Health New Zealand
Te Whatu Ora

Health New Zealand | Te Whatu Ora

Notifiable Diseases Management System (NDMS)

Privacy Impact Assessment

Date: 29 August 2025

Document Details

HNZ Scope of Use	Whole of Health New Zealand | Te Whatu Ora
Business Unit	Major Projects, Protection Directorate, National Public Health Service
Business Owner	Toby Regan – National Manager, Major Projects, Protection, NPHS
Assessment Author	Katie Stokes – Senior Advisor, Major Projects, Protection, NPHS
Current Version	v3
Previous Versions	1) National Disease Management System (NDMS) (6 Oct 23) 2) National Diseases Management System (NDMS) (26 Feb 2024)
NDMS Live Date	28 February 2024
Next Phase Go-Live	October 2025 (approximately)

Privacy assessments are living documents which must be updated and revised whenever significant changes affect the personal information being handled. Additionally, these assessments should be periodically reviewed to ensure they remain accurate and relevant.

Scheduled Review of Assessment	This assessment is to be updated and revised prior to any significant developments or changes are implemented in NDMS. Due to the sensitivity of this system, this Privacy Impact Assessment (PIA) must be reviewed no later than 2 years since the date of the last version.

Summary of Notifiable Diseases Management System (NDMS)

The purpose of this PIA is to assess the current state of the Notifiable Disease Management System (NDMS) – a system stood up in February 2024 which is undergoing developmental phases as it matures. As well as detailing current operations and functionalities, this assessment also includes the next significant planned implementation to ensure any privacy risks and controls, related to that implementation, are captured and addressed prior to its go live.

A copy of this PIA will be available on NDMS webpage of the Te Whatu Ora website - Notifiable Disease Management System (NDMS) – Health New Zealand | Te Whatu Ora

Background

In response to the COVID-19 pandemic, the Ministry of Health | Manatū Hauora (MOH) created the National Contact Tracing Solution (NCTS) to support the public health response in managing COVID-19 cases and contacts, significantly enhancing the capacity and reliability of these activities. Responsibility for NCTS was later transferred to Health New Zealand (HNZ) and expanded to support the public health management of measles. On 28 February 2024, NCTS was decommissioned and replaced by NDMS, which incorporated many features, tools, and lessons learned from NCTS. Case and contact information from NCTS were not migrated to NDMS.

Purpose of NDMS

NDMS is an operational notifiable disease management system that supports the investigation, response and control of communicable disease, and strengthens New Zealand's surveillance systems.

NDMS is operated within a HNZ instance of the Salesforce platform – a Cloud based application. Access by Users to NDMS is through a secure URL which requires a personal secure work account and email login.

The purposes of NDMS are to enable:

- national management of, and reporting on, individual Cases, their Contacts, and details of locations or events where exposure to a disease may have taken place. Activities recorded in NDMS include:
  - identification, investigation and management of Cases
  - identification, follow up and monitoring of individuals who have been in contact with a Case (known as Contacts).
  - collection of relevant information from other individuals or organisations as authorised under the Health Act provisions or other relevant legislation.
- the national and local planning required to provide effective management of an infectious disease in accordance with s92ZZG(2) of the Health Act.

Legislation Applicable to NDMS

Notifiable infectious diseases are set out in the Health Act 1956, Schedule 1, Part 1. NDMS will only be used for notifiable infectious diseases listed under Sections A and B and the conditions listed under Schedule 2.

Sections 74 and 74AA of the Health Act 1956 requires both HP (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 provides a range of duties and powers of the Medical Officers of Health. These powers are wide ranging but are heavily based on a set of overarching principles detailed in subpart 1 of Part 3A.

Subpart 5 in Part 3A 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.

Current Notifiable Diseases Managed by NDMS

- Measles
- Covid-19

Next Phase Implementation

New Zealand Traveller Declaration

In future (anticipated 2026), information from the New Zealand Traveller Declaration (NZTD) is expected to be sourced via the Traveller Journey Index (TJI), a NZ Customs and Ministry of Business Innovation and Employment maintained database via a direct link to NDMS. This will occur under an MoU agreement.

Only personnel in the Finders Service will access TJI for the purpose of tracing notifiable communicable diseases in passengers who have entered or exited New Zealand on a flight or a vessel. More information on the Finders Service can be found in Appendix 1: Finders Service.

While the details of this integration are not fully assessed in this PIA, the proposed approach poses no immediate major privacy concerns and is expected to be privacy assessed (likely led by NZ Customs). If there are significant further privacy considerations for NDMS beyond that covered in this version of the PIA, the PIA will be updated as appropriate in advance of implementation. Otherwise – and as currently anticipated and described – privacy assessment will be carried out as a separate activity and the PIA updated when otherwise being reviewed/updated.

Additional Diseases Managed by NDMS

A rollout will commence in October 2025, whereby all diseases in the in-scope schedules and sections will be loaded into and managed in NDMS. This will comprise:

- Schedule 1 – Infectious diseases, Part 1 – Notifiable Infectious Diseases:
    - Section A – Infectious diseases notifiable to medical officer of health and local authority (13 diseases)
    - Section B – Infectious diseases notifiable to medical officer of health (39 diseases including COVID-19 and measles already in NDMS)
- Schedule 2 – Diseases notifiable to medical officer of health (other than notifiable infectious diseases):
    - Section B – Other conditions (6 diseases)

More sensitive diseases, as contained in Schedule 1, Part 1, Section C, and Part 2, will not be loaded and managed in NDMS at this time. If these were to be considered for adding at a later time this would be subject to further privacy assessment and updating of this PIA.

