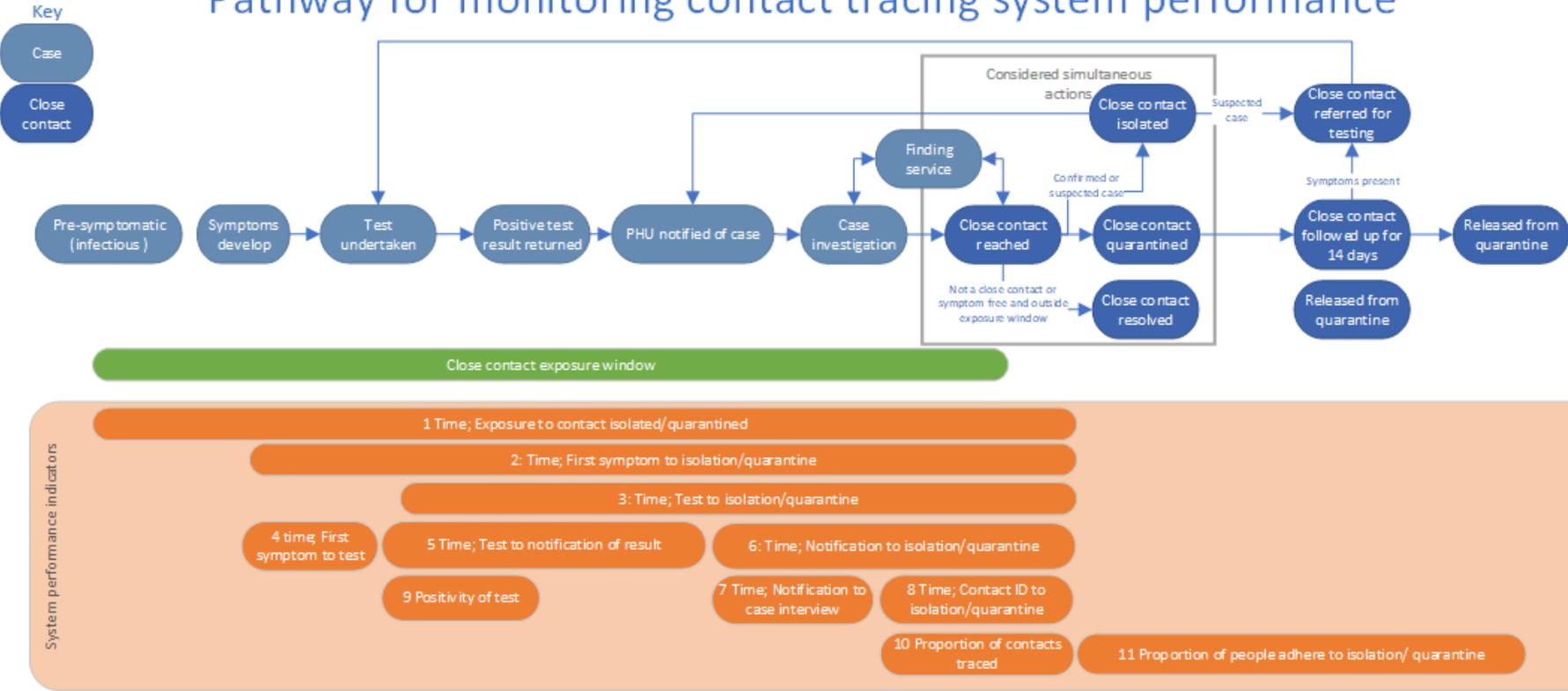
Roles and Responsibilities

| Group | Roles and Responsibilities |
|--|--|
| COVID-19 Response: Technology Governance Group | <ul style="list-style-type: none"> • Approval of workplan (scope) • Approve Change requests impacting workplan (Material scope, timing, budget) • Approval additional funding/drawdown • Sponsorship of initiatives within the Ministry • Liaison / Escalation with AOG |
| COVID-19 Response: Technology Steering Group | <ul style="list-style-type: none"> • Endorsement of workplan (scope, time and budget) • Approval of change requests within the approved workplan • Endorsement of change requests outside of approved workplan • Receive and review of progress via reports from workstream leads to monitor scope, risks/issues, budget and schedule • Ensure appropriate stakeholder engagement for each initiative, including the required operational, clinical and technology representatives are reviewing and endorsing/approving project deliverables • Provide advice and direction to workstream Project/ Programme Managers • Ensure all risks are identified, mitigated, monitored, and where necessary, escalated to SRO |
| Workstreams | <ul style="list-style-type: none"> • Establish workplan to achieve key deliverables (managing scope, time and budget) • Delivery of approved workplan • Management of scope, budget, schedule risks, issues dependencies. • Reporting to Steering Group on progress, scope, risks/issues, budget and schedule • Manage daily activities • Draft change requests for governance approval • Draft funding memos for approval |

Appendix Two – Annex One

National Contact Tracing – System Monitoring

Pathway for monitoring contact tracing system performance



Appendix Two – Annex Two

National Contact Tracing Solution

Terms of Use and Confidentiality Requirements

Welcome new or returning User

Prior to accessing the National Contact Tracing Solution (NCTS) you must read and accept these Terms of Use. You are deemed to have accepted these Terms if you proceed to use the NCTS. Each NCTS user is a trusted part of the COVID-19 response team, and we must all take privacy matters, and the protection of personal and health information, seriously.

As an NCTS User, I accept the following Terms of Use.

- I will comply with the Privacy Act and the Health Information Privacy Code, when using the NCTS or any information related to the NCTS.
- I will keep the NCTS information secure and confidential. I will not knowingly access or disclose any personal or health information about any individual(s) unless such information is essential for me to perform the duties and obligations of my health professional role properly and efficiently.
- I will protect the confidentiality of all personal or health information, including ensuring it is not visible on an unattended computer screen, or in an unattended area which may allow access to the information by unauthorized persons. I will ensure that, so far as it is within my control, such information, whether in the form of paper documents, computerized data or any other form, cannot be viewed by any unauthorized persons.
- I will satisfactorily complete any training offered to me in relation to the NCTS.
- I will not use any unauthorised device to connect to the NCTS and will not download any information from the NCTS unless it is essential to fulfil my role, and I will ensure the security of any such downloaded information.
- I undertake to inform my supervisor/the relevant privacy officer immediately if I become aware of any breach or potential breach of privacy or security in the course of my duties/obligations. The sooner we know, the sooner we can resolve any issues.
- I will cooperate and assist in any investigation or inquiry into any breach, or potential breach, of privacy if requested.
- I understand that my credentials (username and password) for access to the NCTS are only for my own individual use, that I must not disclose the credentials to any other person or use another person's credentials. When I am logged on to the NCTS I will not allow access by any other person to the NCTS or the information on it.
- I understand that my access to the NCTS is always logged and audited. This log and audit information may be used proactively, or reactively in any investigation resulting from a privacy incident / breach.
- I understand that if I do not comply with these requirements my access to the NCTS may be removed, and the matter referred to my employer, or other legal action undertaken if appropriate.
- I will comply with any Standard Operating Procedures applicable to my role as part of the COVID-19 response team.

ACCEPT BUTTON

For more information refer to:

- *Part 3 of the Health Act 1956 concerning infectious and notifiable diseases, and any Orders issued under that Act*

- *The Privacy Act*
- *The Health Information Privacy Code*
- *The Health and Disability Code of Health and Disability Services Consumer's Rights.*

Appendix Three – the Telephony Services Associated with NCTS

1. This section explains the features of the telephone components associated with the NCTS:
 - Technology mechanisms to enhance privacy;
 - Surge workforce; and
 - Training.
2. A large part of Contact Tracing activities involves phone contact with Cases, and Close Contacts. This provides an immediate connection to relevant individuals where a phone contact is available. This gives rise to potential privacy concerns as individuals will be asked over the phone to provide details about themselves and possibly their health.
3. Due to the nature of the pandemic, Cases can occur throughout New Zealand. They are not restricted to remaining within regional boundaries. A significant component of Contact Tracing work is conducted by the 12 Public Health Units. There are also additional available resources within the Ministry in the form of the National Investigation and Tracing Centre, and a contracted 'surge' workforce on standby, trained and ready to assist with contact tracing if the need arises.
4. Remote working arrangements (where individuals work from home in many cases) have become essential during the pandemic. This creates security and privacy risks with working from home scenarios.

