Te Whatu Ora
Health New Zealand

Te Whatu Ora - Health New Zealand

Public Health Outbreak Case and Contact Information System Project

(PHOCCIS)

National Disease Management System

(NDMS)

Interim Privacy Impact Assessment

Date 26/02/2024

The Project

Business Unit:	Protection Directorate, National Public Health Service
PIA Author:	Click here to enter text.
Date PIA prepared:	26/02/2024
Last revision date: *if applicable:*	Click to enter a date.
Version number:	1.4

Review plan

Mid implementation review:	30 September 2024
End of project review:	Project completion date

Contents

Please describe the project (or change) clearly and simply.

- the purpose of the project (or change) and whether it provides a solution to an existing problem.
- what are the benefits and the expected outcomes?
- an overview of what personal information is handled by the project- what will be collected? How will it be used? Who has access to it? Etc
- whether the project utilises a third-party service provider?
- whether the project delivers a solution for a specific location/region or the whole of Te Whatu Ora?

In response to the COVID-19 pandemic Manatū Hauora created the National Contact Tracing Solution (NCTS) to provide a single national operational system to support the 12 Public Health Units and Manatū Hauora's National Investigation and Tracing Centre to manage cases and contacts. This greatly increased the capacity and reliability of case and contact management activities and enabled existing regional expertise to be shared to support the national response.

Since then, this COVID era system has been temporarily expanded to support measles outbreaks due to the significant risk that this disease poses to Aotearoa. The NCTS is being decommissioned in February 2024 to be replaced with the National Disease Management System (NDMS), although many of the features, tools and learnings from the NCTS are being redeveloped within NDMS.

This PIA covers the National Disease Management System (NDMS) and the integrations and functions of the system, which is being developed and progressively implemented between 2023 and 2025. There is a high degree of similarity of approach between the NCTS and NDMS including the Amazon Web Services (AWS) host platform and the system itself (Salesforce), and the Snowflake date warehouse. There are a number of new integrations between the NDMS and other systems eg laboratories systems, EpiSurv, Aotearoa Immunisation Register etc. Wherever possible integration points are being retained and reused. Data for Health Checks will be stored in both AWS (Health Check Questionnaire Service) and Salesforce. This data will only go to Salesforce, CPIR (for the purpose of managing communications only) and Snowflake.

The Institute of Environmental Science and Research (ESR) will provide notifiable disease test results securely into the NDMS to support the notification process and enable the case and contact management processes to be undertaken in respect of all affected individuals. The users of the NDMS include National Public Health Service (NPHS) (local, regional and national functions), ESR, contracted service providers and Manatū Hauora where required to support their National Focal Point communications with other nations, as required through New Zealand's international obligations. Core functions include:

- The NPHS has local, regional and national services within Te Whatu Ora. Members perform case and contact management functions, particularly the initial engagement with cases and contacts while conducting investigative interviews. The national office also provides a finding service for cases and contacts who cannot be located promptly.
- ESR is contracted to provide oversights of the communicable disease surveillance system and provide Manatū Hauora and Te Whatu Ora, who in turn support Te Aka Whai Ora, with specialty public health advice and surveillance.

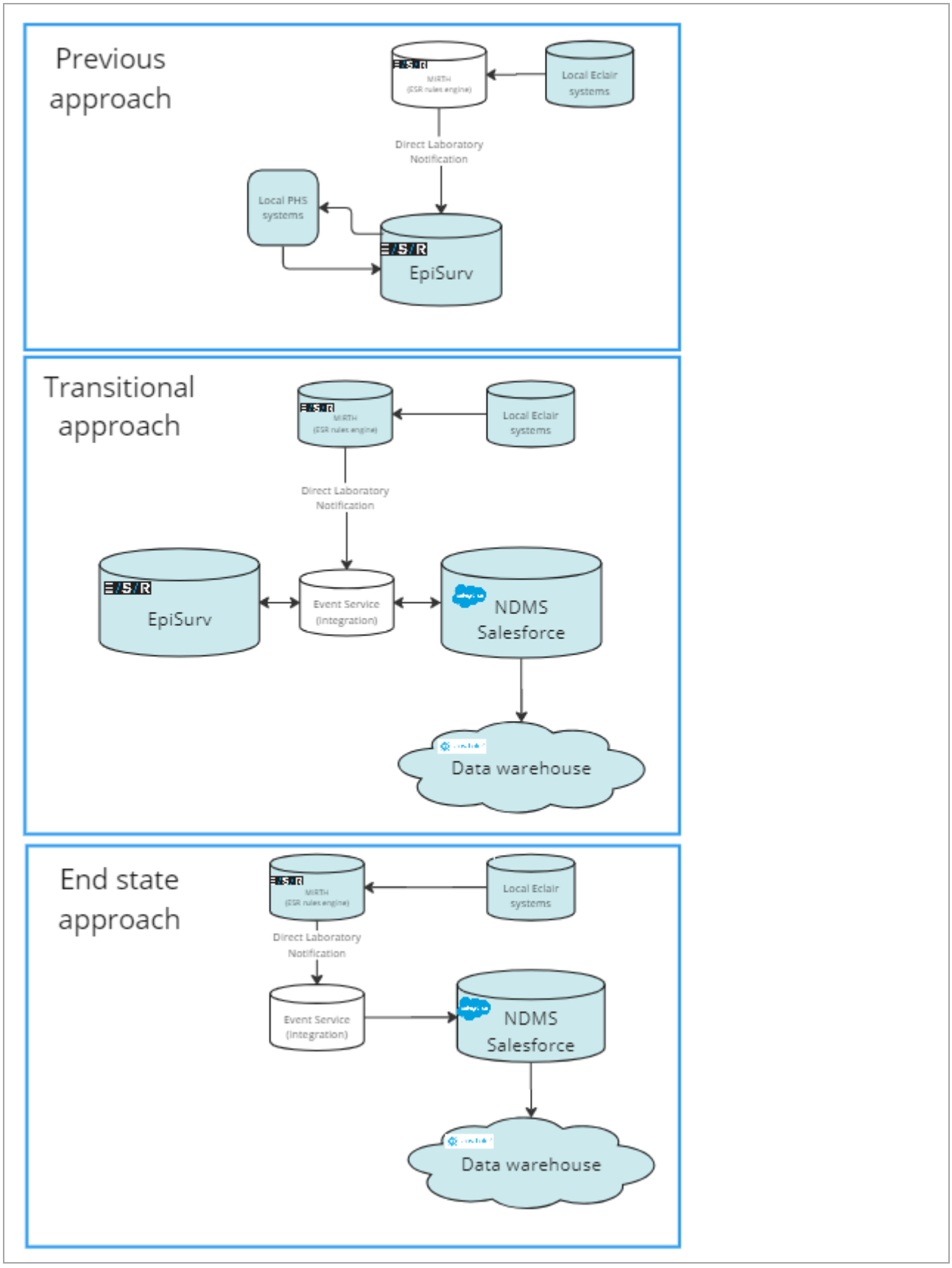
There is still work underway to evaluate exactly what information will be captured for a given disease. This may include things such as a food diary in some instances. As these decisions are made, this PIA will be updated to reflect these changes and as such it is 'interim' until the end of the project.

There is no intention to migrate any case or contact data from NCTS to NDMS. The NCTS data will be stored in a data warehouse, but this NCTS data is out of scope of this PIA. Additionally, core surveillance data from NDMS will be passed to ESR and integrated into the EpiSurv tool. This will be used for the

collection of national surveillance data as an interim measure until the NDMS project has been completed at which time surveillance data will be drawn from the Te Whatu Ora data warehouse.

Information Flow Diagram

The below diagrams show the flows of data between the core Disease Management systems.



The above diagram illustrates the different information flows for cases through the health system.

Scope of Assessment

Please define the scope of this PIA
This PIA covers the core functions and integrations of the NDMS. The initial priority diseases to be embedded within the system include Measles, COVID-19, Meningococcal disease, Pertussis, Mumps, Tuberculosis Typhoid, enteric diseases, legionellosis Hepatitis B and other disease with similar characteristics to these. The scope of the system includes all notifiable disease including more sensitive disease like sexually transmitted infections. The PIA will be expanded to cover the privacy implications for these more sensitive diseases before they are implemented within the system. These diseases are not covered within the scope of this PIA. Most of the functionality of the system has previously been assessed in the NCTS PIA so this PIA builds on that PIA.
Please describe what has been excluded from the scope of this PIA and why
The broad case and contact management process has been excluded from this PIA as it is included within the scope for the NCTS PIA which has undergone significant review and approvals.

Appendices

To finalise this PIA, you may need to provide your Privacy Officer with supplementary documents (*for example, a draft Privacy Statement, Information Sharing Agreement, Cloud Risk Assessment*). You can include these supplementary documents as **appendices** to this PIA.

If you have **added appendices** to this PIA, please list them here:

Appendices	Information
Appendix 1	Risk and Mitigation Table
Appendix 2	Glossary
Appendix 3	Q & A template
Appendix 4	Terms of Use Declaration
Appendix 5	Privacy Statements

Assessment Questions

	YES	NO

Does the project involve personal information?	☒	☐

If you're unsure what personal information is, please see the "Guide to completing a Privacy Impact Assessment". For the purpose of this question, "***involve***" includes to collect, store, use, and/or disclose personal information.

- If the answer is '**No'** then there is no need to continue with this PIA. You **must** still complete a Privacy Threshold Assessment and email this to your Privacy Officer for approval.
- If the answer is '**Yes'**, please move on to the next section (Health Information).

Does the project involve personal health information?	YES	NO
	☒	☐

The Health Information Privacy Code 2020 applies when a project handles health information. The Privacy Act 2020 applies when the project handles any personal information that is not health information. If you are unsure what personal information is, please see the "Guide to completing a Privacy Impact Assessment".

If your project does handle health information, as you work through the remaining sections in this PIA you should apply Rules 1 to 13 of the Health Information Privacy Code 2020 as they correspond to the 13 privacy principles.

Principle 1:
Lawful purpose and necessary collection of personal information

Principle 1 of the Privacy Act 2020 states that personal information **should not** be collected by any agency **unless** the information is collected for a **lawful purpose** connected with a function or activity of the agency, **and** the collection is **necessary** for that purpose.