Noting: this PIA considers the requirements for the diseases which have not yet gone live. If additional information is required, which is not listed in the 'Personal and/or Health Information Involved' section, this PIA will be updated to reflect those changes.

NDMS Core Functions

The core functions of NDMS are designed to enhance the efficiency and effectiveness of contact tracing efforts, improve data management, collect surveillance information and ensure the privacy and security of personal information.

Contact Tracing

NDMS is designed to support the management and surveillance of notifiable communicable diseases by recording and managing information about individuals who have/may have a notifiable communicable disease (Cases), and individuals who may have been exposed to a disease through contact with a Case (Contacts) to prevent further transmission.

Information recorded in NDMS will relate to one of the following categories:

1 An individual who is identified as a Case
2 An individual who is identified as a Contact (some Contacts may become Cases)
3 Details of locations and individuals that may have been a potential source of a notifiable disease
4 Details of a location where an individual(s) with a notifiable communicable disease was present with other individuals whilst infectious (Exposure Event).

Information Collection and Management

NDMS collects and manages information related to Cases and Contacts, including test results, contact details, and information about potential exposure events. Information and data will be used to monitor and manage the spread of diseases.

Case Management

To stop the spread of some infectious diseases, Public Health may require Cases to isolate from others during their infectious period. For diseases that require Cases to isolate, Public Health staff may check-in on Cases to monitor their health and provide support. NDMS provides Users with a regular check-in function to support with this process, which includes regular monitoring of symptoms and health status to ensure timely intervention if needed.

Security

NDMS includes robust security measures to protect the privacy and confidentiality of personal and health information. This includes encryption, role-based access controls, and will conduct regular audits to ensure compliance with privacy regulations.

Refer to Principle 5 which provides greater detail on Security aspects in place for NDMS.

Integration and Use of Other Systems

NDMS integrates with other **health information** systems/databases to ensure accurate and up-to-date information is available for contact tracing and case management.

HNZ operated/maintained system/database	Description of integration
National Health Index (NHI)	To provide NDMS with personal details of cases and contacts e.g. name, age and date of birth
National Enrolment Service (NES)	To provide NDMS with GP details of cases and contacts
Aotearoa Immunisation Register (AIR)	To provide NDMS with immunisation details of cases and contacts
Health Provider Index (HPI)	To provide NDMS with health organisations and practitioners details of cases and contacts
Care Coordination System (CCS)	To enable operational management of clinical care for cases who have a disease that requires longer follow up care than most other diseases, such as tuberculosis and acute rheumatic fever. Cases of these diseases automatically self-populate in CCS to enable more clinical details to be logged under a case. Once treatment logged as completed in CCS, case will be closed in NDMS. This limits access to clinical information such as dosage and treatment dates to only those with access to the CCS (typically primary care staff). (see more detail on page 7-8)
External Agency system/database	**Description of integration**
EpiSurv (PHF Science (formerly ESR))	To ensure PHF Science can still conduct surveillance activities from EpiSurv until it is replaced by NDMS and the NPHS Data Warehouse.
Mirth (PHF Science Labs)	To provide NDMS with direct laboratory notifications

The following databases/systems/solutions may also be accessed and/or used to complete and **collect additional** information for NDMS to support public health action:

- Patient Management Systems (PMS)
- Regional Clinical Systems (Portals) – hospital systems