Technical security controls on telephony use

5. General applicable security requirements for telephony services include:
 - AWS Connect Internet Protocol Telephony is to be used for telephony by the Ministry NCCS, NITC and Triage) and also the contracted surge workforce. PHUs and HomeCare Medical use their own telephony services.
 - Salesforce and AWS controls where multi-factor authentication is set up through Salesforce as the identity provider. Connectivity is over the internet.
 - Only users with NCTS RBAC will be able to access the relevant queues for telephony, and only then those queues assigned to the team with which the user is associated.
 - All user access to NCTS is logged and audited

Operational processes

6. Operational processes designed to improve Consumer interactions with Contact Tracers, and to enhance security includes:

- Development of a phone script designed to maximise relevant information for Contact Tracing, but minimise unnecessary information (and limit the opportunities for a Close Contact to identify who the infected person may have been). Individuals are advised as part of the script that calls are recorded for training and quality purposes.
- The surge workforce is overseen by duty managers who quality assess and provide advice during call management, with remote management limited to Desktop view only. No manual input or change of records allowed by anyone other than the RBAC authority operating the NCTS record.
- A text to be sent to individual's mobile phones prior to first contact, signalling that a Contact Tracer is about to call, nominating a number that they will shortly call from, and requesting the individual accept the call. This provides some warning for individuals and gives them a chance to prepare to have a conversation with a Contact Tracer.

Pre-service checks and Training

7. All PHU users will be subject to their regional employment requirements regarding confidentiality and codes of conduct.
8. Any Ministry employees to work with the NCTS will have existing obligations to comply with the Ministry of Health Code of Conduct, and confidentiality requirements.
9. Surge workforce requirements require, by contract, that services are delivered in accordance with the Ministry of Health Code of Conduct, Health Information Security Framework HISO 10029: 2015 or Health Information Governance Guidelines HISO 10064:2017 as required. Each contracted surge workforce personnel must complete a declaration of confidentiality, and complete the Ministry of Health Pre-employment check.
10. All individuals given NCTS access rights are required to complete privacy training (in their role as PHU employee, Ministry employee or contracted provider). They must also complete the Terms of Use³³.
11. A 'sandbox' version of the NCTS is provided for training, with scenarios for those to work on the NCTS to work through to prepare them for operation in the Contact Tracing environment.
12. Examples of the surge workforce training includes compliance with the following:
 - The latest version of the script (aligned to the Salesforce system) provided and updated by the Ministry
 - Salesforce (or other Ministry directed) training video
 - Script delivery videos
 - NCTS policy statements
 - Frequently asked questions (contained in the MS team site)

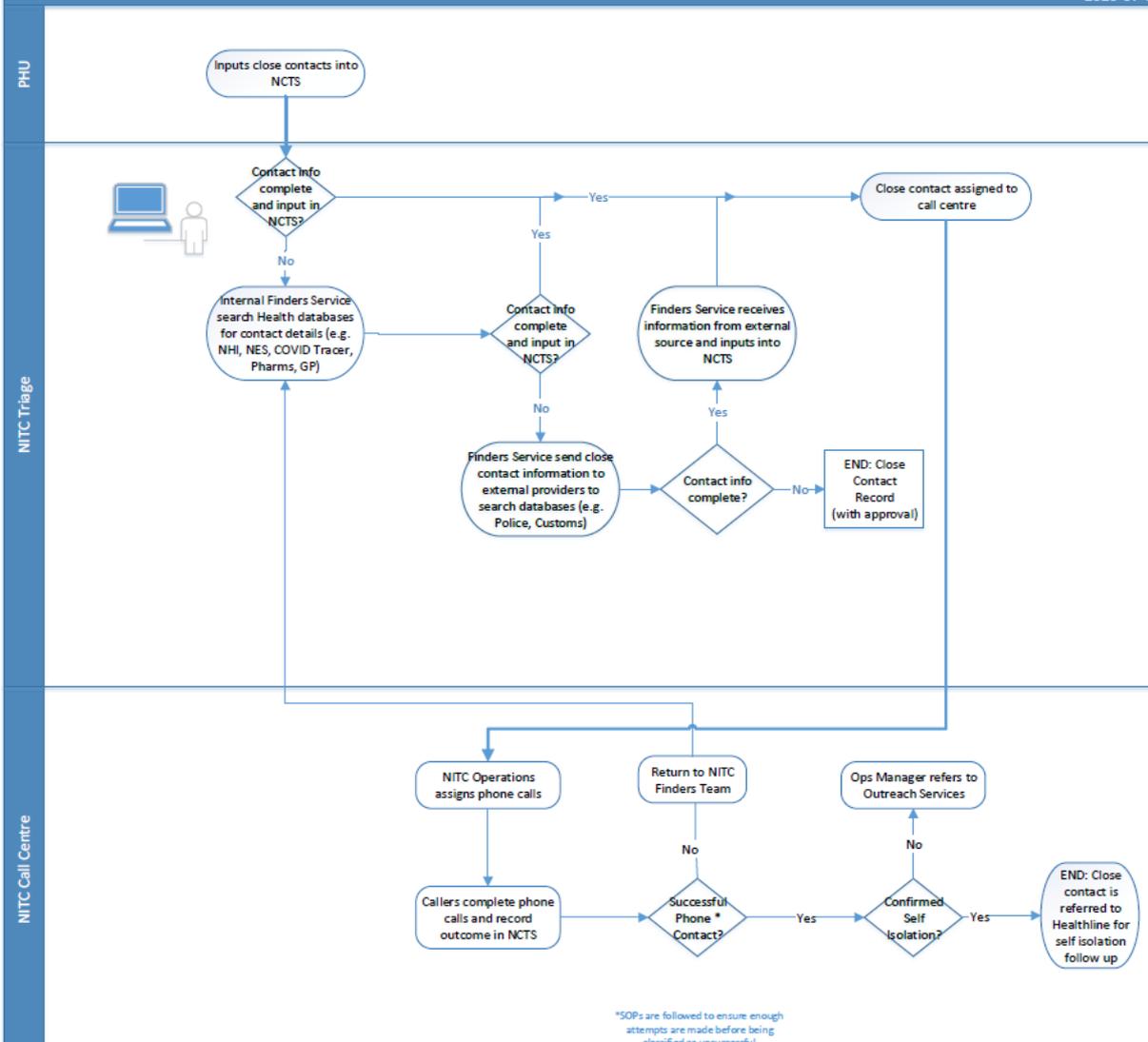
³³ As set out in Appendix Two

- Work from home guidelines, including privacy and confidentiality
- Joint training via Zoom meetings for surge workforce team leads with NITC Operations staff and shift leads
- Regular caller competency assessments

Appendix Four – the Finding Service

1. The Finding service is the specialist part of the National Investigation and Tracing Centre (NITC) that manages location of hard to find individuals involved in the COVID-19 pandemic.
2. The impact of not being able to quickly locate a Close Contact could mean a lost opportunity to deliver the information necessary to provide that individual with appropriate health advice, and to prevent the further spread of COVID-19³⁴. by assisting the individual to manage their self-isolation.
3. The Finding Service works to identify individuals where there may be limited information, and also to find contact details. It is important to obtain this information from the most up to date and reliable sources available, to enable the fastest and most efficient means of contact. Key contact details include the phone and email contacts of the individuals.
4. The NCTS forms a queue of tasks for action, and these are allocated to NITC to attempt to identify and / or locate the Close Contacts via the information available to the Ministry from other health systems or via external information sources.
5. The NITC 'triage' process for locating and contacting Close Contacts is set out in the following flow chart. The Cases will generally be delegated by a PHU Contact Tracer once they have completed Call 1 and Call 2 with the Case (refer to Appendix Two for more details) and have either identified who the Close Contacts are but need contact details, or have Close Contacts who are not yet identified:

³⁴ This will include by assisting the individual to manage their self-isolation or assisting them to move to a facility if necessary.



Finding Service

6. The Ministry has access within the secure NCTS environment to the National Health Index (NHI) and the National Enrolment Service (NES).
 - The NES contains the patient enrolment information collected from general practices. It is not the clinical record held by the practice about the patient. The NES has contact details of enrolled patients, updated at their most recent point of contact with the practice.
 - These NHI and NES services allow authorised NCTS users to identify and locate contact details for a majority of New Zealanders for Contact Tracing purposes.

- NHI is reviewed first, to uniquely identify each person (where possible) so that the relevant contact details can be located in the NES³⁵ for the individual with that NHI. The NES is the most successful source for the Finding Service to locate contact details for potential Close Contacts.
7. Not all individuals, however, can be identified sufficiently to allocate a correct NHI. Not all NES records hold current contact details.