The project should only collect the minimum amount of personal information that is necessary for the relevant function or activity ("data minimisation"). If the project **does not** require identifying information, then we **should not** collect it.

Please complete the following table:

List all information collected by the project	Source of the information	Please state why this information is needed for the purposes of this project
Test result (includes name and NHI) of a 'Case' and other test outcomes.	Community laboratory testing facilities via ESR	To comply with legislation requiring laboratories to notify scheduled diseases.
Name, clinical information and contact details of people with or suspected of having a notifiable disease.	Medical practitioners	To comply with legislation requiring medical practitioners to notify people with or suspected of having a scheduled notifiable disease.
Investigation and contact tracing of cases of notifiable disease to identify source and spread of disease. Including detailed history of case	The case or their parents/guardians or legal representative	To identify the source of the disease and/or people who may have been subsequently infected with the disease.

movements, clinical information, contacts including contact details.		
Contacts of a notifiable disease including demographic and clinical information, address and location, contact details and other information to support contact tracing.	Contacts or their parents/guardians or their legal representative	To confirm identity of contacts and associated information to support contact tracing.
Contact details of contacts if unable to be located from previous options.	External sources as further described in Appendix 4 for the finders service	To identify and / or contact the contact.
Case and contact information related to health monitoring and support for those restricted from certain activities or isolated/quarantined (either voluntary or mandatory.	From individual cases and or contacts directly Public Health Services (PHS) who are contacting cases and contacts to complete the relevant health check questionnaire (including welfare support requirements).	To monitor and support cases and contact to reduce the likelihood of onward transmission of the disease
Source of truth data held on other health data bases.	Eg National Health Identifier (NHI), National Enrolment System (NES), to support the correct identification and management of individuals, the Aotearoa Immunisation Register (AIR) to ascertain immunisation status for cases and contacts.	To support identification of the individual (NHI) and the correct allocation of resources to the individuals case management (NES, AIR)
People who have been at specific locations who may be a source of the notifiable disease, co infected, or be a contact of a case. Data includes names, contact details, or other information to enable identification of these people and or confirm their exposure.	Information held by the location including registers, booking lists, guest lists and the like.	Information to identify other people who may have had, have, or be incubating a notifiable disease.

A detailed set of questions used to collect all the necessary information is attached as Appendix 4. The fields data required for surveillance is worked through with ESR which is responsible nationally for disease surveillance. Fields are determined at a disease-by-disease level.

Please state the lawful purpose for the collection of this personal information.
NDMS will support case and contact management activities and source investigation activities for notifiable infectious diseases in accordance with the Health Act 1956. Notifiable infectious diseases are set out in Part 1, Schedule 1 of the Health Act 1956. NDMS will not be used for all infectious diseases, just notifiable infectious diseases and hazard exposures.

Part 3, subpart 71 and 74 and 74AA of the Health Act 1956 requires both health practitioners and medical laboratories to notify cases or suspected cases of notifiable infectious diseases to the medical officer of health.

Part 3 and Part 3A of the Health Act 1956 provide a range of duties and powers of the medical officers of health and other officers or practitioners. These powers are wide ranging but are heavily based on a set of principles and considerations detailed in Part 3A subpart 1.

Part 3A, subpart 5 of the Health Act 1956 empowers contact tracers to undertake contact tracing in respect of individuals with an infectious disease or suspected of having an infectious disease.

	YES	NO
Could the project use **aggregated or anonymised data** and still satisfy the project's purpose?	☐	☒
Is the project collecting **the minimum** amount of personal information required for the purpose of the project?	☒	☐

Please provide further information here if you're not using the minimum amount of personal information, or you could use aggregated or anonymised data
Click or tap here to enter text.

	YES	NO
Will the project be using cookies or other analytics?	☒	☐

Analytic tools are built into the Salesforce application, this enables contact tracers to enter data and navigate the contact tracing process. Salesforce has been successfully used as a specifically designed IT solution in a number of health applications requiring the management of personal and sensitive information. Manatū Hauora and now Te Whatu Ora has routinely used Amazon Web Services and Snowflake services to extract, store and analyse data from salesforce, and provide analysis of the data.

Analysis of contact tracing data enables a long-range view of the number of cases, contacts and exposures over time and location. This enables the clinical oversight of disease management and surveillance functions for disease control. As previously stated ESR manages national surveillance. Data is also provided to Te Whatu Ora's consumer engagement platform, the Consumer Population Identification and Registration Service (CPIR) for purposes of communicating with consumers, including analysing which consumers to communicate with (including whether a health check has been completed). CPIR has an overarching PIA which covers how it handles personal information for outreach campaigns, and the governance processes for approving use cases. Data will be passed to a Te Whatu Ora Snowflake data warehouse for analytical and business purposes. Access, governance and privacy will be reviewed as this warehouse is scoped and developed and will embed Te Whatu Ora security, data governance and privacy policies and practices.

Compliance check with Principle 1

Does the project comply with Principle 1?	YES	NO	UNSURE
The information is collected for a lawful purpose and the collection is necessary for that purpose	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 2).
- If you have answered "**No**" or "**Unsure"**, please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 1. Once completed, please move on to the next section (Principle 2).

Principle 2: Collection directly from the individual concerned

Principle 2 of the Privacy Act 2020 requires an agency to collect information **directly** from the individual concerned unless an exception applies.

	YES	NO
Are you **only** collecting personal information **directly** from the individual?	☐	☒

- If you have answered "**Yes**", please move on to the next section (Principle 3).
- If you have answered "**No**", please answer the remaining questions in this section before moving on to the next section

Please state why you're not collecting information directly from the individual.
Case and contact investigation and management including contact tracing and source investigation process required to collect information from the individual, their GP/health provider, parent or guardian and third parties to identify cases, contacts and undertake necessary investigations to mitigate risks posed by the disease. This may include restaurants, community groups etc. where a confirmed case has visited.
Please state what legislative exception applies. *The legislative exceptions can be found in Principle 2 of the Privacy Act and Rule 2 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact your Privacy Officer.*
The personal information necessary for contact tracing and source investigation is obtained under Part 3A of the Health Act (Management of Infectious Disease), subpart 5 (Contact Tracing). Information Privacy Principle 2(2)(e)(v) also applies, that information sources other than the individual may be used to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual.

Please complete the following table:

What personal information is collected from third parties?	Who is the third party?
Name, date of birth, sex and contact details (contact phone or email details if available, residential address) will be collected from the case about any contacts.	Health providers, individuals who are cases, other organisations or people in charge of private events where individuals may have visited eg funerals, tangihanga, faith-based venues, restaurants, weddings etc.

Identity and contact details of contacts of each 'Case', and exposure events (locations where contact with the case may have occurred).	Same as above.

Compliance check with Principle 2

Does the project comply with Principle 2?	YES	NO	UNSURE
Are you collecting directly from the individual concerned (or an exception applies)?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 3).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 2. Once completed, please move on to the next section (Principle 3).

Principle 3: Telling the individual what we are doing

Under Principle 3 of the Privacy Act 2020, when an agency collects personal information directly from individuals, there are certain things they **must** do **before** they collect the information or **as soon as practicable** after the information is collected. This includes making sure the individual is aware of:

(a) the **fact** that the agency is collecting personal information.
(b) the **purpose** for which the agency is collecting the information.
(c) the **intended recipients** of the information.
(d) the name and address of the agency that holds the information.
(e) the **consequences** (if any) if that individual does not provide that information.
(f) whether the collection is **mandatory** or **voluntary.**
(g) the **rights of access to, and request correction of,** the information.

There are only **limited circumstances** where we do not need to tell the individual the matters in (a) to (g) above.

	YES	NO
Will the project be telling an individual all the matters in Principle 3?	☒	☐

- If the answer is "**Yes"**, please answer the questions in part A to C below only prior to completing the Principle 3 compliance check.
- If the answer is "**No**", please answer the questions in part D below only prior to completing the Principle 3 compliance check.

A. How you're going to tell the individual

Please describe how will you tell the individual how the project will manage their information. *For example, will you have a consent form, information leaflet, privacy statement etc?*
PHS staff (and staff contracted by a PHS to perform contact tracing and case investigation) are provided with a script to use when first contacting a case or contact. This is available as part of the NDMS inform Q&As. Te Whatu Ora website has privacy statements available to explain the systems that collect, process and manage personal information and handouts of a shorter version of the privacy statement will be

provided. Please see the proposed Privacy Statements in Appendix 6. Once this PIA has been approved, then the Privacy Statements will be published. Providers are expected to use interpreters where necessary in line with organisational policies.
Where will the document be made accessible? *For example, will it be published online? Link in an email? Hard copy?*
Te Whatu Ora Website.
Please include as an **appendix** a copy of any draft document that outlines how you will manage an individual's personal information.

B. When you are going to tell the individual

Will you tell individuals before or after you have collected their information? If you're telling the individuals after you have collected their information, how long after?
Before interviews or other data is collected from individuals.

C. Mandatory or voluntary collection

Please state whether the collection of information is voluntary or mandatory?
Under Part 3A section 92D of the Health Act the approach must first seek voluntary compliance. However, compliance is mandatory and can be compelled under Part 3A section 92ZZC of the Health Act.
Please state to what extent, if any, the individual can opt out of providing some or all their information?
They cannot opt out. Under Part 3A, subpart 2 Directions section 92I(9)(a) the person must be advised that the information being asked for is for the effective management of infectious disease and must be provided.
Please state what happens if the individual does not want to disclose their information?
Should compliance be an issue, written directions may be served on an individual under section 92N and finally an urgent public health order can be made through the District Court under section 92ZA compelling disclosure.

D. Why you are not going to tell the individual

Please state why you are not telling the individual how the project will handle their personal information?
Click or tap here to enter text.
Please state what legislative exception applies? *The legislative exceptions can be found in Principle 3, Privacy Act 2020 and Rule 3, Health Information Privacy Code 2020.*
Click or tap here to enter text.

Compliance check with Principle 3

Does the project comply with Principle 3?	**YES**	**NO**	**UNSURE**

Are you telling the individual how the project will handle their personal information (either before or as soon as practicable after the information is collected) or an exception applies?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 4).
- If you have answered "**No**" or "**Unsure"**, please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 3. Once completed, please move on to the next section (Principle 4).

Principle 4: Fair and lawful collection of information

Principle 4 requires that when an agency collects information they must do so by lawful means **and** by means that, in the circumstances of the case are fair and not intrusive.