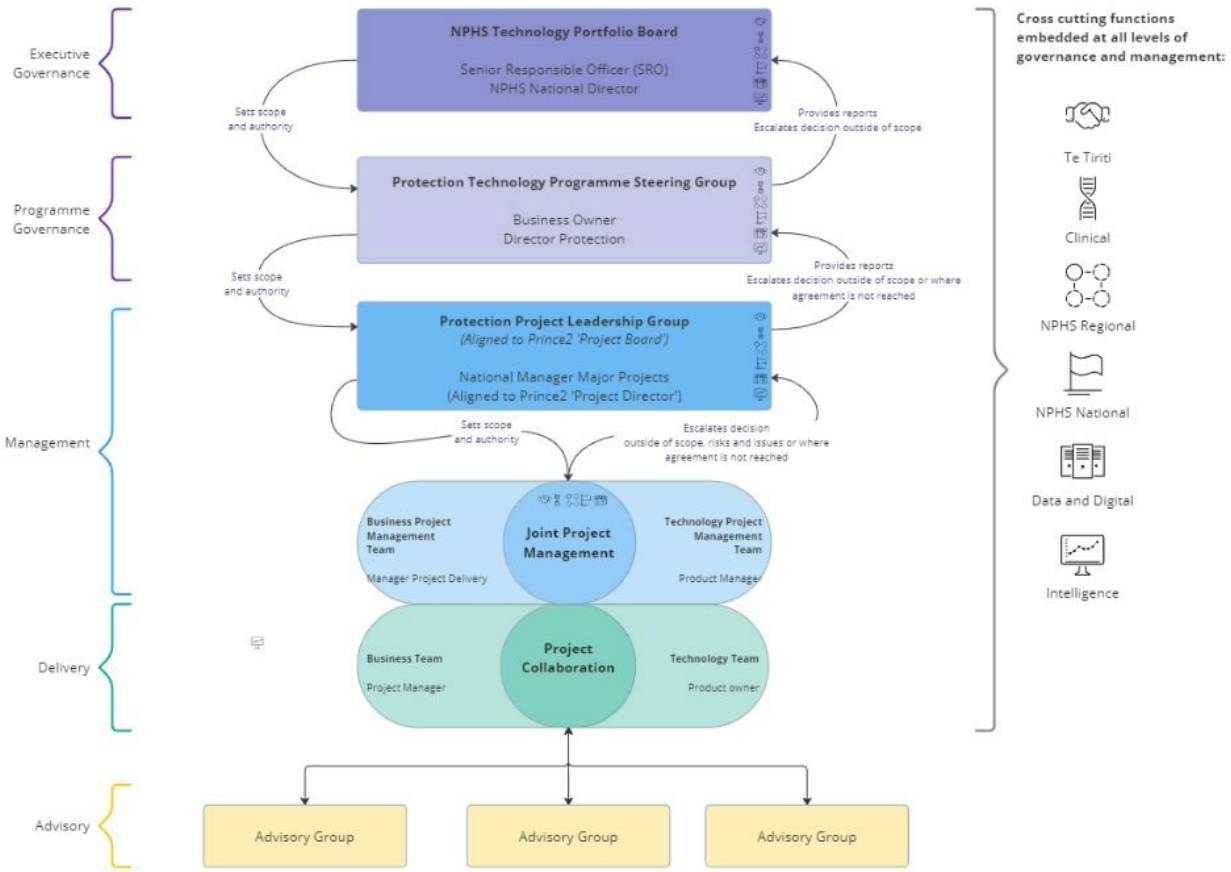
- Laboratory systems not utilising Mirth data sharing mechanism (some labs may send some test results to PHF's Labs which is integrated with NDMS. However, some test results won't be sent to Mirth which will require Public Health to access results manually from Labs)
- Direct Laboratory Notifications (DLNs) (mechanism used to transmit lab results via EpiSurv)
- Air New Zealand – flight information (including persons on flights)
- NZ Police – contact information for difficult to source Contacts
- Traveller Journey Index (TJI) and Customs – NZ Customs
- HNZ Consumer Population Identification and Registration Service (CPIR) - (communications and engagement tool)
- Fast Healthcare Interoperability Resources (FHIR) - (integrated communication function)
- Address Service (eSAM)
- Google Places Application Programming Interface (API) - (integrated geolocation finder)

Governance and Oversight (Interim)

While NDMS is being built, a project governance structure has been established that provides interim oversight of NDMS. An enduring governance structure will be established closer to the end of NDMS build, to ensure the project transitions smoothly into business-as-usual processes.

The interim governance structure provides a comprehensive framework that includes oversight by various governance groups and committees. This ensures that the system operates effectively and in compliance with relevant laws and regulations.

NDMS Governance Model



Current Agreed Interim Governance Responsibilities and Accountabilities

Activity	Business Unit and Directorate responsible	Role accountable
Compliance with Retention of Information Policy	NDMS Product Team, Data and Digital	Product Owner
Monitoring audit logs and reviewing compliance with processes (with consequences for non-compliance)	NPHS, Protection	Regional Kaitātaki Health Protection & Director, Protection
Oversight of provision of appropriate training to Users (with updates as required when new functionality or new issues arise)	NPHS, Protection	Director, Protection

For additional and ongoing (i.e non-interim) responsibilities relating to user access and data stewardship, see pages 23 and 24.

Agency Collaborations

PHF Science

EpiSurv is New Zealand's national surveillance system for notifiable diseases, managed by the New Zealand Institute for Publich Health and Forensic Science (PHF Science) (formerly the Institute of Environmental Science and Research (ESR)). It collects detailed information on cases of infectious diseases, which helps Public Health monitor trends, identify outbreaks, and implement control measures effectively. It is envisaged that the case management of notifiable disease within EpiSurv will be replaced solely by NDMS as notifiable diseases are built.

Until then, notifiable infectious diseases are securely notified directly to NDMS and EpiSurv to support the notification process and enable the case and contact management processes to be undertaken in respect of all affected individuals.

A direct integration/interface with PHF Science enables a 'feed' of pre-determined information fields into NDMS of confirmed test results and associated NHI identification/contact details.

National surveillance data (anonymised data showing trends and insights on infectious diseases) from NDMS is also fed back to PHF Science for incorporating into EpiSurv. This is an interim process. As NDMS builds functionality for each disease, data will be integrated with the Snowflake data warehouse (known as the NPHS data warehouse) instead of EpiSurv to phase out use of this system and keep all data within HNZ.