Identity details

8. The infected person will 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.
9. In this instance, the Finding service will work to piece together the known information with other information sources to attempt to identify that potential Close Contact.

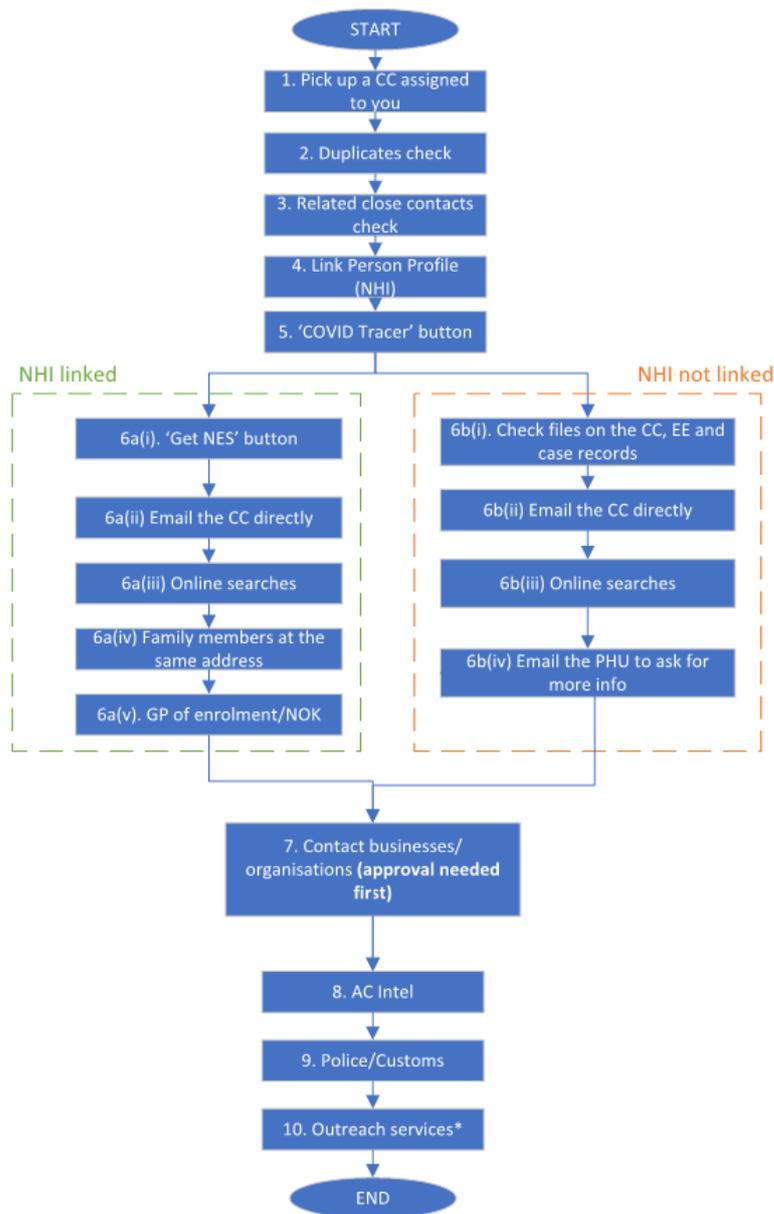
Contact details

10. Alternatively, a Case might know who an individual is, but not how to contact them. Not all practice management systems send email or phone details to the NES. Consumers may have changed their contact details since they were last updated in the NHI or NES services, they may not be residing at their usual address or they may be travelling. Other sources for contact details then must be reviewed.

Finding Processes

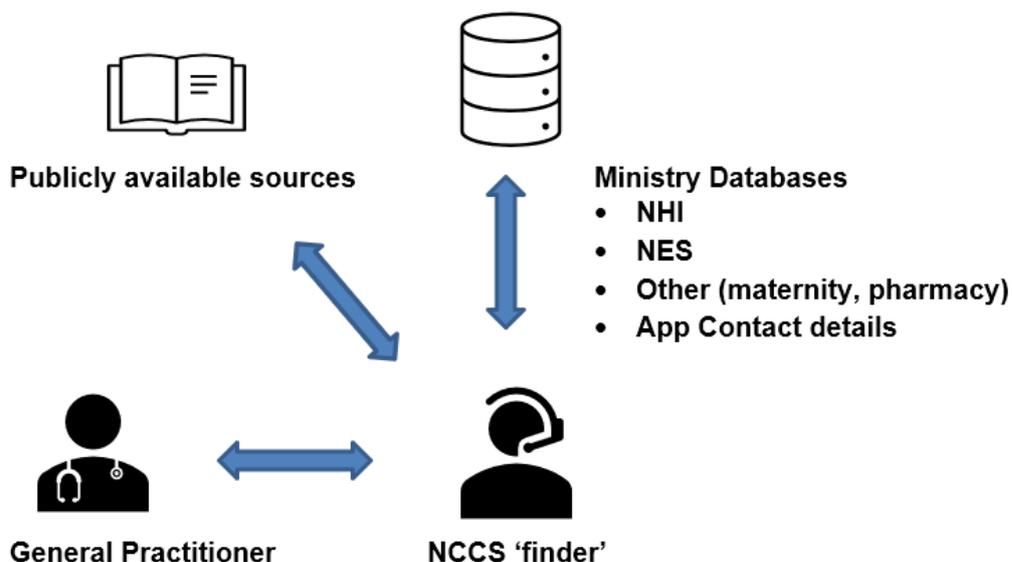
11. If the individual being sought is unable to be readily contacted (or in some cases their identity needs to be further clarified) it is not reasonably practicable in the circumstances to source the information from the individual (reference Rule 2(2)(d) of the HIPC). In addition, a requirement to collect the contact information from the individual could prejudice the interests of the individual concerned (as they may need to know promptly that they could have been exposed to COVID-19), and the safety of those who may be in Close Contact if this individual had unknowingly been infected with COVID-19.
12. The intention of the Finding process is to proceed from the least sensitive information sources, only looking further when the individual has been unable to be identified or contacted. If a person can be adequately identified to link an NHI this will enable contact points to be found within the NES. The preferred contact points are phone or email. Due to the speed required for locating people, a physical address is not as helpful, except for confirmation that the correct person has been located in the database reviewed.
13. The current Finding service process documents the general pathway followed to find contact details (for those with a linked NHI) and identity confirmation (for those without a linked NHI). All processes are supported by extensive training and reference documentation:

³⁵ The PHO enrolment process, including template enrolment forms, and Use of Health Information Statement provides that a 'purpose' for collection of a person's health information is to help 'keep you and others safe'.



14. If an NHI can be linked, an NES search may produce the necessary contact details. If no contact can be made from the available details (or there are no current details) the Finding Service will progress to look at further options.
15. If an NHI cannot initially be linked (as the identity of the individual is uncertain), the Close Contact and Exposure Event files on the NCTS are reviewed to look for any additional identification or contact details in those locations. If that is unsuccessful the Finding Services will look at other alternative information sources.
16. If there is a concern about non-compliance (for example the phone is picked up and hung up a number of times) then outreach services may be engaged to see if an alternative approach can make contact. This could include, for example, identifying a Contact Tracer with an appropriate cultural or language background who may be able to engage in an appropriate manner to encourage cooperation. In addition Pacific and Māori outreach services may also use local services to provide wrap-around services (for

example helping to organise welfare assistance or to book COVID-19 test appointments if required).



17. Information sources for contact details include:

- Review of additional Ministry databases if there is a recent health service interaction recorded for that individual which discloses a potential close contact identity or current contact details. This could include contact details from maternity and pharmacy claim payment records for example. This is considered consistent with the general purposes for which information is collected, for the 'improvement, promotion and protection³⁶' of the health of New Zealanders. This will include care and treatment of the individuals (or the care and treatment of other individuals in the case of infectious disease).
- The Contact Tracing App. This can also provide a source to check for up to date details of App registrants (either the Case themselves, or a potential Close Contact). This collection is authorised by individuals as part of the App sign up process (in accordance with the terms of the App Privacy Statement).
- General practitioners may be contacted as part of this service, if an NHI has been identified, to find up to date contact details of a Case or Close Contact (and only as a last resort obtain Next of Kin (NoK) / Emergency Contact details). General Practitioners have been found to be a useful source of additional contact phone numbers which may not have been updated on the NES, and also, for contact details for a NoK if other avenues for contact are limited. Disclosure is in reliance on the exception to Rule 11(2)(d)(i) and (ii), that the disclosure of the information is necessary to prevent or lessen a serious threat to public health or safety or the health of the individual concerned or another individual.