⚠ Your method of collection may be unfair if it involves threatening, coercive, or misleading behaviour. What is fair also depends on the circumstances. You **need** to take particular care when collecting information from children and young people or other vulnerable groups. It may not be fair to collect information from children in the same manner as you would from an adult.

Please describe the current proposed method of information collection *If the information is not being collected fairly or lawfully, consider how the collection method could be adapted or modified to meet this Principle 4.*
Yes, information is collected fairly, either directly from the individual or via third parties who have had contact with the individual eg event organisers, parents, guardian.
If you're collecting information from children or young people, **please state** what steps are you taking to address any power imbalance, and to obtain genuine consent for the collection (or authorisation) of their family/whānau?
Parents/guardians or their legal representatives of minors under the age of 16 will be contacted rather than the minor.
If there are any cultural considerations, how you have assessed this, and, as appropriate, with whom you have consulted about how to ensure you collect the information in a culturally appropriate way
Case investigators and contact tracers will have completed all mandatory Te Whatu Ora cultural competency training as appropriate for their role and function. For collection of information please refer to the Communicable Disease manual: https://www.tewhatuora.govt.nz/for-the-health-sector/health-sector-guidance/communicable-disease-control-manual/general-consideration/

Compliance check with Principle 4

Does the project comply with Principle 4?	**YES**	**NO**	**UNSURE**
Are you collecting information in a lawful manner and by means that are fair and not intrusive?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 5).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 4. Once completed, please move on to the next section (Principle 5).

Principle 5:
Storage and security

Principle 5 of the Privacy Act 2020 requires an agency that holds personal information to ensure that the information is protected by such **security safeguards that are reasonable** in the circumstances to take against loss, access, use, modification, disclosure, or other misuse.

A. Cloud Computing Services

	YES	NO
Does your project/solution use any cloud-based services? Cloud services are infrastructure, platforms, or software that are hosted by third-party providers and made available to users through the internet.	☒	☐

Please provide a brief explanation:
The NDMS is made up of several components, including:

- Integration and Amazon Web Service (AWS) capability, and
- Salesforce Health 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 NDMS, Health Connect provides additional configuration.

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

Amazon Web Service (AWS) and Salesforce are applications used by Te Whatu Ora that have undergone assessment from a security and privacy perspective. They are deemed to be appropriate IT services for managing personal health information.

B. Engaging with Information Security

	YES	NO
Have you engaged your relevant information security team for this project/solution?	☒	☐
Has a Security Risk Assessment (SRA) been completed by your relevant information security team?	☐	☒
Has a Cloud Service Provider Due Diligence Questionnaire been completed by your relevant information security team?	☐	☒

Please provide a further information:

A security assessment is underway by the Te Whatu Ora security team. A design review was completed and remediations have been identified, which are currently being implemented. The assessment has now progressed to the Control Assessment. A third-party configuration review was not required but it is instead being completed by the Te Whatu Ora security team.

At the time this Privacy Impact Assessment is being submitted to HNZ Privacy for approval, an Authority to Operate has not been approved for this Project.

Consequently, the Project seeks conditional approval of this PIA from the HNZ Privacy.

Once the ATO has been approved:

- The Project will inform HNZ Privacy

- Any key risks and impacts from the ATO impacting Privacy will be included in this PIA and this PIA will be resubmitted to HNZ Privacy for approval as required.

Once the remediations identified by the design review are in place, the team will commence a full security risk assessment for the NDMS and an Authority to Operate will follow.

Salesforce and Amazon Web Services are in use in the Te Whatu Ora digital ecosystem. The NDMS system shares the same Salesforce Org as the Aotearoa Immunisation System, which has been in production since 2023. The Amazon Web Service digital capability is also shared and used by other areas within Te Whatu Ora to enable to sharing and The Amazon Web Services digital capability is also shared and used by other areas within Te Whatu Ora to enable sharing and storage of data.

Please contact your information security team for more information and support. Note that an SRA/ Cloud Service Provider Due Diligence Questionnaire may be completed concurrently with the PIA.

C. Storage

Please describe the system and location where the information is stored?
See above (section 5A)

D. Access

Please state the roles that will have access to the personal information.
A record is maintained of all authorised persons who have access. All staff with access are aware of and have agreements on confidentiality as part of their employment. There are four categories of users: • those undertaking contact tracing, • staff providing clinical guidance or management of the infectious disease, • analysts with surveillance responsibilities and • system administrators and managers. Any person or group seeking access for research purposes will be required to undergo a thorough application process which will include an assessment of the research value and cover data security and confidentiality requirements. Access to records will not be limited via region as people may move around throughout the duration of their illness.
Please describe why these roles need access to the personal information.
All users will have access to all of diseases, except where a disease requires individual control where it is deemed they are more sensitive. The PIA will be updated as these role-based controls are updated.

User role	Example	Purpose
Internal (Edit user)	Clinical Adviser (eg Group Manager, Medical Officer of Health)	Coordinate National Outbreak Response Conduct Response Management and Coordination for inter-regional outbreak Cluster Management Oversee Case Management

Internal (Edit user)	Regional Public Health Services Officer/ Lead (eg Public Health Nurse, Health Protection Officer, Communicable Disease Nurse, Contact Tracers, Case Investigators)	Case Investigation and management Contract tracing Build Reports Create List views
Internal (Read only user)	Support analysts	

As more diseases are brought online to the NDMS, some may be deemed more sensitive (i.e., sexually transmitted diseases) and access to these will be tightly controlled via the role base access to the system.

Please describe how access will be controlled or monitored?

- Explain the process for granting user access and removing user access (including if someone leaves or changes roles)
- Describe access controls (for example, role-based access)

All users are required to electronically confirm terms of use prior to being granted access to the NDMS for the first time, and again on each password change (compulsory every three months). A copy of the terms of use are attached as Appendix 4. Users who have either left the organisation or been inactive in the system for a period of time (currently 1 month but this will be reviewed) will have their access removed from the system)

Salesforce also has audit functions (capturing systems access, record views and data changes) available which means inappropriate access can be monitored. This audit information will be retained within the Te Whatu Ora for 2 years unless specified in policies elsewhere.

An audit process will be put in place that will review user access for system administrators and other high-profile cases (as determined by the business – for example public figures of interest).

Will access be controlled **by at least two-factor authentication**? The Office of the Privacy Commissioner has said that agencies may be in breach of the Privacy Act 2020 if they do not use at least two factor-authentication where applicable.	**YES**	**NO**	**INA**
Salesforce operates two factor authentication systems which has been incorporated into the NDMS	☒	☐	☐

E. Auditing Accounts

Please state:

- if, and to what *extent*, the project can *audit* user access to the personal information
- what will be audited, who will con duct the audit, how regularly the audit will occur etc.

The identity of members of staff who have accessed an individual's information is personal information about that individual. This means this is something that individuals are entitled to request under the Privacy Act 2020.

Optional security and privacy components have been included as part of the design of the NDMS, including the Salesforce Shield7 technology which provides enhanced \audit logging capability to provide better protection of, and tracking of access to, confidential information held in the solution. Implementation of proactive monitoring of record views for high profile individuals will be implemented shortly after the system goes live, see Control Table. The definition of high-profile individuals are those people who have

had a notifiable disease and this information has been made public. This will be extended to align with the development of the national Te Whatu Ora a clinical system audit policy.

F. Any other Information

Please state any other steps the project has taken/will take to prevent loss, misuse, unauthorised access, modification, or disclosure of personal information.

For example:

- *Is information encrypted at rest and in transit? What other relevant safeguards are utilised during the transit of information?*
- *Is there a need for additional privacy training, new policies, processes, or contracts?*
- *How will you keep physical copies of documents secure?*
- *How will you ensure conversations are not overheard?*
- *What checks will be done to ensure you're talking to, and sharing information with, the right person?*
- *What are the security classifications and any endorsements the information will have (for example, IN-CONFIDENCE, MEDICAL IN-CONFIDENCE etc)*
- *What backup processes is the project putting in place? Do they include backups of metadata (for example, audit logs)? Where are backups stored?*

With any network connected and complex system such as the NDMS 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.

The intended mitigation strategies rely heavily on the design and underlying platforms of the NDMS, specifically to incorporate the necessary security measures to provide protection and mitigate damage from such intrusion. This includes, for example:

- 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:
    - 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 NDMS will be encrypted while at rest 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). Te Whatu Ora has balanced its risk with the contracted provider for the Te Whatu Ora holding the AWS encryption keys on behalf of the Te Whatu Ora. Salesforce holds the encryption keys for Salesforce.

Operational Security – Users

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:

- 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:
    - require Users (or their contracted managers) to confirm / sign terms of use declaration;
    - provide basic training to Users; and
    - the timely offboarding of users no longer working on NDMS
- 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:
    - system controls implemented within NDMS with access and event tracking.
    - use of audit logs and review processes (with consequences for non-compliance) to discourage non-compliant behaviour.
    - 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 Te Whatu Ora.
    - monitoring Users requirements to confirm Terms of Use as part of the access credential process, prior to being able to access the NDMS. This recommendation has been implemented and standard Terms of Use (as set out in Appendix 4) are now a standard confirmation screen as part of the access credential sign up process; and
    - Oversee provision of appropriate training to Users (both system specific and general privacy requirements (with updates as required when new functionality or new issues arise).
    - Information to be held offshore.

A jurisdictional review was completed for the National Screening Solution. The NDMS relies on its similar architecture to proceed with the NDMS on the basis that the jurisdictional review is effectively identical. The AWS hosting (storage and transmission) components of the NDMS AWS services will be implemented using dedicated Te Whatu Ora Accounts and use a Virtual Private Cloud (VPC) in the prescribed Sydney Region (ap-southeast 2) – with the VPC creating a '*private isolated section of the AWS Cloud where the customer can launch AWS resources in a virtual network that the customer defines*'[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).

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 '*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…'*. Te Whatu Ora and Manatū Hauora are satisfied that the decision to host the NDMS on the same platform as the Aotearoa Immunisation Register (AIR) is an appropriate choice and provides the necessary security.

Compliance check with Principle 5

Does the project comply with Principle 5?	YES	NO	UNSURE
When the project holds personal information, is it using security safeguards that are reasonable to protect against loss, access, use, modification, disclosure, or other misuse?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 6).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 5. Once completed, please move on to the next section (Principle 6).