NZ Customs

Two agreements are attributed to NZ Customs for the specific purpose of locating and contacting individuals who have been exposed to a notifiable infectious disease during international travel. Both are applicable only to the Finders Service. See commentary on sharing information under the Principle 10 discussion in this PIA for more detail on these agreements.

- Memorandum of Understanding - request for information for the purposes of Contact Tracing
- Direct Access Agreement (s315 Customs and Excise Act 2018) – supplementary to the MoU. Currently in draft, authorises direct access to information held in the TJI relevant to Contact Tracing.

NZ Police

An MoU with NZ Police, applicable only to the Finders Service, which relates to the sharing of information about Cases and Contacts between HNZ and Police for contact tracing purposes in relation to notifiable infectious diseases. This is to be used in instances where Police may hold contact information for Cases and Contacts not otherwise readily available to Contact Tracers. Information

obtained by the Finders Service will be manually entered into NDMS. See commentary on sharing information under the Principle 10 discussion in this PIA for more detail on the MOU.

Air New Zealand

An MoU with Air New Zealand, applicable only to the Finders Service, which agrees to the sharing of information about Cases and Contacts for the purposes of contact tracing notifiable infectious diseases.

The MoU enables HNZ access to New Zealand flight border arrivals, transit or departures which involve a Case or Contacts and New Zealand domestic flights which involve a Case or Contacts. Relevant personal details obtained by the Finders Service will be manually entered into NDMS, for the purposes of contact tracing. See commentary on sharing information under the Principle 10 discussion in this PIA for more detail on the MOU.

Surge Workforce

In the event of the NPHS surpassing capacity to manage communicable diseases (e.g. in a pandemic scenario), a surge workforce may need to be stood up. This scenario has been considered in the design and development of operational processes, including the criteria for NDMS Users, as specified in NDMS User Framework (see Principle 5 for more detail on this Framework).

NDMS Users (Overview)

Users of NDMS will be those directly involved in the management of notifiable diseases within the National Public Health Service (NPHS), this includes Medical Officers of Health, Public Health Nurses (PHN), Health Protection Officers (HPO), Communicable Disease Nurses (CDN), Contact Tracers and those supporting these activities.

More information on Users can be found in Principle 5.

Finders Service

The Finders Service is a function within the national Communicable Disease Group that plays a role in identifying the location of hard-to-find Cases with an infectious disease or Contacts exposed to an infectious disease.

Finders Service can also determine whether a person is still in New Zealand and notify the National Focal Point (NFP) if the person has left New Zealand, the details of the flight they departed New Zealand on, and, when information is available, further connecting flights.

The Finders Service is named in a number of Information Sharing Agreements and MoUs as their discrete function limits the privacy risks involved. See commentary on sharing information under the Principle 10 discussion in this PIA.

Data Analysis via Snowflake

Identifiable information will be provided to **NPHS data warehouse Snowflake Instance** for analytical and reporting purposes, crucial for clinical oversight of disease management and surveillance functions of disease control. Data may also be used for research purposes.

A separate privacy assessment will be completed which will clarify the purposes and uses for the data available in this repository.

Use of CPIR

HNZ Consumer Population Identification and Registration Service (CPIR) has been engaged to provide the following services:

- delivers questionnaires/surveys
- communicates with identified cohorts of the population as and when required
- analyses which consumers to contact and whether a health check has been completed

A separate NDMS use case for CPIR is being developed to provide further detail on the use of this specific tool.

Connection to Care Coordination System (CCS)

The Care Coordination System is a register currently being built to improve outcomes for those diagnosed with diseases requiring longer term care. This system will improve the recording and delivery of best practice secondary prevention care plans.

Access to this system will be limited to health practitioners responsible for delivering this care, (largely primary care staff). Only public health staff responsible for delivering long term care for people with the conditions managed by CCS will have access to both systems.

Only the information needed to fulfil the function of NDMS (e.g. case status) will be automatically updated within a case record in NDMS when logged in CCS.

This will enable NDMS to fulfil reporting and surveillance requirements, just as it would for other diseases, whilst enabling the logging of more detailed care information in the CCS, fulfilling separate functions that still support one another. A PIA on CCS has been completed, with a copy available from the National Privacy Office.

Expected Future Developments

NDMS is a system that will be maturing and building throughout 2025. As noted above, where a significant impact on person/health information is expected from these developments, this PIA will be updated.

Assessment Scope

Please define the scope of this PIA

This assessment will look at the impact on the privacy of an individual's personal and health information which will be collected, used, stored, and/or disclosed through NDMS.