³⁶ Section 3 of the New Zealand Public Health and Disability Act

- Phone numbers can be changed with some frequency by some individuals. If the Ministry's internal databases do not hold a current contact phone number for a Close Contact, it may be that another person living at the same location with the same surname may be identified.
 - In this situation a call may be made by the Finding Service representative to that other person with a request made to provide the Close Contact's phone contact number.
 - The internal Finding representative training includes awareness of the obligations of s92ZZG which requires that the identity of the individual who may have transmitted COVID or created a risk of exposure is not identified (as far as is practicable).
 - In the event that individuals at the address with different names, or likely family members at a different address have an identified contact phone number and may be able to provide contact details for the Close Contact, a senior member of the internal contact tracing team will review the matter. They will determine the likely currency and accuracy of the information (to determine if it is relatively recent, and reliable), and the extent of the 'serious threat' that applies, before a call is placed to request the Close Contact's phone number be provided.

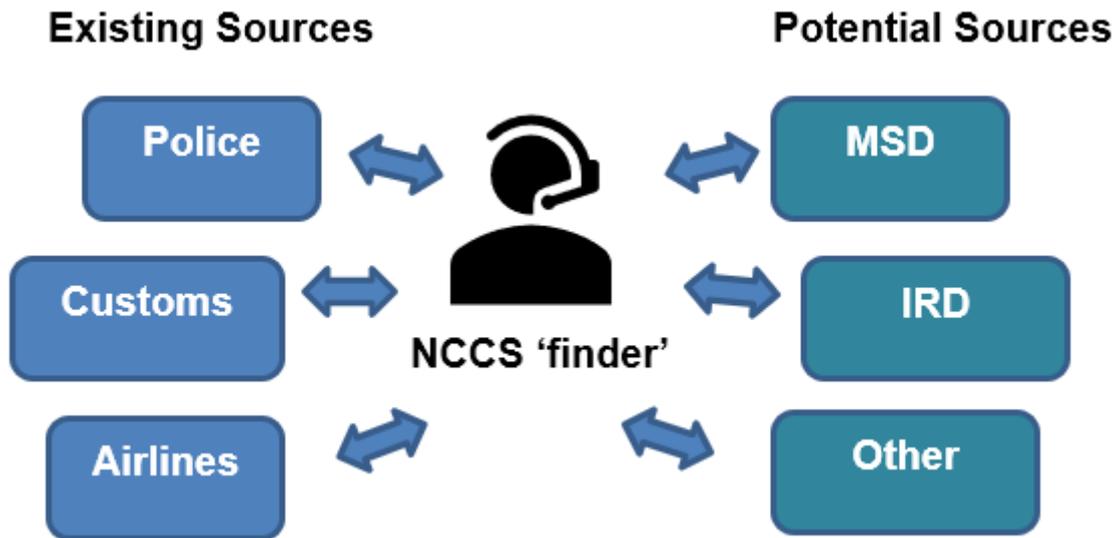
18. If there have not been sufficient details for the Finding Service to link an NHI to an individual, other methods may be required to confirm an identification.

- If an email address for a Close Contact is available an email may be sent seeking a response – and this has had some success in the recent Auckland outbreak.
- Publicly available source information has been referenced when the identity of an individual is not certain (for example only a first name and a possible employment role is known). These sources may include white pages, google search of an individual's name, workplace, or event (where known), publicly available Facebook information, LinkedIn etc.
- This additional open source information has been useful to the Finding Service to assist in providing links to support existing identification information (such as date of birth or a matching employment role to the information obtained by the Contact Tracers).
- If open source activities occur the Finding Service will follow the Ministry Standard Operating Procedures: Information Gathering and Use and use designated Ministry Facebook or LinkedIn accounts to search the publicly available settings (no 'friend' requests or equivalent will be sent to elicit a deeper access level to the source information).

19. In every instance, once the person is contacted, their details will be checked, and confirmation obtained that the individual is the person who may have been at the exposure location prior to proceeding further with the Contact Tracing process.

Finding Service – external information sources

20. In the event that the Finding Service has not located the individual in question after following the relevant processes noted above, there are a number of external sources that may be contacted.



21. External sources that have been used to date for contact information have involved requesting disclosure pursuant to Rule 11(2)(d) of the Health Information Privacy Code, as the individuals are either a Case, a potential Close Contact or a casual contact. The sources have included:

Close Contact contact details

- Police - They investigate requests about contact details for identified individuals using the NIA / TESA databases. NIA is the Master Police Database for all information held by Police on persons, vehicles, locations and police interactions. TESA is the linking Spark/Telecom database for phone numbers which includes information relating to Spark, Vodafone and some 2degrees numbers. This includes landline telephone numbers where existing.
- Customs – Requests about specific individuals are made to the New Zealand Customs Services seeking contact information or identification details if held by Customs.

Exposure Event

- An Exposure Event is any location and time that has been identified by the Contact Tracing Case investigator as a high risk for people to have been exposed to COVID-19.

Flight related Exposure Events:

- The New Zealand Customs Service has formalised an Information Disclosure Agreement under section 316 of the Customs and Excise Act with, the Ministry of Health and the New Zealand Police. Section 316 of the Customs and Excise Act 2018 specifies that the following dataset may be disclosed to the Ministry (in accordance with the Agreement). This will enable identification of all arrivals on a flight landing at the New Zealand borders:

| <i>Field</i> | <i>Data Type</i> | <i>Field also present on the Arrival Card</i> | <i>Description of Meaning</i> |
|--------------------------------------|------------------|--|---------------------------------------|
| Pax Person Surname | Text | Yes | Passenger surname |
| Pax Person Given Names | Text | Yes | Passenger given names |
| Gender | Text | No | Sex |
| Pax Person DOB | Date | Yes | Passenger date of birth |
| Pax Passport Number | Text | Yes | Passenger passport number |
| Pax Nationality Code | Text | Yes | Passenger nationality |
| Pax Type | Text | No | Passenger or Crew |
| Pax Primary Flight/Craft Name | Text | Yes | Flight name |
| Pax Flight/Craft Scheduled Date/Time | Date | No | The scheduled date and time of flight |
| Pax Flight/Craft Actual Date | Date | Same as the date of the signature on the arrival card. | The actual date and time of arrival |
| Departure Port | Text | Yes | Port of departure |
| Arrival Port | Text | No | Port of arrival |

- Customs International would be contacted if the event is an international flight, and also MFAT for chartered flights.
- Airlines (Air NZ, JetStar, Other) will be contacted for flight details in the event a Case has been on a flight to identify those who may have been seated next to the Case during the relevant time. Previously it was also important to identify contact details of travellers who had entered New Zealand and may have been travelling – currently these individuals will be located in a Managed Isolation Facility and are able to be promptly located.

All other Exposure Events:

- Other 'Exposure Events' can be any location, where there may be a risk of close contact between a Case and other in the public, such as restaurants and bars, supermarkets, gyms.
 - Depending on the Alert Level business registers may not have been kept. This has increased the importance of potential access to other sources of information, particularly to identify event attendees.
 - If the events had bookings there may still be an available list identifying attendees and contact details. If not, such as a Friday night attendance at a bar, then it can be more challenging to obtain the necessary information on any potential Close Contacts.
 - Contact can be made with relevant organisations, and if required, assistance can be compelled via section 92ZZF of the Health Act (by Contact Tracers appointed under s92ZZA of the Health Act). This can include an individual's employer, an educational institution attended by the individual, a business or organisation that the individual has dealt with or an event co-ordinator or person likely to have a list of who attended an event.
 - The organisation may be requested to look through their own information (such as CCTV footage, and bank records) to report back on who Close Contacts are. The organisations will be requested to release the findings back to the Finding Service or directly to the relevant Contact Tracer.
22. Information had been exchanged between government agencies from the outset of the pandemic under the Civil Defence National Emergencies (Information Sharing) Code 2013 and the serious threat exceptions under the Privacy Act. This Code expired in June of 2020, and can no longer be relied on to justify disclosures.
23. The Ministry is consulting with the Office of the Privacy Commissioner on appropriate sharing of information into the future.
24. In the interim, the serious threat exemption under the HIPC will be used, if necessary, in the event that there is an urgent need to identify and / or locate an individual at risk of contracting COVID-19.
25. Ongoing consideration is being given to the possibility of amendment of Part 3A subpart 5 of the Health Act. There is no current date for finalising any legislative change, nor final decision about the need for any change.
26. One important change would consider is a specific obligation to provide contact details (including phone or email contact details) in s92ZZF(1), instead of just name and address details. Address details are not as useful and would slow down the contact tracing processes if that is the only method of contact.