Principle 6: Access to personal information

Under **Principle 6** of the Privacy Act 2020 an individual has the right to confirm **if an agency holds personal information** about them, **and** if it exists, to have **access** to that information.

Access to personal information includes the right to ask who has accessed it (i.e., information from audit logs). If an individual is given access to their information, the individual must be advised that they may request correction of their information.

Please outline how individuals will be able to access their information. *For example, will it be through existing information request processes (for example, requests for clinical records), or will a new process need to be put in place?*
Individuals can access their information through application to Te Whatu Ora, as detailed in appendix Five which contains information on the process and will be available on the Te Whatu Ora website, as a handout for service providers and within this PIA. Corrections can also be made through this process.
Please outline how you intend to ensure that it is possible to find the information about a specific individual?
Users will have the ability to retrieve and amend information relating to an individual if requested, in line with standard business processes and procedures, see appendix four.

Compliance with Principle 6

Does the project comply with Principle 6?	YES	NO	UNSURE
Is there a process in place to ensure an individual can ask Te Whatu Ora if it holds personal information about them and the individual can access that information?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 7).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 6. Once completed, please move on to the next section (Principle 7).

Principle 7: Request to ask for correction of information

Under **Principle 7** of the Privacy Act 2020, where an agency holds information, the individual concerned is entitled to request correction of the information.

Please describe how an individual can ask to have their information corrected? *For example, will it be through existing processes, or will a new process need to be put in place?*

Individuals can access their information through application to Te Whatu Ora, as detailed in appendix five. Corrections can also be made through this process.
Please outline how you intend to ensure that it is possible to find the information about a specific individual and to correct it (or add a statement of correction) if required?
Users will have the ability to retrieve and amend information relating to an individual if requested, in line with standard business processes and procedures.
Please outline how a statement of correction provided by that individual will be managed so that it is always able to be viewed together with the disputed information. *For example, does your proposed system have the capacity to link or attach a statement of correction to a person's file?*
If the information cannot be updated in the NDMS, a note will be added to the file in NDMS and attached to the information. If the source is from outside the NDMS then the relevant team(s) will also be notified to update their information.

Compliance check with Principle 7

Does the project comply with Principle 7?	YES	NO	UNSURE
Is there a process in place to enable an individual to request the correction of their personal information?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 8).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 7. Once completed, please move on to the next section (Principle 8).

Principle 8:
Accuracy of personal information before it is used or disclosed

Principle 8 of the Privacy Act 2020 states that an agency must not use or disclose information without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

If you're not collecting information directly from the individual, or are relying on old records, (as examples) there is a risk that the information will not be accurate or up to date. Carefully consider the consequences for individuals if the personal information is not accurate or up to date.

How will you ensure that only **accurate, up to date, complete and relevant** information is acted on?
Data collection processes are robust. Data is sourced wherever possible from the case or contact, or their parents or guardians, various tools are available to ensure that information is accurately captured such as self-completion forms or in-built Q & As. When a person is contacted, their contact details will be confirmed and updated where needed. NDMS uses other health systems that are considered a 'source of truth' for certain data e.g., the National Health Index (NHI) and these are imported directly and ensure that information is accurate and up to date.

Compliance check with Principle 8

Does the project comply with Principle 8?	YES	NO	UNSURE
Does the project ensure that information is accurate, up to date, complete and relevant before the information is used?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 9).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 8. Once completed, please move on to the next section (Principle 9).

Principle 9: Do not keep information longer than necessary

Principle 9 of the Privacy Act 2020 states that an agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

⚠ Principle 9 (*and rule 9 of the Health Information Privacy Code)* does not apply in a vacuum. There may be other rules and regulations that will specify how long certain information must be kept for (*for example, Public Records Act 2005)*. Once those other legislative requirements for retention have been met, then under Principle 9 (*or Rule 9)* the information should be disposed of when it is no longer needed for the project. We strongly recommend you engage your Records Manager to ensure records are managed consistently with the relevant general/functional disposal authority.

Please state how long the information will be held by Te Whatu Ora
The information will be retained in accordance with the Health (Retention of Health Information) Regulations 1996, which requires that information is kept for at least 10 years since the last interaction unless the information is transferred to a new provider. Where health information doesn't form part of a person's health record and it is not required to be held for other legitimate reasons eg specific requirements under legislation, it should be destroyed once there is no longer a lawful purpose for retaining it. See Risk and Mitigation table and associated Control table for further actions to clarify and detail scope and requirements.
Please **state** the applicable legal requirements for retention of information (if any). *For example, Health (Retention of Health Information) Regulations 1996, Public Records Act 2005, General Disposal Authority 6, Functional Disposal Authority 1.*
Health (Retention of Health Information) Regulations 1996 and ISO15189 Data Retention Requirements
Please state: • whether all the personal information needs to be retained by the project • whether the information needs to be retained in a form that identifies the individual (*can it be retained in a de-identified manner)*
The information will be retained in accordance with the Health (Retention of Health Information) Regulations 1996, which requires that information is kept for at least 10 years since the last interaction unless the information is transferred to a new provider. Where health information doesn't form part of a person's health record and it is not required to be held for other legitimate reasons eg specific requirements under legislation, it should be destroyed once there is no longer a lawful purpose for retaining it. See Risk and Mitigation table and associated Control table for further actions to clarify and detail scope and requirements.
Please state: • how the information will be disposed of

• who is responsible for ensuring disposal occurs
Disposal will occur in line with current practices. More detail is set out in Appendix 7

Note: We also recommend:

1. **prior** to disposing of any the information, that you engage your Records Manager,
2. subject to the advice of your Records Manager, you keep a list of what has been disposed of and under what general/functional disposal authority.

Compliance check with Principle 9

Does the project comply with Principle 9?	YES	NO	UNSURE
Subject to satisfying any records management requirements, personal information is only retained for as long as it is required for the purposes of the project	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 10).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 9. Once completed, please move on to the next section (Principle 10).

Principle 10: Limits on use of personal information

Principle 10 of the Privacy Act 2020 requires that an agency which obtains personal information for one purpose **must not** use the information for any other purpose **unless** the agency believes on reasonable grounds that an exception applies.

The Office of the Privacy Commissioner recommends keeping in mind the "no surprises test"- would the way in which you're planning to use the personal information come as a surprise to the person you collected it from?

Please describe how the information will be used in this project?

For example, if we are using information to assess an individual's eligibility to deliver a service, outline what information is being used for assessing the eligibility and what is required to deliver the service.

The information is to be collected for the following purposes, limited to uses associated with a notifiable infectious disease case. Such uses will include:

- Management of the infectious disease in accordance with Part 3A of the Health Act. This will include national and regional management and planning.
- 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 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)).
- Reporting and analysis to support these management objectives in line with standard data access protocols.

- Research purposes as authorised by Manatū Hauora and Te Whatu Ora in line with standard research approval processes.
- Auditing activities on the NDMS system and contact tracing related services.
- Quality improvements to the NDMS system.
- Statistical analysis.

	YES	NO
Are the uses listed above consistent with the purposes of collection you have outlined in Principle 1?	☒	☐
If the answer is "**No**", **please state** what legislative exception applies. *The legislative exceptions can be found in Principle 10 of the Privacy Act or Rule 10 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact your Privacy Officer.*		
Click or tap here to enter text.		

	YES	NO
Does the use of information by the project involve information matching or sharing?	☒	☐
If the answer is "**yes**", please provide more information here. *Please consider any additional issues that may arise (for example, the need for agreements to enable and regulate matching and sharing).* Please annex any relevant documents to this PIA.		
Yes, it will integrate with National Health Index (NHI), National Enrolment Service (NES), COVID Clinical Care Module (CCCM), Consumer Population Identification and Registration Service (CPIR) and EpiSurv using existing integration plus some modifications to enhance the quality of data e.g., E-sam geocoding for addresses. This data integration and sharing brings together already existing health data sources that facilitates NDMS users expedite public health actions to prevent the spread of infectious disease, enabling effective case and contact management and public health surveillance. COVID Case Data will be shared with COVID Care in the Community users (using CCCM) for the purpose as articulated in the "Care in the Community (CitC) – COVID Clinical Care Module (CCCM)" PIA, replacing the existing interface from NCTS. Probable COVID cases identified in CCCM will be sent to NDMS replacing the existing interface from NCTS. ~~E~~ESR is a contracted provider, managing public health surveillance of notifiable infectious diseases via EpiSurv on behalf of the Ministry of Health and Te Whatu Ora. EpiSurv data will eventually be replaced by NDMS data when fully implemented.		

Compliance check with Principle 10

Does the project comply with Principle 10?	**YES**	**NO**	**UNSURE**
Will the personal information only be used for the purpose it was obtained for or does an exception applies?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 11).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 10. Once completed, please move on to the next section (Principle 11).

Principle 11:
Limits on disclosure of personal information

Principle 11 of the Privacy Act 2020 states that an agency must not disclose the information unless the agency believes on reasonable grounds that an exception applies.

The Office of the Privacy Commissioner recommends keeping in mind the "no surprises test"- would the way in which you're planning to disclose the personal information come as a surprise to the person you collected it from? Please note that **principle 11 does not limit** storing personal information in "the cloud" or sharing information with a service provider that stores or processes information on our behalf.

	YES	NO
Will the project disclose personal information to individuals or agencies outside of Te Whatu Ora?	☒	☐

- If you have answered "**No**", please move on to the next section (Principle 12).
- If you have answered "**Yes"**, please answer the following questions before moving to the next section.

Please state the basis for disclosing personal information

The grounds can be found in Principle 11 of the Privacy Act or Rule 11 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact your Privacy Officer.

Information may be disclosed to a range of agencies where the agency is:

- Carrying out work on behalf of Te Whatu Ora for individual health, public health or public safety purposes (ref Information Privacy Principal 11(1)f/ HIPC 11(2)(d));
- Carrying out work that is covered by one of the purposes for information to be collected (e.g., research) (ref Information Privacy Principal 11(1)h/ HIPC 11(1)(C));
- Carrying out research using the information (usually provided in a non-identifiable way) (ref Information Privacy Principal 11(1)h)/ Rule 11(2)(c)(iii) and subject to any relevant ethical committee approvals being obtained).
- NZ Police, to enforce compliance with the mandatory requirements to provide information under Part 3A section 92ZZC of the Health Act. Disclosure is allowed under IPP11(1)(e)(i) to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences. Written directions may be served on an individual under section 92N of the Health Act 1956 and finally an urgent public health order can be made through the District Court under section 92ZA compelling disclosure.