Please describe what has been excluded from the scope of this PIA and why

The following systems/programmes of work have been excluded from this assessment and mentioned only where relevant, as each will be subject to its own privacy and/or security assessments:

- All HNZ and External Agency systems/databases as detailed in ***Core Functions - Integration with Other Systems*** (including those listed, but not integrated)
- The Salesforce Platform
- The Snowflake Platform including the NPHS data warehouse instance of Snowflake and details of data use and reporting for NDMS data in the NPHS data warehouse
- NDMS use of CPIR
- Laboratory testing pathways
- Details of the integration between NDMS and the Traveller Journey Index
- The activities of the Finders Service (except as these relate to the recording and use of relevant information in the NDMS)
- Training of relevant health professionals (e.g. Contact Tracers and Medical Officers of Health) in their role responsibilities – apart from their specific use of NDMS – including with respect to the collection of information from cases and contacts
- Ministry of Health sharing of information with international partners under agreements and legislation
- The details of contractual arrangements with PHF Science

Appendices & Supporting Documents

Appendices	Information
Appendix 1	Finders Service
Appendix 2	Exposure Events
Appendix 3	NDMS Terms of Use (updated 19 Nov 2024)
Appendix 4	Summary of NDMS-relevant Mandated Collection in the Health Act 1956
Supporting Document 1	Privacy Statement – Phone Scripts (updated 20 August 2025)
Supporting Document 2	Privacy Statement – Full (updated 18 August2025)
Supporting Document 3	NDMS ATO (9/05/2025)

Glossary

Term	Definition
AIR	Aotearoa Immunisation Register
AWS	Amazon Web Services
Case	A person who has an infectious, notifiable, or communicable disease and symptoms meet the case definition
Contact	Any person who has been exposed to an infectious disease where there was a risk of infection
CPIR	Consumer Population Identification and Registration Service
CCS	Care Coordination System
DLN	Direct Laboratory Notification – an automated process whereby test results are sent from Community/Hospital labs to NDMS
EpiSurv	Repository for data to be used for public health surveillance (managed by PHF Science)
HNZ	Health New Zealand | Te Whatu Ora
HP	Health Practitioner
NCTS	National Contact Tracing Solution
NDMS	Notifiable Disease Management System
NZTD	New Zealand Traveller Declaration
NES	National Enrolment Service
NHI	National Health Identifier
NPHS	National Public Health Service
OPC	Office of the Privacy Commissioner

Personal/Health Information	Personal information refers to any details that can identify a living individual. It does not need to be sensitive or private. The information could identify an individual without necessarily naming them directly. If there is a reasonable chance a person could be identified, including where it is combined with other information, it can still be personal information for the purposes of the Privacy Act 2020. Health information is a subset of personal information. Examples of Personal and Health information (not an exhaustive list) – name, address, phone number, age, date of birth, employee record, scan, test result, photo, biometrics, NHI number, Driver's License, IP Address.
PHF Science	New Zealand Institute for Public Health and Forensic Science (formerly ESR)
PHS	Public Health Service
PIA	Privacy Impact Assessment
PMS	Patient Management System
STI	Sexually Transmitted Infection
TJI	Traveller Journey Index

Personal and/or Health Information Involved

Please list **all** personal and/or health information that will be collected, used, stored or released with this initiative. Refer to Glossary for the definition of what Personal/Health Information is.

The Privacy Act 2020 applies when any personal information, that is not health information, is handled.
The Health Information Privacy Code 2020 applies when health information is handled.

SOURCE – for the purposes of the following table, to provide clarity please note:

Individual	the case or contact to whom the record relates or their lawful representative (unless their Guardian).
Guardian	a parent or guardian, of a child aged under 16 years to whom the record relates.
Third party	a person, who is not authorised to act on the individual's behalf, providing information about another person, to a contact tracer, such as a case providing details of contacts or an individual in relation to a service (e.g. place of work, school).
Reporter	person who has notified the Case, usually the individual's GP or other medial practitioner.
System	HNZ system (e.g. NHI) or associated Lab system.

The legal basis for collecting this information is to carry out disease management and contact tracing measures. **Some information** collection is **mandatory under legislation** (see Heath Act 1956, Part 3 and Schedule 3 of the Health (Infectious and Notifiable Diseases) Regulations 2016). See Appendix 4 for a summary of key sections of the legislation.

List of Information Involved in NDMS	Source	Why this information is needed
Individual – Case		
Personal Details		
First/Last/Preferred Name	Individual, guardian, system (NHI, Lab), reporter	Identification
NHI	System (NHI, Lab, PMS), reporter	Identification, access health history to identify risk factors, link with other health systems
Date of birth	System (NHI, Lab), individual, guardian, reporter	Identification and to identify any clinical/public health risk factors for disease
Gender		
Ethnicity (including Iwi)		
Person with disabilities and disability details	Individual, guardian, representative, system (PMS)	Identify any clinical/public health risk factors for disease and provide information in an accessible format
Phone number	Individual, guardian, system (PMS, Lab)	Communication (Case follow up)
Email	Individual, guardian, third party	
NHI Address	NHI	
Current Address	Individual, guardian, third party	

Notification Address	System (Lab), Reporter	Communication with Case and assist with identifying possible Contacts
Guardian and Spokesperson Details		
Guardian/Spokesperson First Name and Last Name	Individual, guardian, third party, system (PMS)	Case follow up
Guardian/Spokesperson Phone		
Guardian/Spokesperson Email		
Occupation details		
Primary occupation and Work/Organisation Name	Individual, guardian, third party, reporter	To identify any clinical / public health risk factors for disease and identify any potential contacts
Work or Organisation Contact Name, Phone, Address, Email and Role		To support contact tracing, communication
GP Details		
Usual Doctor, Practice Name, Address and Phone	Individual, guardian, system (PMS, NES)	Liaise with GP and confirm public health action taken
Support & Welfare Needs		
Support Required and details	Individual, guardian	Enable case to comply with public health action e.g. isolate
Clinical Outcome		
Hospitalised	Individual, guardian, system (PMS, Regional Clinical Systems, Lab System, reporter	Health monitoring, context for public health follow up
Date Hospitalised		
Hospital Name		
Date Discharged		
Deceased		
Was This Disease Primary Cause of Death? If No, Specify Cause		
Date of Death		
Case information		
Disease type	System (Lab), reporter	Context for public health follow up
Case classification (e.g. Under investigation, Probable, Confirmed, Not a Case)		
Date reported		Calculate isolation period/public health action period