27. An example of where additional legislative clarity would be beneficial in s92ZZF(2) would be to specifically include both regular requests from government departments, or records from within the banking sector. Each of these organisational types, appropriately, safeguard Consumer information. They may however hold information that is of key importance in the contact tracing process that could ultimately limit the spread of COVID-19.
28. Discussions are underway with the Inland Revenue Department to address the possibility of seeking up to date contact details for identified individuals (no other information would be required for Contact Tracing purposes) under a Memorandum of Understanding. This will be addressed with the Office of the Privacy Commissioner as discussions progress.
29. The Ministry is considering an interim 'standard' type arrangement whereby it clarifies the limits that would apply to any information obtained for contact tracing purposes, including retention and destruction of information by both the NCTS and the disclosing party. This would be used to underpin any request for information under the 'serious threat' ground and also any s92ZZF request for information.
30. This is an area that will continue to be explored to ensure there are no gaps in the authorisation, and best practice is followed, to obtain information to meet contact tracing objectives.

Third party notification

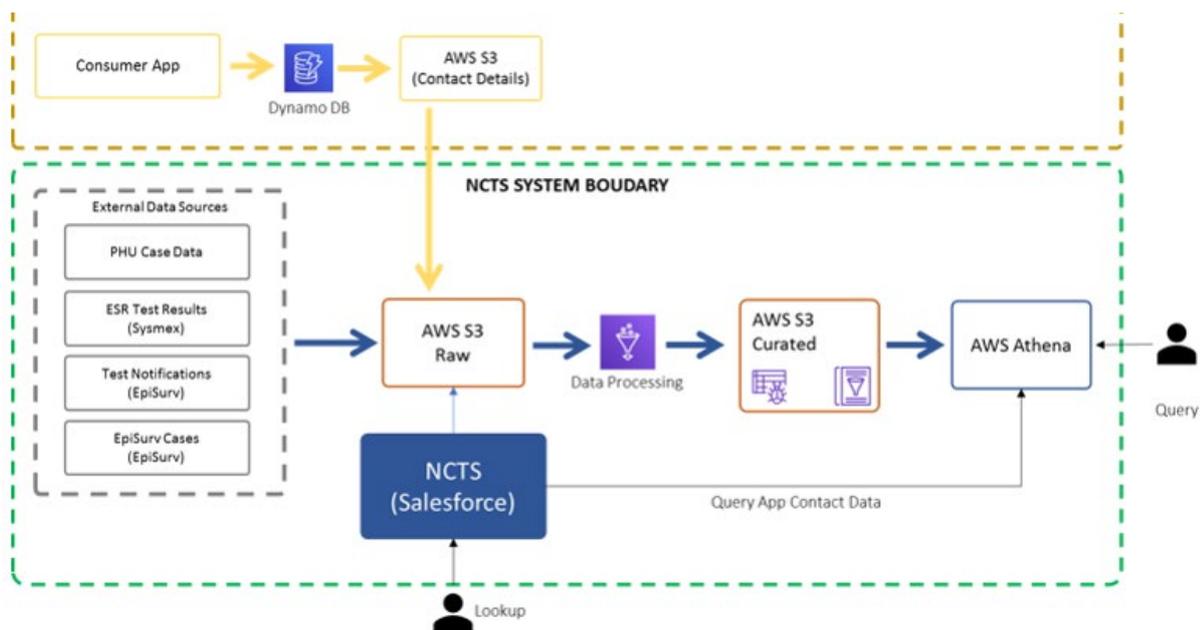
31. There are situations where notification is provided to third parties advising of a potential confirmed or suspected Case or Close Contact:
 - The Managed Isolation and Quarantine Facilities are advised, when appropriate, of potential Close Contacts of any Case, if they are resident in one of the managed facilities. This disclosure will be under the 'serious threat' exemptions under the Privacy Principles (and Health Information Privacy Code).
 - New Zealand International Focal Point is advised when a Close Contact has left New Zealand. The National Focal Point (NFP) is a function required in accordance with Article 44 (Collaboration and Assistance) of the International Health Regulations 2005 (IHR) to provide information to other countries. It acts as a formal single point of contact between countries and with the WHO to support management of all potentially serious events, such as outbreak of a communicable disease. The NZ NFP's role in the COVID-19 response is in line with the above description. The NZ NFP is the single point of contact to share (receive/send) information with other countries about suspected/confirmed COVID-19 Cases and close contacts for Public Health follow up (as deemed appropriate under each country's protocols and procedures). This information may include personal information, which is supplied in accordance with the International Health Regulations 2005 and maybe used or disclosed only for the purpose of assessing and managing a public health risk in accordance with and subject to the requirements of Article 45 of the IHR. The NFP is also used to provide official reports and updates to WHO.

Appendix Five - CCTA interactions with NCTS

1. The Ministry identified the opportunity to support national Contact Tracing processes by use of a Mobile 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).
2. The Ministry has also provided a web-interface to manage the application process for the QR Code (which will enable the generation of QR Code posters for display – to be scanned by the App).
3. There is a specific Privacy Impact Assessment that has been created to address the CCTA operations. It can be found [here](#). The Privacy Statement associated with the QR Code can be found [here](#).

Contact details

4. Consumers may choose to submit their contact details via the App to the CCTA data store to enable fast contact to be made with them by contact tracers. As at 28 September approximately 97% of people (2,008,566) had submitted both their name and phone number to the CCTA data store. 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 Close Contacts of a person with a confirmed or probable Case of COVID-19.



5. 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.
 - The access is logged into the NCTS audit records. This audit trail records which Contact Tracer used their view access to an individual Consumer's contact details.
 - The contact information is only entered into NCTS once it has been verified by the Contact Tracer 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.
6. A CCTA Consumer may request that their contact details are deleted. The NCTS can do this deletion on request, but will not be able to remove a phone number from its audit logs if a contact of that person has been made or attempted. That audit log record will not however be connected to that Consumer's name.

Digital Diary details

7. If a Consumer (who is a confirmed or probable Case) is requested by a Contact Tracer to indicate the places they have been and the people they have been in contact with, the Consumer may choose to use the CCTA's electronic release facility to upload the Digital Diary details recorded on their device to the NCTS.
 - The Consumer will have created 'Locations' by using their mobile App to scan a QR Code at a business or other location with a Ministry approved QR Code³⁷. The Location details will include the unique Global Location Number (GLN) of the Location and the time the Consumer scanned the QR Code.
 - The Consumer (from App Release 3) will also be able to record manual entries identifying places they have been, activities they have been involved in and people they have been in contact with (at their choice).
 - The Consumer's device will only contain a maximum of 60 days' worth of Digital Diary information (the App automatically deletes information older than this).
8. If the Consumer does upload the Digital Diary data, it is linked against the NCTS Case record associated with the "Data Request Code" (set when the Contact Tracer sends the invitation to upload).
 - The Consumer Digital Diary information can be accessed by the Contact Tracer through Salesforce (NCTS) which retrieves the data relating to that Case from the data store. The Contact Tracer will have provided a unique code to the Consumer prior to the upload so that they can locate that Consumer's information from the information submitted.

³⁷ QR Codes are generated via the [Ministry of Health web portal](#).

- Any Contact Tracer access to the uploaded Digital Diary records 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 Digital Diary details.
 - NCTS will retrieve business information about each scanned Location by using the GLN to query the NZBN and QR Code database, so Contact Tracers have the information necessary to continue their investigation.
 - The Contact Tracer will then discuss each Digital Diary entry in detail with the Consumer to identify who the Consumer had been in contact with, how long the Consumer was at any Location, what they did there and whether there is a risk that the Consumer was infectious when at that Location. This will enable the Contact Tracer to use their expertise and identify if it is likely that other individuals may have been exposed at that Location (an Exposure Event).
 - Where a Location is identified as an Exposure Event, an Exposure Event will be created within the NCTS. This can only apply to Locations with a GLN. This Exposure Event and the associated Contact Location will be retained as part of the NCTS Case record.
9. Information uploaded by a Consumer from their Digital Diary but not selected by the Contact Tracer as relevant from the secure S3 bucket (i.e not included on the NCTS with the relevant Consumer Case record) will be deleted on a rolling six month basis.