If there is a disclosure to someone **other than the individual concerned, please:**

- list all parties that you will disclose the information to,
- explain why those third parties need the information, and
- outline what safeguards will be put in place to ensure that the information is secure once it has been shared with the third party.

Access to NDMS for users outside of Te Whatu Ora is strictly controlled. This would be based on a clear business need and the decision to grant an users access outside of Te Whatu Ora be managed by an appropriately delegated manager in Te Whatu Ora. The external users of NDMS currently include:

- Manatū Hauora will require access to the front-end system for the purposes of National Focal Point reporting to other sovereign nations in accordance with international agreements, use

access will be restricted to the minimum number of people to enable Manatū Hauora to operate this 7 day a week service.

- ESR will also require access to the front-end of the system to support their active surveillance and outbreak detections purposes as well as critical quality control and system integrity functions ie to ensure the data integrations are operating correctly.
- Other agencies that have been contracted to undertake work on behalf of Te Whatu Ora, for example Reach Aotearoa who have been contacted to provide support with contract tracing services. In these instances, there is to be clear service specifications managed through contracts and service agreements with at least the same level of user approvals training and declarations as other users.

Note: All users who have access to NDMS will have:

- Completed privacy training, in line with current Te Whatu Ora standards,
- Been approved by one of the NDMS user approvers (specific people within the National Public Health Service authorised to approve system access), and
- Agreed to the Terms of Use declaration.

Access to the data warehouse analytics layers (not the live system) is governed through the Te Whatu Ora data governance group who have established processes for assessing use and levels of access required. Included within the remit of the Te Whatu Ora data governance group is alignment with the principle of Māori data governance and sovereignty.

Compliance with Principle 11

Does the project comply with Principle 11?	YES	NO	UNSURE
Personal information is not disclosed to an individual or agency outside of Te Whatu Ora or an exception applies	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 12).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 11. Once completed, please move on to the next section (Principle 12).

Principle 12: Disclosure of information outside of New Zealand

Principle 12 of the Privacy Act provides that an agency may only disclose personal information to a foreign person or entity (B), if:

- The individual authorises it in situations where B may not be able to protect the information to the same degree as a New Zealand entity would; or
- B carries on business in New Zealand and is therefore subject to the Privacy Act 2020; or
- B's privacy laws offer comparable safeguards to the New Zealand Privacy Act 2020; or
- B is bound by contract or agreement to protect the information with similar safeguards to New Zealand standards.

⚠ Please note that **principle 12 does not limit** storing personal information in "the cloud" or sharing information with a service provider that stores or processes information on our behalf

	YES	NO
Will Te Whatu Ora disclose personal information to a foreign person or entity?	☐	☒

- If you have answered "**No**", please move on to the next section (Principle 13).
- If you have answered "**Yes"**, please answer the following questions before moving to the next section.

Please state: • The foreign entities or persons that we will be disclosing personal information to. • Where the foreign entities or persons are based (i.e., which jurisdiction). • Why the foreign entity or person needs to have the personal information. • What evidence you have that the foreign entity receiving information has the same safeguards available to protect the information as are provided under the Privacy Act 2020.   ○ If the foreign entity cannot provide the same safeguards, indicate whether that has been explained to the individual, what has been explained and whether the individual consents to the sharing of their information with the foreign entity. Please provide evidence of that consent. • Provide details on what safeguards have been put in place to protect the individual's information (such as a contract or an agreement with the foreign entity). • Has an ethics or research committee, such as Health and Disability Ethics Committee, approved overseas disclosure?
Te Whatu Ora does not disclose information offshore, but Manatū Hauora may • disclose de-identified death and notifiable disease data to the World Health Organisation in compliance with the International Health Regulations, and • identifying information for the purposes of National Focal Point reporting to other sovereign nations in accordance with international agreements.

Compliance check with Principle 12

Does the project comply with Principle 12?	YES	NO	UNSURE
Personal information is not disclosed outside of New Zealand, or it is authorised under Principle 12	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Principle 13).
- If you have answered "**No**" or "**Unsure**", please complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 12. Once completed, please move on to the next section (Principle 13).

Principle 13: Creation or use of unique identifiers

Principle 13 of the Privacy Act 2020 says an agency may only **assign** a unique identifier to an individual if that identifier is necessary to enable the agency to carry out one or more of its functions effectively.

To avoid doubt, Te Whatu Ora does not assign unique identifiers when it records, and uses a unique identifier so that we can communicate with another agency about the individual.

Please see "Guide to completing a Privacy Impact Assessment" for more information on unique identifiers.

	YES	NO
Will the project **assign** unique identifiers?	☐	☒

Will the project **use** unique identifiers?	☒	☐

- If you have answered "**No**" to these questions, please move on to the next section (Principle 13).
- If you have answered "**Yes"** to any one of these questions, please answer the following questions before moving to the next section.

Please explain:

- What unique identifiers will be assigned or used for this project?
- How will the unique identifiers be created?
- If you are proposing to use NHIs, can the project's purpose be achieved by using an alternative unique identifier?
- Are you intending to use a unique identifier that has been assigned by another agency? *If so, please consult your Privacy Officer.*

NDMS will integrate with NHI, NES, EpiSurv using existing integration plus some modification to enhance the quality of data.

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 National Investigation Centre (NIC) will progress to look at further options.

If an NHI cannot initially be linked (as the identity of the individual is uncertain), the existing records on the NDMS are reviewed to look for any additional identification or contact details in those locations. If that is unsuccessful, staff will look at other alternative information sources. This process is covered in the NCTS PIA.

In addition to using the NHI, the NDMS will assign record numbers to each case and/or contact. These are system generated numbers, which will only be used within the systems at Te Whatu Ora. The Salesforce Profile ID within the Case Salesforce Record is used in the backend and is a unique identifier of each profile within the Salesforce system. While this could be understood to be a unique identifier of an individual, it is more literally an identifier of a file and serves a purely technical purpose.

Compliance check with Principle 13

Does the project comply with Principle 13?	**YES**	**NO**	**UNSURE**
Will the project be using or assigning unique identifiers?	☒	☐	☐

- If you have answered "**Yes"**, please move on to the next section (Review and sign off).
- If you have answered "**No**" or "**Unsure**", complete the Risk and Mitigation Table (Appendix 1) in respect of this Principle 13. Once completed, please move on to the next section, Artificial Intelligence.

Artificial Intelligence

There is no single, universally accepted definition for Artificial Intelligence (**AI**). For the purposes of this PIA, we use the definition for AI from New Zealand's AI Forum - "*advanced technologies that enable machines to reproduce or surpass abilities that would require intelligence if humans were to perform them. This includes technologies that enable machines to learn and adapt, to sense and interact, to reason, predict and plan, to*

optimise procedures and parameters, to operate autonomously, to be create, and to extract knowledge from large amounts of data"[1].

Use of Artificial Intelligence at Te Whatu Ora	YES	NO
Does your project/solution involve the design, development, deployment, and/or use of any form of **AI**?	☐	☒

If you have answered '**yes'** to this question, please complete the "**Assessment- Artificial Intelligence at Te Whatu Ora"**. Please contact your Privacy Officer/ Privacy team for more information.

Third Party Artificial Intelligence	YES	NO
Has your project been asked to **share** information that Te Whatu Ora holds (including personal or health information) with a third party to enable the third party to design, develop, train and/or deploy their own AI?	☐	☒
If Te Whatu Ora will contract with a third party for this project/ solution, do the contract terms/ Terms of Service etc., allow the third party to use Te Whatu Ora information to develop, train and/or deploy their own AI?	☐	☒
If the answer is **'yes'** to either of these questions, please provide additional information:		

Once you have completed this section (Artificial Intelligence), please move on to the next section (Review and sign off).

[1] As defined by AI Forum in The New Zealand AI Impacts Research Project, May 2018.

Review and Sign Off

Privacy Officer/Privacy Committee/Privacy & Security Governance Group review	
Name: Emma Graddon – Principal Privacy Advisor Signature: Emma Graddon	Date: 27/02/2024
Business Owner	
Name: Becky Jenkins – Director Protection, National Public Health Service, Te Whatu Ora Signature: 	Date: 23/02/2024
Project Manager	
Name: Toby Regan – National Manager, Major Projects, Protection Directorate, National Public Health Service, Te Whatu Ora Signature: 	Date: 23/02/2024

Appendix 1: Risk and Mitigation Table[2]