Symptoms & Underlying Conditions		
Symptoms and details of onset	Individual, guardian, reporter	Health monitoring, context for public health follow up and identify any clinical risk factors
Pregnant/Pregnancy Trimester		
Medication		
Other Underlying Conditions		
Low Immunity		
Lab Confirmation Details		
Lab Confirmation Status	System (Lab)	Case and contact follow up and surveillance
Lab Confirmation Date		
Immunisation Details		
Details of vaccination status	Individual, guardian, third party, system (AIR)	Verify immunity and need for public health action
Disease Source		
Source type (imported/import-related/endemic)	Individual, guardian	Identify source and map spread of disease. Support public health follow up and contact tracing
Region/City Imported From		
Country Imported From		
Contact with Confirmed Case		
Details of any confirmed case Individual has been in contact with including: Full Name, Age or Date of Birth, Contact Date, Contact Location, Phone, Email, possible exposure locations	Individual, guardian	Identify source and support public health follow up and contact tracing, surveillance
Domestic Travel		
Been in NZ Locations with Outbreak	Individual, guardian	Identify source and map spread of disease. Support public health follow up and contact tracing
NZ Outbreak Location Details		
Other Potential Exposure Locations		
Overseas Travel		
Details of any travel overseas, including when they arrived in NZ and the last country(ies) they visited whilst overseas	Individual, guardian	Identify source and spread of disease. Support public health follow up and contact tracing
Individual – Contact		
Personal Details		
First, Last and Preferred Names	Individual, guardian, third party, system (NHI)	Identification, enable public health to follow up, identify clinical/public health risk factors for disease, communication,
NHI		
Date of Birth and Age		
Gender		
Ethnicity (including Iwi)		

Person with Disabilities and disability details		provide information in an accessible format, contact tracing follow up
Phone, email and address	Individual, guardian, third party	
Guardian and Spokesperson Details		
Name, relationship to Disease Contact, Phone and Email	Individual, guardian, system (PMS)	To enable contact investigation and follow up
Occupation Details		
Primary occupation and Work/Organisation Name	Individual, guardian	To identify any clinical / public health risk factors for disease and identify any other potential contacts
Work or Organisation Contact Name, Phone, Address, Email and Role		To support contact tracing, communication
GP Details		
Usual Doctor, Practice Name, Address and Phone	Individual, guardian, third party, system (PMS, NES)	To liaise with GP and confirm public health action taken
Exposure Details		
Details of Exposure	Individual, guardian	To support contact tracing and source investigation
Details of Others at Event		
Support and Welfare Needs		
Support required, Support details	Individual, guardian	To support contact management
Immunisation details		
Details of vaccination status	Individual, guardian, system (AIR)	Verify immunity and need for public health action
Symptoms & underlying conditions		
Symptoms and details of onset	Individual, guardian	Health monitoring, context for public health follow up and identify any clinical risk factors
Pregnant/Pregnancy Trimester		
Medication		
Other Underlying Conditions		
Low Immunity		
Household members		
Name, age, status	Individual, guardian	To support contact management and further contact identification

NZTD Individual Information (only if required)*		
Passport Number	System (TJI)	Identification
Contact ID		Identification, to assess the appropriate public health service for follow-up, provide contact information, and to prioritise individuals with occupations or travel history of higher risk.
NZTD completed for own travel (yes/no)		
NZTD completed on behalf (yes/no)		
Name and Email address of Authorised representative		
Preferred Name		
Name as shown on Passport		
Surname/Family Name as shown on Passport		
Email Address		
Phone Number		
Date of Birth		
Date of Arrival into NZ		
Flight Number / Vessel Name		
Departing from (Port)		
Date and Time of Departure		
Arriving into (Port)		
Contact or Residential Address in New Zealand		
Occupation/job		
In which country last lived for 12 months or more		

* This information is currently sourced manually. The same or similar information may be sourced through direct access to the Custom's TJI database under future plans (see page 3).

Principle 1:
Lawful purpose and necessary collection

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 state the lawful purpose for the collection of this personal information
Information collected for NDMS is required and necessary to undertake case and contact management activities, source investigation activities and for the effective management, including surveillance, of infectious diseases in accordance with Part 3A of the Health Act 1956. Details in relation to Contact Tracing are outlined in subpart 5, noting: 92ZY **Purpose of contact tracing** The purpose of contact tracing is to obtain information about the contacts of persons with infectious diseases or suspected of having infectious diseases in order to— ▪ identify the source of the infectious disease or suspected infectious disease: ▪ make the contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary: ▪ limit the transmission of the infectious disease or suspected 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		
Not Applicable		

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 "**No**", please answer the questions in this section

Please state why you're not collecting information directly from the individual

Information pertaining to NDMS may be collected from multiple sources, as well as the individual concerned (See Personal and/or Health Information Involved in Summary for full details). This collection from other sources is essential to identify cases and contacts, and to conduct necessary investigations to mitigate the risks posed by the disease.