Exposure Event Notification

10. 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 for contacts of the positive Case (who may meet the criteria for Close Contacts), a clinical decision will be made as to whether it will benefit the Contact Tracing process to send a Notification via the App, in addition to the other methods available for identifying Close Contacts.
 - 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.
11. This would retain clinical flexibility to meet the specific Exposure Event conditions.
12. The NCTS will have a feature (a button for 'Escalate Exposure Event') to enable each Contact Tracer to indicate that an Exposure Event may have created Close Contacts and therefore be appropriate for Notification via the CCTA.
13. Only a limited number of authorised senior Contact Tracers will be able to use the interface in NCTS to create an Exposure Event of Interest (EEOI) for Notification (an EEOIN).
14. A decision by the senior clinician to create an EEOIN will enable the relevant Location information to be prepared within the NCTS for consumption by the CCTA. The clinician will also set time parameters for when it is considered that the person was at the premises (as the App only records the scan-in time, not scan-out). The NCTS will then create a Notification to be published to a register within the CCTA platform.

15. 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.
 - The clinical oversight and final decision making on sending the Notification is designed to weigh that balance in decision-making.
16. Notification of an EEOI is available to Consumers who subscribe to the alert Notifications, and who have a matching date, time and scanned Location on their device.
- Upon a successful match of an Exposure Event on a Consumer's device, the Consumer is provided with a Notification that they may have been in contact with COVID-19.
 - Appropriate resources will be included on a weblink contained in the Notification about the symptoms to look for, and what to do in the event the Consumer needs further assistance (including Healthline contact details).
 - A specific message can also be created that will appear on the Consumer phone if there is a match with a Notification sent.
 - A 'call back' option is also available to accompany Notifications considered of higher risk, which Contact Tracers may choose to activate when the Notification is sent.
17. Consumers are not compelled to respond and may decline to acknowledge the Notification. The Consumer will not be identified via the App or the NCTS, and no information about the Consumer identity will be passed to Contact Tracers.

Security and Retention on NCTS

18. Any information that originated with the CCTA processes that is entered into the NCTS will be stored in accordance with standard NCTS security and retention requirements.

Appendix Six – the Daily Check-In

1. The Daily Check-in provides a method to regularly monitor for any potential COVID-19 related health symptoms of people in certain categories where they may be, or have been, exposed to COVID-19. It will also enable those individuals to advise if they require any related assistance.

Categories of individuals who complete the Daily Check-in process

2. Different categories may have different obligations in respect of how often they must complete the Daily Check-in process.
3. The categories include:
 - A confirmed or probable Case or a Close Contact. These Consumers will generally be required to self-isolate and use the Daily Check-in for a period of approximately 14 days. This time frame will be determined in discussion with public health system representatives. This is the process addressed in this PIA. The following two 'check-in' processes will be managed within other applications and will be addressed in the relevant Privacy Impact Assessment for those applications.
 - Consumers required to reside in a Managed Isolation or Quarantine Facility. These people may be required to complete a Daily Check-in process while they remain in the facility. This is likely to be managed by the health professionals engaged in the MIQF and will be recorded in the relevant clinical system by those health professionals.
 - Border workers, who may be required to complete the Check-in process as part of their role at the border. This could be an ongoing obligation while the worker remains in that role. If this is implemented this will be in the Border Worker Testing Register Privacy Impact Assessment.

Method of completing the Daily Check-in

4. The Daily Check-in is completed by either:
 - a daily phone call to the individual (Public Health Units or Healthline are currently responsible for making these calls); or
 - by direct submission to the NCTS via a web-interface. This will be managed through an email verification process to commence the process. This option may be available to border workers or Consumers who have been identified as being suitable for this 'self-service' Daily Check-in. This daily check-in will also be supplemented with occasional direct phone calls to ensure the process is working appropriately.
5. If a person opts to complete the Daily Check-In electronically via the NCTS they will be verified with an email link.
 - For Consumers, this Daily Check-In information would be submitted directly to the Consumers record on the NCTS (they will be either a 'Case' or a potential 'Close Contact').

- All Daily Check-in survey data is encrypted in transit via http(s) between the Consumer’s browser and the NCTS Salesforce servers. There is no personally identifiable information contained within either the body of the questions or in the URL of the survey itself. The only ID information present is in the URL and relates to the NCTS ID for the relevant Consumer’s Case to create a link to that Consumers NCTS file, (or to the border workers record) against which the survey answers will be recorded.
 - The survey itself is hosted on the same infrastructure as NCTS, so there’s no transmission of information across servers. It’s a secure web page and data is saved directly into Salesforce.
 - Survey responses are not encrypted at rest, but the responses are not identifiable to the individual. However all personally identifiable, clinical and diagnostic data is encrypted in the NCTS (including all data necessary to link survey responses to the consumer).
6. A draft Privacy Statement for the Daily Check-in Process is noted in Appendix Seven, and when finalised will be incorporated into the Ministry COVID-19 website.

Information collected via Daily Check-in

7. This Daily Check-In process will follow a standard survey questionnaire which has been prepared with oversight from public health clinicians.
- Answers provided through the survey will be attached to the Consumer’s Case record in NCTS. If pathway triggers are raised the file will be referred for review by a public health official, and possible follow up phone call or other action if required.
 - If any follow up is required that cannot occur over the phone (such as a welfare check, or in-person assistance for example, if a person was sick and isolated by themselves and did not respond to the Daily Check-in email and could not be reached by phone), in this instance contact information may be disclosed to the relevant government agency only for assisting in those purposes directly related to the COVID-19 response – with a focus on potentially serious health risks.

Welcome Screen Requirements

| Survey | Welcome Screen Copy |
|-------------------------|---|
| COVID Case Follow Up | <p>Please complete the survey below – this includes your daily follow up questions to check whether you have become unwell or need any additional assistance. Please answer all questions.</p> <p>Your Public Health Unit or Healthline will be in contact if they have any queries regarding your answers.</p> <p>If you become unwell and need urgent assistance, please contact emergency services (dial 111).</p> |
| Close Contact Follow Up | <p>Please complete the survey – this includes your daily follow up questions to check whether you have become unwell or need any additional assistance. Please answer all questions.</p> <p>Your Public Health Unit or Healthline will be in contact if they have any queries regarding your answers.</p> <p>If you or a member of your household becomes unwell with COVID-like symptoms*, please promptly seek advice from a health professional and stay at home until you have received advice:</p> <ul style="list-style-type: none"> • You can contact your health care centre / doctor – do not turn up without calling first • Contact the COVID-19 Healthline on 0800 358 5453 • If you need urgent assistance, contact emergency services (111). <p>*COVID-like symptoms are a fever (feeling hot and cold), shortness of breath, cough, sore throat, runny nose and loss of sense of smell.</p> |

8. The current detail of the survey question flows is separated into two question sets. One for a confirmed or suspected COVID-19 Case, and the other for Close Contacts. The survey questions will follow the general format below – the example is for the confirmed or suspected COVID-19 Case. It is also noted this may be adjusted from time to time to match the standard phone processes being followed by the Contact Tracers:

The Q&A for the COVID Case Follow Up Survey is decomposed into three sections:

- Your Symptoms (1/3)
- Your Bubble (2/3)
- Welfare and Other Assistance (3/3)

| Your Symptoms (1/3) | | | | |
|---|---|-----------------------|---------------|--|
| Question | Answers | Format | Status | Field mapping for response - Follow Up Check-In (Task) |
| Have your symptoms changed at all? | Yes No | Radio buttons | Mandatory | NSS_Has_Symptoms__c |
| Do you have any of the following symptoms? | Yes / No for each of the following options: Fever (feeling hot and cold) Shortness of breath Cough Sore throat Runny nose Loss of sense of smell | Radio buttons | Mandatory | NSS_COVID_Symptoms__c |
| Do you have any of these other symptoms? | Yes / No for each of the following options: Headache Muscular Pain General Weakness Irritability/confusion Chest Pain Abdominal Pain Joint Pain Nausea/vomiting | Radio buttons | Mandatory | NSS_Symptoms__c |
| Please provide any further details. | - | Text box (length 255) | Non-mandatory | NSS_Symptoms_Other__c |
| Are you feeling worse than yesterday? | Yes No | Radio buttons | Mandatory | NSS_Feeling_Worse__c |
| Have you checked your temperature in the last 24 hours? | Yes Below 38 degrees Above 38 degrees No | Radio buttons | Mandatory | NSS_Temperature__c |
| Please provide any further details. | - | Text box (length 255) | Non-mandatory | NSS_Symptom_Details__c |
| Your Bubble (2/3) | | | | |
| Have you left your property in the last 24 hours? | Yes No | Radio buttons | Mandatory | NSS_Left_property_in_last_24_hours__c |

| | | | | |
|---|--|-----------------------|--|---|
| Have any people visited your house? | Yes No | Radio buttons | Mandatory | NSS_Had_Visitors__c |
| Please provide further details regarding whether you have left your property or had visitors. | - | Text box (length 255) | Conditional Mandatory IF Have you left your property in the last 24 hours? = Yes OR Have any people visited your house? = Yes | NSS_Compliance_Details__c |
| Welfare and Other Assistance (3/3) | | | | |
| Do you require any welfare assistance? | Yes No | Radio buttons | Mandatory | NSS_Welfare_Assistance_Required__c |
| What welfare assistance do you require? | Food Accommodation Financial Support Prescriptions Animal Needs Medical Needs Disability Needs | Checkboxes | Conditional Optional IF Do you require any welfare assistance = Yes, display | NSS_Welfare_Assistance_Details__c |
| Is anyone in your household feeling anxious or stressed? | Yes No | Radio buttons | Mandatory | NSS_Mental_Health_Support_Required__c |
| Is there anything else concerning you or anything else you need? | - | Text box (length 255) | Non-mandatory | NSS_Additional_Concerns_Needs__c |
| Is there anyone else that you have been supporting who will be affected by your self-isolation? | Yes No | Radio buttons | Mandatory | NSS_Impact_on_Supported_People__c |
| Please provide details about the impacted people. | - | Text box (length 255) | Non-mandatory | NSS_Impact_on_Supported_People_Details__c |

Finish Screen Requirements

| Survey | Finish Screen Copy |
|-------------------------|---|
| COVID Case Follow Up | Thank you for completing the daily survey. For further information or any questions, please visit our COVID-19 website here: https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus |
| Close Contact Follow Up | Thank you for completing the daily survey. For further information or any questions, please visit our COVID-19 website here: https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus |

Retention of information

9. This Daily Check-In information for a confirmed Case will be retained on the basis that it is a health record of the Consumer, as the Daily Check-in will ask for a daily report on symptoms (or lack thereof) that the Consumer has experienced. If a Close Contact Consumer becomes symptomatic and becomes a Case themselves, then that record will also be retained as a health record.
10. All other Daily Check-In survey results (for asymptomatic Consumers) will be deleted after six months, but a record will be retained on the NCTS that the person has participated in / completed the Daily Check-In process.

Release from self-isolation

11. For those Consumers who have been isolating in the community as potential Close Contacts, an email will be sent to them from the NCTS to confirm their release from the required isolation/ quarantine (if they have provided an email contact).
 - The email release will be authorised from a Public Health Unit or the NITC to confirm release from isolation / quarantine. This email is to enable those individuals to show others (such as schools or employers) that they are authorised for release back into the community.

- Only the first and second name of the individual will be included in the email, and it is part of the scripted calls process with each individual to carefully check all contact details, including email addresses, at the outset of the Daily Check-in process.

Privacy and Security Statement – Case and Close Contact Daily Check-in Process

All of us in New Zealand are facing the challenges of COVID-19 together.

One of the tools the Ministry of Health is using to limit the transmission of COVID-19 is the National Contact Tracing Solution (NCTS). This is a secure database managed by the Ministry of Health and is used to support Contact Tracers. It also helps monitor individuals who may have been exposed to COVID-19.

What is the Daily Check-in process?

The NCTS will be used to record the responses from people who are required to complete the Daily Check-in process. This process is to determine if they are exhibiting any possible symptoms of COVID-19.

You may be required to complete a Daily Check-in if you are a Case or a Close Contact of a confirmed or probable Case of COVID-19. You will generally be required to self-isolate and use the Daily Check-in for a period of approximately 14 days. This time frame will be determined in discussion with public health system representatives.

The Daily Check-in can be completed by responding to regular phone contact from a public health representative, who will record your responses in the NCTS. If given the choice, you may instead complete the Daily Check-in by a web interface with the NCTS.

What is the purpose of the Daily Check-in?

Personal information collected during the Daily Check-in process will only be used as part of our public health system response for the purposes of the COVID-19 pandemic response. It is a regular monitor of any potential COVID-19 related health symptoms you may experience and will enable you to advise if you require any related assistance.

What steps are we taking to protect your privacy?

We take your privacy seriously. We have engaged with the Office of the Privacy Commissioner during development of NCTS processes to ensure your personal information is managed appropriately.

A Privacy Impact Assessment (PIA) has been completed for the NCTS. You can look at the latest version [here](#).

What happens to your information?

Any information you share with the Ministry via the NCTS Daily Check-in will not be shared with other Government agencies unless they are directly involved in assisting with the public health response to COVID-19. We will contact you for additional information if your responses indicate that is necessary.

If you are requested to complete the Daily Check-in process it is mandatory that you do so. Depending on your circumstance you may be provided the option of completing the Daily Check-in through an online survey that will be sent to your email address, otherwise you will be called by a Public Health representative. The information you provide as part of the Daily Check-in process will be recorded on your Case or Close Contact record, (depending if you are being managed as a Case or a Close Contact) to support us to monitor your isolation and to support COVID-19 disease tracking and monitoring services.

Will my information be secure?

When you provide your personal information for the NCTS Daily Check-in it will be held securely in compliance with Ministry standards. Your personal information will be held and managed in accordance with the Privacy Act 1993 and Health Information Privacy Code 1994.

Strong measures are in place to protect your information from unauthorised access. Access to the NCTS is limited to only authorised users, and that access is recorded and can be audited. In order to deliver the NCTS services we use Amazon Web Services (AWS) located in Sydney, Australia.

How long will my information be kept for?

Information you provide about yourself to enable the NCTS Daily Check-in, including your name and contact details and the fact you have completed (or not completed) the Daily Check-in process, will be stored for the duration of the COVID-19 pandemic response. Then it will be deleted. If you are not symptomatic, the symptom details returned in the Daily Check-in will be deleted within six months.

Information about the health records of any positive Cases will be retained as required by the Health (Retention of Health Information) Regulations.

Other information held on the NCTS, including identification and physical address(es), will be stored for the duration of the COVID-19 pandemic response, and then deleted.

How can I view or change my information?

To view any personal information held by us about you, or if you have any concerns or questions about the personal information that we hold and wish to request a correction, please write to:

The Privacy Officer
Ministry of Health
PO Box 5013
Wellington

Email: information@health.govt.nz

We may require proof of your identity before being able to provide you with any personal information.

Who can I contact if I have a privacy concern?

If you're not satisfied with our response to any privacy-related concern you may have, you can contact the Privacy Commissioner:

Office of the Privacy Commissioner
PO Box 10-094
Wellington
New Zealand

Phone: 04 474 7590

Email: enquiries@privacy.org.nz

National Contact Tracing Solution (NCTS) Information Sheet

All of us in New Zealand are facing the challenges of COVID-19 together.

The Ministry of Health's elimination strategy is a sustained approach to 'keep it out, find it and stamp it out'. Contact tracing is a key part of this approach, and is designed to limit the transmission of COVID-19.

The National Contact Tracing Solution (the NCTS)

The Ministry of Health has developed a secure national electronic database to support Contact Tracers to keep accurate and secure records of all contact tracing activity.

What are the purposes of the NCTS?

The purpose of the NCTS is to support Contact Tracing to limit the transmission of infectious disease. The NCTS is used to record information collected about persons with, or suspected of having, COVID-19 in order to identify the source of the infection and help prevent its spread. This will enable Contact Tracers to make Close Contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary.

The NCTS is also to be used to support the effective management of infectious disease by the Ministry of Health, District Health Board Public Health Units, and the Crown Research Institute of Environmental Science Research. Effective management may include national and regional management and planning, audit of contact tracing related services, quality improvement, statistical purposes and research purposes authorised by the Director-General of Health, provided that approval by an ethics committee, if required, has been given for that research and it will not be published in a form that could reasonably be expected to identify any individual.