Risk Reference Number	Privacy Principle or Rule	Privacy Risk Description *Description of the potential and actual privacy risk identified*	Existing Controls (preventative or detective) *Existing systems and safeguards in place that act to minimise the privacy risk identified*	Assessment of current residual risk *Assess the risk with the existing safeguards and systems in place*	Recommended mitigations or privacy enhancements *Specify recommendations for how the residual risks can be removed and or managed to ensure the individual is protected*	Revised risk rating *Assess the risk when the new safeguards are implemented*	Rationale for revised risk rating
R.01	9	Unclear retention policies result in more information than necessary being retained which may lead to the information being unintentionally released or caught up in a breach.	Existing disposal schedules, see appendix 7, and the General Disposal Authorities currently in place in the health system may address this risk. However further clarification of the definition of a clinical case record and its application to Notifiable Diseases is required to confirm this.	Probability: Likely Consequence: Major Risk rating: High 21	C01 Retention Policy C11 Legal basis for holding Notifiable disease information	Probability: Rare Consequence: Major Risk rating: Medium 10	
R.02	3	Individuals are not adequately advised of their information being collected, used, managed and disclosed leading to individuals viewing the collection as unreasonable or unfair and Te Whatu Ora suffering reputational damage.	Privacy Statements are available on the Te Whatu Ora website and are read out to cases and contacts, see appendix 5 for wording.	Probability: Unlikely Consequence: Moderate Risk rating: Medium 9	C02 Privacy Statement	Probability: Rare Consequence: Moderate Risk rating: Medium 4	
R.03	4	Consideration is not given to how information is collected from individuals who may be vulnerable leading to a breach of R4(1)(b) of the HIPC which will negatively impact the trust and confidence in the health sector.	Policies are in place to ensure that children are represented by their parents/guardians or their legal representatives when they are identified as being a confirmed or suspected as a case or a contact	Probability: Possible Consequence: Moderate Risk rating: Medium 13	C03 Privacy Training	Probability: Unlikely Consequence: Moderate Risk rating: Medium 9	
R.04	5	An authorised user accesses and/or discloses or alters personal information and / or Insider curiosity for an unauthorised purpose leading to one or more individuals' privacy being breached, resulting in reputational damage and loss of trust and confidence in the health sector.	All users require to be approved by a designated Approver who has been nominated by a senior manager/Director. All users will have completed Te Whatu Ora privacy training and agreed to the Terms of Use (at least every three months) and agreed to the Te Whatu Ora code of conduct or for external users a similar and appropriate code of conduct. Users agree to undertake system training, which include aspects of privacy and security. Role-based access controls are in place. NDMS will apply Te Whatu Ora clinical IT systems audit policies to ensure any improper access is logged and can be monitored.	Probability: Possible Consequence: Major Risk rating: High 18	C03 Privacy Training C04 Access Controls C06 Active Monitoring C13 Oversight C14 User Approval C16 Exporting of data	Probability: Possible Consequence: Major Risk rating: High 18	
R.05	5	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.	Penetration testing and security assessment and reviews are conducted to identify system vulnerabilities. Proactive tested and regression testing of the system and its integration function before and system updates to production identify issues before potential of exposing data within the live environment.	Probability: Possible Consequence: Major Risk rating: High 18	C09 Penetration testing C10 Pre-deployment testing	Probability: Unlikely Consequence: Major Risk rating: High 14	
R.06	10	NDMS information is used for a purpose other than that for which it was collected.	Policies are in place to ensure that users are aware of data use policies with all users signing the NDMS Terms of Use Declaration. Proactive monitoring of system access and use implemented.	Probability: Possible Consequence: Moderate	C02 Privacy Statement C07 Governance C08 Terms of Use Declaration	Probability: Unlikely Consequence: Moderate Risk rating: Medium 9	

[2] Based on the Te Whatu Ora Enterprise Risk Management Framework

				Risk rating: Medium 13	C15 Questionnaire Service		
R.07	-	That the PIA is not reviewed and updated to consider the implications of sensitive disease specifically Sexually Transmitted Infections (STIs) before these diseases go live in the system	The PIA is scheduled to be reviewed by September 2024, the expectation is that this review would include the use case for STIs.	Probability: Possible Consequence: Moderate Risk rating: Medium 13	C12 PIA review	Probability: Unlikely Consequence: Moderate Risk rating: Medium 9	

Appendix 2: Control Table

Control Reference Number	Control Name	Control Description	Status	Control Owner	Date of Implementation
C01	Retention Policy	Specific time periods should be identified for removing information after it has not been updated (by way of a patient interaction) for 10 years (as required by the Health (Retention of Health Information) Regulations 1996). Information that is to be retained for analysis and research should be de-identified. This will be achieved through alignment with Te Whatu Ora data retention policies.	In process	Project lead – Toby Regan	30 June 2024
C02	Privacy Statements	Privacy Statements which clearly state how the information will be used, disclosed, retained, and protected, should be updated (attached in this PIA) and uploaded to the Te Whatu Ora website. At the time of signing this PIA, there are some minor amendments and updates required for the Privacy Statement before it is published (to ensure we meet our IPP3 requirements(. HNZ Privacy will work with Project Lead to update this PS as soon as practicable ready for publishing.	In Progress	Project lead – Toby Regan	
C03	Privacy Training	1. In addition to Users of the systems will having completed Te Whatu Ora mandatory privacy training additional training may be required to support case investigation and contact tracing for vulnerable people or related to on sensitive information eg sexually transmitted infections contact tracing. 2. Refresher training on privacy and training on privacy in relation to collecting information from minors will align to Te Whatu Ora standard training policies and practice, once developed.	In process	Project lead – Toby Regan	31 October 2024 Within 6 months of policy implementation.
C04	Access Controls	Ensure role-based access controls are updated to reflect all new disease types added to NDMS.	Ongoing	Project lead – Toby Regan	Progressive to project completion date estimated 31 Dec 2025
C05	Audit logs	Audit logs of review views are capture within the system and available for proactive and reactive review	Complete	Product Manager Amelia Vela	
C06	Active monitoring	Implementation of proactive monitoring of record views and for high profile individuals.	In process	Product Manager Amelia Vela	30 June 2024
C07	Governance	Ensure data governance is in place to ensure information is not used for any purpose other than that for which it was collected, or where an exception applies.	In process	Manager Communicable Disease – Nadine Stephens	30 June 2024
C08	Terms of Use	All users are required to read and sign the NDMS Terms of Use Declaration, see appendix 5.	Complete	Project lead – Toby Regan	
C09	Penetration testing	Security testing complete and Approval to Operate given	In Progress	Product Manager Amelia Vela	
C10	Pre-deployment testing	Test phases of Unit Testing, Functional Testing and User Acceptance Testing completed and signed off by the business and product team	Complete	Product Manager Amelia Vela	
C11	Legal basis for holding Notifiable disease information	Review the legal basis for classifying Notifiable Disease data as 'clinical case records' and the scope of this as it pertains to case investigation and contact tracing records and the implications for storage and destruction of records if is differs from the standard retention of health records for at least 10 years.	In process	Project lead – Toby Regan	30 June 2024
C12	PIA review	The PIA is reviewed and approved to ensure it takes into consideration the privacy implications for the on boarding of sensitive diseases (STIs) prior to these diseases going live in NDMS	In process	Project lead – Toby Regan	30 September 2024
C13	Oversight	Appointment of a role to oversee the appropriate user of the system in respect to application of system access controls, review of use of audit logs in line with monitoring processes, monitoring and reporting of code of conduct breaches, application of onboarding and off boarding processes. Issues identified will be escalated to the Business Owner	In process	Project lead – Toby Regan	30 June 2024
C14	User Approval	Review the User Approval process to ensure that it remains current, robust and that clear records are retained showing appointment of approvals, scope of their licence to approve Users, ie what type of user that can and cannot approve. Review the criteria that users must meet to be eligible to user the system and ensure that any changes are promulgated to the Approver community.	In process	Project lead – Toby Regan	30 April 2024
C15	Questionnaire service	Any change in system (currently Salesforce, CPIR and Snowflake) that uses the questionnaire service will be discussed with Privacy team before use and if appropriate the PIA will be updated to take this into account	On going	Group Manager Products – Ed Faloon	
C16	Exporting of date	Engage with Privacy team to review and consider appropriate controls around the export of reports from NDMS	In process	Project lead – Toby Regan	30 April 2024

Appendix 3: Glossary

Please complete the following table with terms, abbreviations, and acronyms you have used in this PIA.

Term	Definition, description, relationship, and business rules
NDMS	National Disease Management System
NCTS	National Contact Tracing Solution
ESR	Institute of Environmental Science and Research
NIC	National Investigation Centre
EpiSurv	Repository for data to be used for public health surveillance (managed by ESR)
NES	National Enrolment Service

Appendix 4: Sample of Q & A for cases and contacts

The list below is a sample of the types of questions that will be asked of cases and contacts. As this is an operational system these questions will change from time to time so this list should not be treated as a definitive list rather it should be treated as indicative. Typically this information will be collected by case investigators and contact tracers and may be collected via a range of processes including person interviews, phone calls, surveys etc.

Core case Q&A information as at 31 October 2023

Section	Question in Q&A
Identity verification	Can you please tell me your full name? Insert [Account name]
	Can you please tell me your date of birth? Insert [Birthdate]
	Ask to speak to a guardian as this person is under 16.
	*Do you need a support person or someone to speak on your behalf?
	Explain the purpose of the call e.g. I'm calling because of a GP notification or a lab result.
	This is the ethnicity information we currently have recorded for you. [Insert all ethnicities linked to the person account (Ethnicity_c)]
	Do you identify with any other ethnicities?
	Ethnicity:
	Read the privacy statement
	Privacy statement or link to privacy statement
	Confirm the person understands the privacy statement
Guardian or spokesperson details	Their first name
	Their last name
	What's the spokesperson's relationship to the case/ disease contact?
	Their phone number
	Their email
Personal Details	*What language do you feel comfortable using for this interview?
	Do you need an interpreter for this call?
	Arrange to call back with an interpreter to complete the interview. Remember to update the nominated spokesperson information with the interpreters details when it's been arranged.
	Do you identify as a disabled person, or a person with disabilities?
	Details of disability
	Do you identify as a tangata whaikaha Māori?
	Māori person with disabilities determined to do well and create opportunities for themselves.
	Details

	Confirm you've informed the case
Contact Details	*Is this the best number to contact you on?
	Current primary phone number: [Primary phone number]
	Preferred phone number:
	Can you tell me your email address? Insert [PersonEmail]
	We will need an email to send you any information you may need; including exclusion letters.
	Can you tell me your current address? Used across episode, needs to be visible/accessible on DC and Case
	Update address
	Address input field
Occupation	What's your primary occupation?
	This includes paid employment, volunteer work, unemployed, retired, aged care resident, other long-term care resident, child, child at home, child at school, student, parenting a child at home.
	Name of workplace or organisation
	Contact name
	Contact phone
	Contact email
	Contact address
GP Details	What's the name of your usual doctor?
	What's the name of the practice?
	What's the GP phone number?
	Not enrolled with a GP
Underlying conditions	*Are you currently pregnant?
	Which trimester are you in?
	*Do you have a condition that means you have low immunity or are more likely to get sick?
	For example: - Organ or bone marrow transplant recipient - Having chemotherapy or radiotherapy - Have an immunodeficiency illness such as HIV or blood cancer - Medications that cause low immunity e.g. steroids, medicines for rheumatoid arthritis, inflammatory bowel disease medication.
	Record any relevant medication e.g. if immunosuppressed
	Record any relevant details about health issues here
Exposure Details	*Can you confirm you were in the household while the case was infectious
	Start [NDMS_Exposure_Start_Time__c] and End [NDMS_Exposure_End_Time__c]
	If this is different to the date and times above please make a note and update the Managed Under Exposure after completion of the Q&A
	If the contact was not in the household while the case was infectious, update the Managed Under Exposure to Not Exposed after completion of the Q&A.
	*Can you confirm you were present at the event?
	If the contact was not at the event, update the Managed Under Exposure to Not Exposed after completion of the Q&A