Source and Reason for Collection:

Community Laboratories: By law, all positive test results for a notifiable infectious disease must be sent directly from the lab to PHF Science (if conducted by a non-PHF Science lab) where it is automatically sent through to NDMS to as a Case notification. This transfer of information is by way of a Direct Laboratory Notification (DLN). Section 74AA and 74B of the Health Act require reporting of all Cases where a person 'is, has been, or may be or have been, infected with a notifiable disease'.

Health Practitioner: Health practitioners are required by Section 74 of the Health Act 1956 to report to the Medical Officer of Health any patient they have 'reasonable suspicion' is suffering from a notifiable disease. This may include cases still under suspicion (e.g. measles) or can only be clinically diagnosed (e.g. rheumatic fever). This information is added in to NDMS.

Additional Laboratory Information: Where Cases require further testing once they have been notified through a DLN, not all results will feedback to NDMS via PHF Science. For example, some diseases require genotyping to determine the severity of the strain or correct course of treatment for that disease. In instances where these test results are ordered by the Case's GP or medical professional (i.e. not a Medical Officer of Health), the test result may only be sent back to the test requestor. This means that NDMS Users will have to seek out the lab results to build a full profile of the Case and inform public health action.

Case: A Case may be asked for additional information to investigate possible sources of the disease and/or to identify other persons who may have been potentially exposed to a disease. Information requested about the Contact may consist of their name, age, sex, address and other contact details. This is initiated on a voluntary response basis, although there are legislative obligations in section 92ZZC of the Health Act if required.

Parent/Guardian/Authorised Representative: Section 92ZZC (5) enables a contact tracer to collect information that may be required from a parent/guardian or authorised representative where a Case or Contact is too young or unable to provide the necessary information themselves.

Health New Zealand Personnel: Information may be collected through the provision of healthcare services provided to a Case/Contact, or in the context of a Medical Officer of Health when notifying under suspicion, who would be adding information to NDMS such as symptoms and underlying conditions.

Primary care and Regional Clinical Systems: Where clinical information has not been provided by an individual or laboratory, Information may be requested from primary care and hospital systems on an individual lookup basis to ensure the correct public health action is taken.

NHI & NES: used to obtain current contact details and administrative data of a Case and/or Contact if necessary.

Aotearoa Immunisation Register: Used to verify immunisation status of an individual

Agencies/Organisations (Government or Private): Information may be requested from other government databases (where MoUs exist – see Summary above) in pursuit of locating difficult to contact individuals, or from other agencies (e.g. private businesses, employer, community groups and education institution).

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 the privacy team.

Health Act 1956 – Part 3A, subpart 5 – addresses the collection of personal information for contact tracing and source investigation, and specifically outlines the procedures and legal requirements for obtaining personal information necessary for managing infectious diseases.

Noting, persons referred to in subsection(2) of 92ZZF (third parties such as businesses or other organisations) must provide information in response to a request made under subsection (1) despite anything in the Privacy Act 2020. As above, Section 92ZZC (5) enables a contact tracer to collect information from a parent, guardian, legal representative or person in charge of an individual who lacks legal capacity.

However, prior to invoking legislative authorisation and the fact that compliance to Principle/Rule 2 could prejudice the safety of a Case and/or Contact, where compliance is not reasonably practicable in urgent circumstances of needing to prevent the spread of infectious disease:

Privacy Act 2020 – Rule 2: Source of Information

(2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—
  (e) that non-compliance is necessary—
    (v) to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual

Health Information Privacy Code – Rule 2: Source of Information

(2) It is not necessary for a health agency to comply with subrule (1) if the agency believes, on reasonable grounds,—
  (c) that compliance would—
    (iii) prejudice the health or safety of any individual; or
  (d) that compliance is not reasonably practicable in the circumstances of the particular case.

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?*
Privacy Statement – Phone Scripts PHS staff (and contracted staff) are provided with a short privacy script which will be read to an individual when they are first contacted if they are a suspect/confirmed Case or Contact. The Script is reflective of the requirement of respect for individuals (s92C of the Health Act) and voluntary compliance is obtained where possible (s92D of the Health Act). See Supporting Document 1: Privacy Statements – Phone Scripts (updated 19 Aug 2025) **Privacy Statement – Full** The current Privacy Statement (last updated 19 Aug 2025) has been updated to include sufficient information to meet requirements as set out in Principle 3 and the upcoming changes to Principle 3A. See Supporting Document 2: Privacy Statements – Full (updated 19 Aug 2025). As part of this PIA review, the privacy statement has been updated to provide additional details about information sourced from third parties. This is intended – as a future proofing measure – to practicably meet the requirements of the expected new Information Privacy Principal (IPP) 3A, which will normally require notification of indirect collection of information about a person [to that person], and is expected to come into effect from 1 May 2026. This update reflects a commitment to transparency around the collection of NDMS data. It is acknowledged that IPP3A is not yet law, and additional information – including internal HNZ guidance around compliance – may require a change in approach. This will be considered if required at a future point.
Where will the document be made accessible? *For example, will it be published online? Link in an email? Hard copy?*
The Full Privacy Statement is available on NDMS dedicated page of Te Whatu Ora website: Notifiable Disease Management System (NDMS) – Health New Zealand | Te Whatu Ora Printed copies of the Full Privacy Statement may also be provided to individuals during the course of an investigation.
Please include as an **appendix** a copy of any draft document that outlines how you will collect and handle 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?
Phone – the short privacy script will be read to an individual before any information is collected. Full – available before, during and after information is collected.