Who will be able to see the information on the NCTS?

Only authorised users who have been granted access credentials are able to access the NCTS, and these users will all be involved in Contact Tracing and related processes. All access by those authorised users to information on the NCTS is tracked and monitored.

How do Contact Tracers use the NCTS?

Contact Tracers are specially trained, and authorised under the Health Act, to make inquiries of those people who have tested positive for COVID-19, and advise those they may have come in contact with of any risk of infection.

The NCTS assists Contact Tracers by performing the following functions:

- **Test Results:** Recording and allocating the results of COVID-19 tests for management by Contact Tracers. This enables Contact Tracers to make contact to inform individuals in each region if they have a positive result (they are a positive Case). It is also important to address negative test results as part of the follow up, as these individuals may be Close Contracts of someone who is a positive Case.

- **Making Contact:** The NCTS assists to locate individuals by providing access to National Health Index information (the unique identifier assigned to every person who uses health and disability support services in New Zealand). This enables the correct identification of individuals, and links to the National Enrolment Service contact details so contact can be made with those identified individuals. There is also access to the contact details of those who have chosen to submit this information via the NZ COVID Tracer App.
 - For a small number of Cases where a potential Close Contact may not be readily identifiable, information may be requested from other sources to locate contact details. It is important that these individuals are identified and informed of the risk of exposure to COVID-19, so that they and their contacts can be protected
 - These other sources could include open source social media (using accounts that are registered with Ministry of Health identifiers), or other government agencies who may have relevant contact details. This will be managed by the Finding Service, who will follow standard processes designed to protect privacy.
 - No information from these sources is used for purposes other than contact tracing.
- **Recording:** The NCTS enables a single national collection point to record the Case management records for COVID-19 and all relevant Contact Tracing details. The Contact Tracers will work with positive Cases to identify what their activities have been and what locations they have visited in the period when that person may have been infectious. As the NCTS is available to Contact Tracers nationally this enables Cases that have travelled across multiple regions to be appropriately managed and also will enable Contact Tracers from other regions to assist if additional support is required due to high case loads.
 - **Exposure Events:** If Contact Tracers identify any locations where others may have been exposed to COVID-19 (an Exposure Event) this will be recorded on the NCTS. Contact Tracers will then work to identify everyone who may have involved in an Exposure Event. This could include, for example, a flight, a party at a bar, or a church service.
 - **Close Contacts:** If a Close Contact is hard to find the NCTS has a group of trained 'finders' who can make inquiries with other parties to help locate as many of these Close Contacts as possible. The Close Contacts will each then be given the relevant information to help keep themselves and others safe.
 - **Daily Check-in:** Positive Cases and potential Close Contacts may be called daily, or choose to complete a web template, to enable them to be monitored during any period of self-isolation. The details will be recorded on the NCTS.
- **Pathways:** All Cases proceed along NCTS pathways that are clinically designed to make sure all necessary steps are taken, no potential Close Contacts are overlooked, and opportunities for COVID-19 to spread unchecked are minimised.

Is the collection of information voluntary or mandatory?

The initial collection of COVID-19 test results from ESR is mandatory, as a positive Case is the point from which a Contact Tracer will commence their Contact Tracing activities to limit the transmission of COVID-19. Information such as test results, and NHI or NES contact details will be collected onto the NCTS without any direct contact with individuals.

Contact Tracers when making contact with positive Cases or Close Contacts will always seek to work with individuals to obtain information on a voluntary basis. As this information is so important however, if necessary, the Contact Tracers may use the provisions of Part 3 of

Subpart 5 of the Health Act and require individuals and other persons to provide information on a mandatory basis in accordance with the provisions of that Act.

What steps are we taking to protect your privacy?

We take your privacy seriously. We have engaged with the Office of the Privacy Commissioner during development of NCTS processes to ensure your personal information is managed appropriately. We will keep the OPC informed of any significant changes to the NCTS.

Your personal information will be held and managed in accordance with the Privacy Act 1993 and Health Information Privacy Code 1994. Any information collected onto the NCTS will be held securely in compliance with Ministry standards. Measures are in place to protect your information from unauthorised access. In order to deliver the NCTS service we use a secure Salesforce platform based on Amazon Web Services located in Sydney, Australia.

A Privacy Impact Assessment (PIA) has been completed for the NCTS. The PIA will be updated to reflect new features and functionality of the NCTS. You can look at the latest version [here](#).

How long will your information be kept for?

Information about the health records of any positive Cases will be retained as required by the Health (Retention of Health Information) Regulations.

Other information held on the NCTS, including identification and physical address(es), will be stored for the duration of the COVID-19 pandemic response, and then deleted.

Other information that is not relevant for Contact Tracing purposes will either not be recorded in NCTS or be regularly deleted (for example, the details returned in the Daily Check-in will be deleted within six months – only the record of completion of the Daily Check-in will be retained).

How can you view or change any information about you?

To view any personal information held by us about you, or if you have any concerns or questions about the personal information that we hold and wish to request a correction, please write to:

The Privacy Officer
Ministry of Health
PO Box 5013
Wellington

Email: information@health.govt.nz

We may require proof of your identity before being able to provide you with any personal information.

Who can I contact if I have a privacy concern?

If you're not satisfied with our response to any privacy-related concern you may have, you can contact the Privacy Commissioner:

Office of the Privacy Commissioner
PO Box 10-094
Wellington
New Zealand

Phone: 04 474 7590

Email: enquiries@privacy.org.nz

Appendix Eight - Glossary

The following are definitions used in this Assessment:

| Terms | Description, relationship and business rules |
|------------------------|---|
| AWS | Amazon Web Services |
| Case | A person who has tested positive or is a probable case of COVID-19 |
| Casual Contact | Any person with exposure to the Case who does not meet the criteria for a Close Contact. |
| CCTA | A supportive technology tool for the Contact Tracing processes. This includes the 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 (the CCTA). |
| Close Contact | This is any person who has been exposed to a confirmed or probable Case of COVID-19 during the Case's infectious period without appropriate personal protective equipment. The contact is more fully detailed on the Ministry website here: https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-novel-coronavirus-health-advice-general-public/contact-tracing-covid-19 |
| Confirmed Case | A Case of a person who has had a positive laboratory test for COVID-19. Case definition of COVID-19 infection can be found here . |
| Consumer | An individual in New Zealand who may be a confirmed or probable Case, an actual or potential Close Contact or a user who registers or downloads and signs up to use the NZ COVID Tracer mobile app or website |
| Contact Tracer | An individual who is authorised to fulfil the role of contact tracer in accordance with section 92ZZA of the Health Act, and includes those assisting in finding and location services from the National Investigation and Tracing Centre operated by the Ministry. All Contact Tracers are subject to an obligation of confidentiality. If working in a PHU Contact Tracers are commonly referred to as Case investigators. |
| Contact Tracing | This is the process used to find people who may have been exposed to an infectious disease, which is aligned with the provisions of the Health Act 1956 Part 3A, subpart 5. If a person is identified as a Close Contact of someone with COVID-19 they can be expected to be contacted by a Contact Tracer, generally by telephone. |

| Terms | Description, relationship and business rules |
|---------------------------------------|--|
| Data management layer | Where all data is collected, consolidated and curated into a single place within the secure NCTS environment |
| EEOI | Exposure Event of Interest |
| EEOIN | Exposure Event of Interest Notification |
| Exposure Event | A Location, and associated date and time range where there is potential for an individual Case to have contracted COVID-19 or a potential Close Contact to have been exposed to COVID-19. This will be determined by a Contact Tracer. |
| GLN | Global Location Number. |
| Healthline | The Ministry contracted national telephony service |
| Location | The GLN recorded on the Consumers mobile, which includes a date and time of scan. |
| NITC | National Investigation and Tracing Centre, the Ministry component of the Contact Tracing services |
| Notification | The App notification to Consumer mobiles which have an Exposure Event matching a Location recorded on that Consumers mobile. |
| PHU | Public Health Unit(s) operated regionally by District Health Boards |
| Privacy Notice Materials | 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 most current Privacy Impact Assessment. |
| Privacy and Security Statement | The second part of the layered privacy notice. It is linked from the Privacy Statement available to Consumers at registration. |
| Privacy Statement | The notice available to Consumers at point of registration with the CCTA. |
| Probable Case | A probable Case is one without a positive laboratory test, but which is treated like a confirmed Case based on its exposure history and clinical symptoms. A probable Case is a symptomatic Close Contact. |