	If known, can you tell me about the type of contact you had with the confirmed case?
	Some examples may be; in the same confined space, wore a mask, shared food or drink, in the same classroom.
	*Did anyone else go with you to the event?
	Details of others at event
	*I have confirmed to this person they are a disease contact
Source Investigation	*During this incubation period, have you had contact with a confirmed case?
	What was their name?
	Do you know their date of birth or age?
	When did you first have contact with them?
	Where did you last have contact with them?
	Do you have a phone number we can contact them on?
	Do you have an email address we can contact them on?
	Have you had contact with any other confirmed cases?
	Gather details and enter as a note on the case record.
	*During this incubation period, have you been to particular places where you might have been exposed?
	For instance, an early childhood centre, a school or kura, a university, a hospital, doctors waiting room.
	Please provide details of the place / setting:
	*During this incubation period, did you spend any time with any overseas visitors?
	Can you provide details of the visitors?
	Name, date of birth, where have they come from?
Overseas Travel	*During this incubation period, did you go overseas?
	Date arrived in New Zealand:
	Last country visited:
	City/Region:
	Date entered:
	Date departed:
	Did you visit any other countries?
	Country
	City/Region:
	Date entered:
	Date departed:
	Did you visit any other countries?
	Country
	City/Region:
	Date entered:
	Date departed:
New Zealand Travel	*During this incubation period, have you visited any areas in New Zealand where there have been reports of cases?
	If yes, can you provide details?

	*During this time, are you aware of any other places where you may have been exposed to someone with?
	Can you provide details?

Measles immunisation and symptoms Q&A information as at 31 October 2023

Section	Q&A question
Immunisation	*Have you received the MMR vaccination? How many doses?
	*Were you vaccinated in Aotearoa New Zealand?
	What country were you vaccinated in?
	Did you receive the MMR vaccine in the last six weeks?
	*Have you had measles previously?
	Can you provide evidence of this infection? E.g. Doctor's records.
	Can you provide evidence of these vaccinations?
	When did you have your vaccination/s?
	Vaccine date (MMR0)
	Vaccine date (MMR1)
	Vaccine date (MMR2)
	*Do you recommend contact has MMR vaccine?
	If contact has had 1 dose and within 72 hours from first exposure recommend 2nd dose (unless immunocompromised or pregnant). If no doses, and within 72 hours from first exposure. recommend 1st dose of MMR If contact does not know if they're vaccinated consider MMR vaccination if appropriate
	Does the contact agree to arrange MMR vaccine?
	*Have you ever had blood tests to confirm you are immune or protected from measles?
	Details of previous serology
	Do you recommend contact has blood test to show immunity?
	If contact does not know if they're vaccinated and within 7 days from date of first exposure request blood test to show immunity status
	Contact agrees to blood test to show immunity status.
Symptoms	*Have you had any of these symptoms? Please select all that apply
	Details of other symptoms:
	*What date did the fever start?
	*Did you have a fever when you first noticed the rash?
	*When did the rash appear?
	*Where on your body did the rash start?
	If the rash has spread, where has it spread to?
	Are you currently on or have been on antibiotics in the last week before symptom onset?
	*Do you currently have any measles symptoms since your exposure?
	*What symptoms do you currently have? Ask and respond to each symptom separately
	Fits criteria for immunoglobulin recommended?
	If contact gets immunoglobulin quarantine is for 18 days ~~days~~ after last exposure to a case (NHIUG can prolong incubation period).
Isolation & welfare	Explain what it means to isolate and provide isolation advice. They must isolate from <NCTS_Rash_Onset_Date__c> for four days and are free to resume normal activities the following day.
	*Will you be isolating at your current address you gave me at the start of the interview? [Current address]
	*Will you need any help to be able to isolate?
	Details of support needs:
	Remember to advise to contact Healthline/GP if symptoms get worse or if they are concerned about their health. If it is an emergency, advise to dial 111.
	Supporting or other information from the call:
Contact management & quarantine	*Based on the information provided during this call is the contact required to quarantine?

	Quarantine (stay home) start date <NDMS_Planned_Quarantine_Start_Date__c>
	Quarantine (stay home) end date <NDMS_Planned_Quarantine_End_Date__c>
	Will you be quarantining at the current address you gave me? [Current address]
	*Will you need any help to be able to quarantine?
	Details of support needs:
	Do you need an exclusion letter for your employer/school/early childhood centre?
	Are you aware of anyone in your household who is not immune to or vaccinated against measles?
Source Investigation	The incubation period is [NDMS_Incubation_Period_Days__c] days before the rash onset date - use that timeframe to ask the following source investigation questions.
	Rash onset date for this case is [NDMS_Rash_Onset_Date_c]

Measles health checks Q&A information as at 31 October 2023

Section	Q&A question
Symptoms **(Disease contact health check)**	*Do you currently have any measles symptoms?
	Note: If fever present at onset of rash and rash started on the head, consider advancing to probable case.
	*Contact advised to test for measles?
	*Have any of your symptoms worsened since your last health check?
	What are the details of your worsening symptoms?
	Have you had an MMR vaccine for since your last health check?
	Have you had a blood test (serology) to confirm your immunity since your last health check (if applicable)?
Release Decision	*Has the contact completed the required days in quarantine since their last exposure with case?
	*Release from quarantine?
	Remember to extend quarantine on the contact record
	*Who was involved in this release decision
	Additional release decision details
Symptoms **(Case health check)**	*Are you feeling worse than yesterday?
	What are the details of your worsening symptoms?
	If symptoms are worsening, refer to Healthline/GP and in an emergency 111.
	If the case has met the requirements to be released, 4 days post rash onset and release on day 5.
	Do you need any help to continue to isolate?
	E.g. Do you have whanau support? Assistance with groceries etc?
	Details of support needs:
	Advise case to contact GP if symptoms get worse or if they are concerned, if no GP then advise 111.

Appendix 5: Terms of Use Declaration

Terms of Use and Confidentiality Requirements

Welcome new or returning user

Prior to accessing the National Disease Management System (NDMS) you must read the Terms of Use and agree to the Declaration outlined below. By agreeing, you are deemed to have accepted the Terms of Use and Declaration.

As a quick reminder please confirm the following points:

- Privacy is a key priority for all of us working with the NDMS. Public trust is important, and we must all work together to earn that trust.
- You must comply with the Privacy Act and the Health Information Privacy Code, when using the NDMS or any information related to the NDMS.
- You must take care of NDMS information and keep it secure and confidential.
- You will only look at the information you need to perform your role, and not disclose it to anyone else unless they need it to perform their role.
- You will not share your access credentials with anyone or let anyone else use yours.
- You will only access the NDMS by secure devices approved by your organisation (they must be kept up to date with all security software releases and have strong password protection or encryption to prevent unauthorised access).
- You understand that all access to the NDMS by you will be logged and may be monitored.
- You will let your manager, or the Privacy Officer know immediately if you think there may have been, or is about to be, a privacy or security breach. The sooner we know, the sooner we can resolve any issues.

User requirements

In your role you are to be authorised as a user of the NDMS. You will have access to personal and health information, and in your interactions with individuals. Each user is a trusted part of health system, and we must all take privacy matters, and the protection of personal and health information, seriously.

There are requirements that all users must meet. All users must:

- Understand their obligations under, and comply with, the requirements of the New Zealand Privacy Act 2020 and the Health Information Privacy Code 2020.
- Operate in a manner consistent with the requirements of the code of conduct for the State Services – Standards of Integrity and Conduct.
- Complete and sign their agreement to these Terms of Use and the Declaration of Confidentiality prior to accessing the NDMS (or further accessing the NDMS if they are amending their password for access).
- Complete any training offered to them in relation to the NDMS operations satisfactorily.
- Cooperate and assist in any investigation or inquiry into any breach, or potential breach, of privacy if requested.

If any user does not comply with the user requirements or acts contrary to the declared statements below, their access to the NDMS may be removed, and the matter may be referred to the users employer, or other legal action may be undertaken if appropriate.

Declaration requirements

As an NDMS user, I hereby declare that:

- I will not knowingly access or disclose any personal or health information about any individual(s) unless such information is essential for me to properly and efficiently perform the duties and obligations of my role.
- I will protect the confidentiality of all personal or health information, ensuring it is not visible on an unattended computer screen, or in an unattended area which may allow access to the information by unauthorised persons. I will ensure that, so far as it is within my control, such information, whether in the form of paper documents, computerised data or any other form, cannot be viewed by any unauthorised persons.
- I will not use any unauthorised device to connect to the NDMS and will not download any information from the NDMS unless it is essential to fulfil my role, and I will ensure the security of any such downloaded information.
- I will inform my supervisor/the relevant privacy officer immediately if I become aware of any breach of privacy or security in the course of my duties/obligations.
- I understand that my credentials (username and password) for access to the NDMS are only for my own individual use, that I must not divulge the credentials to any other person or use another person's credentials. When I am logged on to NDMS I will not allow access by any other person to the NDMS or the information on it.
- I understand that my access to the NDMS 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.

AGREE / **NOT AGREE**

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 2020*
- *The Health Information Privacy Code 2020*
- *The Health and Disability Code of Health and Disability Services Consumer's Rights.*

Appendix 6: Privacy Statement and Information Sheet

Privacy statement script for Cases:

- *"Before we continue, I want to reassure you that this call is confidential, and your information will be kept safe in accordance with the New Zealand Privacy Act.*

- *We may need to share some of your personal information with other agencies for health purposes and to ensure we meet our legal obligations. We may also share information for statistical and research purposes, but no information will be published in a form that could reasonably be expected to identify any individual.*

- *To prevent the spread of disease, we may need to talk to your contacts, and information about where you've been and your movements while infectious may need to be shared with others. While we do everything we can to make sure that you remain anonymous, in certain situations more information may need to be given to contacts to prevent or reduce a serious threat to public health – this will always be discussed with you first.*

- *If you would like more information about how your personal information is managed, please go to the Te Whatu Ora website, and look for our 'privacy & security' webpage.*

- *Our calls may be recorded for quality assurance and training purposes."*

Privacy statement script for Disease Contacts:

- *"Before we continue, I want to reassure you that this call is confidential, and your information will be kept safe in accordance with the New Zealand Privacy Act.*

- *We may need to share some of your personal information with other agencies for health purposes and to ensure we meet our legal obligations. We may also share information for statistical and research purposes, but no information will be published in a form that could reasonably be expected to identify any individual.*

- *If you would like more information about how your personal information is managed, please go to the Te Whatu Ora website, and look for our 'privacy & security' webpage.*

- *Our calls may be recorded for quality assurance and training purposes."*

Notifiable Disease Management System (NDMS) Privacy Statement for Handouts

The Notifiable Disease Management System (the NDMS)

Health New Zealand - Te Whatu Ora uses a secure national electronic database to support the notification of infectious diseases and the accurate and secure recording of all notifiable disease case and contact activity.

Case investigation and contact tracing is a normal part of the management of all notifiable diseases. It's key to ensuring that we limit the spread of the disease.

This Privacy Statement outlines how Health New Zealand (referred to as "we" or "us") may collect, use, store and otherwise handle your personal information in NDMS in accordance with the Privacy Act 2020 and Health Information Privacy Code 2020.

We may update this privacy statement from time to time. This privacy statement was last updated on **27 February 2024.**

What are the purposes of the NDMS?

The purpose of the NDMS is to provide a national collection of notifiable infectious diseases and hazard events and to support case investigation and contact tracing. Information is collected and used for the following purposes:

- national and regional management, planning and reporting,
- auditing case investigation and contact tracing related services,
- quality improvements and statistical analysis,
- research purposes will be authorised by the Director-General of Health, if required and approval by an ethics committee has been given for that research and it will not be published in a form that could reasonably be expected to identify any individual.

Only authorised users who have been granted access credentials are able to access the NDMS, and these users will all be involved in case investigation and contact tracing related processes.

Is the collection of information voluntary?

Under the Health Act 1956, the initial notification of laboratory results is mandatory, and medical practitioners are required to notify people who have or are suspected of having a notifiable infectious disease.

Depending on the risk associated with that disease, case investigation and contact tracing activities will be undertaken to limit the spread. Some information will be sourced from other databases such as test results and contact details without any direct contact with individuals.

Case investigators and contact tracers will always seek to work with individuals to obtain information on a voluntary basis as this information is so important. However, if necessary, the case investigators and contact tracers may use the provisions of Part 3 of Subpart 5 of the Health Act 1956 and require individuals and other persons to provide information on a mandatory basis in accordance with the provisions of that Act.

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 1996. This means at least 10 years from the latest interaction. Other information that is not relevant for the management of notifications, case investigations and contact tracing purposes will either not be recorded in NDMS or be regularly deleted.

Storing Information Securely

We take reasonable steps to ensure your personal information is protected against loss, unauthorised access, use, modification, disclosure, or other misuse.

Access to and requests to correct the information

You have the right to access any information we hold about you and ask us to correct it if you think it is wrong.

To access any personal information held by us, or if you wish to correct your information, please email [to be confirmed].

When making a request to access or change your information, please include:

- your name
- contact address (email or postal)
- contact phone number
- details of the information you want or want to correct - this needs to be as clear and specific as you can make it.

We may ask you for more details.

Please note that before we can provide you with your information or make any changes we need to be satisfied about your identity. To do so, we may need to ask you further questions or to view identification which establishes your identity.

Requesting information on behalf of someone else

If you are requesting information on behalf of someone else, you will need to provide their authorisation or other documentation to support that you have the right to do so.

Queries or Concerns

If you have any queries or concerns about how your personal information has been managed, please contact us to see if we can resolve the problem.

You can-

- Email us at hnzprivacy@health.govt.nz
- Write to us at Privacy Officer - Te Whatu Ora, PO Box 793, Wellington 6140, New Zealand I

If you're not satisfied with our response to your concerns, you can contact the Office of the Privacy Commissioner. For more information see the Office of the Privacy Commissioner's website.

Notifiable Disease Management System (NDMS) Privacy Statement for Web

The Notifiable Disease Management System (the NDMS)

Health New Zealand - Te Whatu Ora uses a secure national electronic database to support the notification of infectious diseases and the accurate and secure recording of all notifiable disease case and contact activity.

Case investigation and contact tracing is a normal part of the management of all notifiable diseases. It's key to ensuring that we limit the spread of the disease.

This Privacy Statement outlines how Health New Zealand (referred to as "we" or "us") may collect, use, store and otherwise handle your personal information in NDMS in accordance with the Privacy Act 2020 and Health Information Privacy Code 2020.

We may update this privacy statement from time to time. Please check this privacy statement regularly for modifications and updates. This privacy statement was last updated on **27 February 2024.**

What are the purposes of the NDMS?

The purpose of the NDMS is to provide a national collection of notifiable infectious diseases and hazard events and to support case investigation and contact tracing. The NDMS is used to record information collected about people with, or suspected of having, a notifiable infectious disease and hazard events to identify the source of the infection and help prevent its spread.

This enables contact tracers to make contacts aware that they have been exposed and advise them to take appropriate precautions to keep themselves and their whanau safe. It will also be used to identify and manage the source of the disease, where appropriate.

The NDMS is used by Te Whatu Ora, National Public Health Services, and the Crown Research Institute of Environmental Science Research (ESR) to support the effective management of infectious disease by undertaking the following activities:

- national and regional management, planning and reporting,
- auditing case investigation and contact tracing related services,
- quality improvements and statistical analysis,
- research purposes will be authorised by the Director-General of Health, if required and approval by an ethics committee 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 NDMS?

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

How do case investigators and contact tracers use the NDMS?

Case investigators and contact tracers are specially trained, and authorised under the Health Act, to make inquiries of those people who have, or are suspected of having, a notifiable disease, and advise those who may be at risk of infection.

The NDMS assists case investigators and contact tracers by performing the following functions:

- **Receive notifications:** Recording the laboratory test results for notifiable diseases and receive notifications from medical practitioners for people who have or are suspected of having a notifiable disease.

- **Making contact:** Providing access to National Health Index (NHI) and National Enrolment Service (NES) information. This means we can make sure we have the correct identification of individuals and the most up to date demographic and contact details. Cases investigators and contact tracers may contact cases to gather additional information and undertake contact tracing, this may occur

in person, via phone or through surveys and questionnaire (manual and electronic). Sometimes contact tracers will check in with cases and contacts to see how they are. This can be done either by phone call or online using NDMS.

- **Recording:** Storing case management information for notifiable diseases and all relevant contact tracing details.

- **Pathways:** All cases proceed along NDMS pathways that are clinically designed to minimise risk to cases, contacts and the general public.

- **Investigating:**

    - **Seeking information:** Sometimes it can be difficult to identify or locate cases or contacts. In these instances, we make inquires outside of the NDMS to help locate them so they can be given the relevant information to help keep themselves and others safe.
    - **Exposure Events:** These are place where people may have been exposed to a disease. This could include, for example, a flight, a party at a bar, or a church service.

Is the collection of information voluntary?

Under the Health Act, the initial notification of laboratory results is mandatory, and medical practitioners are required to notify people who have or are suspected of having a notifiable infectious disease.

Depending on the risk associated with that disease, case investigators and contact tracing activities will be undertaken to limit the spread. Some information will be sourced from other databases such as test results and contact details without any direct contact with individuals.

Case investigators and contact tracers will always seek to work with individuals to obtain information on a voluntary basis as this information is so important. However, if necessary, the case investigators and 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. NDMS processes ensure your personal information is managed appropriately.

Your personal information will be held and managed in accordance with the Privacy Act 2020 and Health Information Privacy Code 2020. Any information collected onto the NDMS will be held securely in compliance with Te Whatu Ora standards. Measures are in place to protect your information from unauthorised access. To deliver the NDMS 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 NDMS. The PIA will be updated to reflect features and functionality of the NDMS.

How long will your information be kept for?

Information about the health records will be retained as required by the Health (Retention of Health Information) Regulations 1996.

NDMS data is retained for at least 10 years in accordance with various legislative requirements such as:

- The Health (Retention of Health Information) Regulations 1996

- ISO15189 data retention requirements.

Where health information doesn't form part of a person's health record and it is not required to be held for other legitimate reasons eg specific requirements under legislation, it will be destroyed once there is no longer a lawful purpose for retaining it.

Access to and requests to correct the information

You have the right to access any information we hold about you and ask us to correct it if you think it is wrong.

To access any personal information held by us, or if you wish to correct your information, please email [to be confirmed].

When making a request to access or change your information, please include:

- your name
- contact address (email or postal)
- contact phone number
- details of the information you want or want to correct - this needs to be as clear and specific as you can make it.

We may ask you for more details.

Please note that before we can provide you with your information or make any changes we need to be satisfied about your identity. To do so, we may need to ask you further questions or to view identification which establishes your identity.

Requesting information on behalf of someone else

If you are requesting information on behalf of someone else, you will need to provide their authorisation or other documentation to support that you have the right to do so.

Queries or Concerns

If you have any queries or concerns about how your personal information has been managed, please contact us to see if we can resolve the problem.

You can-

- Email us at hnzprivacy@health.govt.nz
- Write to us at Privacy Officer - Te Whatu Ora, PO Box 793, Wellington 6140, New Zealand I

If you're not satisfied with our response to your concerns, you can contact the Office of the Privacy Commissioner. For more information see the Office of the Privacy Commissioner's website.

Appendix 7: Disposal of information

Information to be deleted within six months of collection: data that is not used as part of active Contract Tracing
Survey responses from the Daily Check-In for all Contacts who have not developed any symptoms. If they remained asymptomatic it is not considered a health record (although a record will be retained confirming the individual did complete the Daily Check-In process).
Retained for two years post creation of the record
Any tracking and auditing information of User access within the NDMS, unless specified elsewhere including organisation policies.
Retained as a 'health record' for minimum of 10 years
Records of notified cases and their contacts and exposure events are considered clinical records and these records will include the name, identification and contact details, NHI, test result (if any), health check records.
Research and planning
Non-identifiable (or de-identified) information may be retained, to be used for purposes related to the public health response 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 contact information to enable effective management of infectious disease as contemplated by the Health Act Part 3A.