C. Mandatory or voluntary collection

Please state whether the collection of information is voluntary or mandatory?
Any person exercising powers or duties under Part 3A of the Health Act, relating to the management of infectious disease must take into account the principles set out in section 92C to 92H of the Health Act, including enabling an individual to voluntarily comply with measures before further adverse actions are taken. Under Part 3A of the Health Act, a **contract tracer** may require an individual to provide certain information to the contract tracer if the purposes of contract tracing under s 92ZY is likely to be achieved by doing so. Before requiring information from an individual, a contract tracer must consider whether it would be appropriate for the individual to undertake contact tracing, before requiring the individual to provide that information to the contact tracer. A **contact tracer** may *require*: • a **case or suspected case** to provide information about people they have been in contact with (covering: name, age, sex, address and other contact details, or any other information required by regulations made under the Health Act) and the circumstances in which they believe they may have contracted or transmitted the infectious disease (See Health Act s92ZZC) • a **specified person (which may include a specified organisation)** to provide the names and addresses of the contacts of a case or suspected case (see Health Act s92ZZF) While not normally expected to occur in practice (as most information collection will be handled under contact tracing provisions as above), for completeness it is noted that a Medical Officer of Health may make directions requiring relevant information for the effective management of infectious diseases to be provided (see sections 92I(9) and 92J(9)). A District Court may also make Public Health Orders which could, theoretically, cover information provision (see Subpart 3 and particularly 92ZA(1)). Provision of information not specifically covered by legislation or under a legitimate and appropriate direction [by a Medical Officer of Health] or Public Health Order, is **not** mandatory to provide.
Please state to what extent, if any, the individual can opt out of providing some or all their information
Where an individual is required to provide information under Part 3A of the Health Act that is lawfully requested (i.e. the relevant requirement of the legislation has been complied with) an individual cannot *opt out* of providing some or all of that information. (For completeness: an individual can appeal a direction made by a Medical Officer of Health under s92T. Public Health Orders may be cancelled or varied by the District Court (section 92ZR) or appealed to higher courts under section 92ZT or 92ZU.) An individual who is asked to provide non-mandatory information may opt out of providing this information.
Please state what happens if the individual does not want to disclose their information?
Where information is lawfully requested under Part 3A of the Health Act, and an individual either fails to provide the information without lawful excuse OR intentionally omits information OR gives information they know to be false, an individual could be liable upon conviction to financial penalties up $2000 and – in relation to Public Health Orders, imprisonment up to 6 months. See in particular sections 92V, 92ZW and 92ZZH.

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?
Under current legislative requirements, this is not applicable. Any person from whom information is collected directly (about them or someone they legally represent) will be directed to the privacy statement.

Anticipating IPP3A (see above) there are likely to be some individuals captured by NDMS who cannot be contacted, or who do not need to be contacted and whose records may be held potentially for only a short time (e.g. information on travellers on flights provided through NZ Customs). In those circumstances it is anticipated HNZ would rely on non-practicality and non-prejudice exceptions. However, this may be considered further once IPP3A is in effect and clearer guidance on compliance is available.

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

Not applicable under current legislation but see above anticipating IPP3A.

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

When communicating with a Case, Contact or organisation identified as associated with a notifiable disease, the approach is to first seek cooperation from individuals, and only use compulsion provisions under the Health Act if necessary. This is particularly important when working directly with individual Cases to identify Contacts, as it will enhance public trust, in working towards a common goal – rather than appearing punitive. A more open dialogue is likely to be created potentially generating more useful information if people can be engaged to participate willingly in the Contact Tracing process.

A third-party may want the comfort of legislative protection (for example a request under s92ZZF of the Health Act) if they are to release personal information.

These variables have been included in the training materials for NDMS Users.

The collection of information itself is lawful with its general population health focus. Contact with individuals is expected to be managed in accordance with legislative processes.

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?

For a person under 16, or lacking legal capacity the Contact Tracer may require information from a legal guardian or legal representatives (section 92ZZC(5)). This would ensure that support would be available for a young person, or other individuals who may require assistance, in the event that they were required to be involved in the Contact Tracing process.

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
PHSs have localised processes and networks that account for cultural considerations when contact tracing, and outreach services which may assist in individual Cases to encourage contribution of information in a setting that may be more comfortable or acceptable to the Case or Contact. This may include specialised language or cultural assistance and, if necessary, meeting with the individual. Outreach services' case and contact management processes are expected to use interpreters where necessary in line with organisational policies. For Medical Officers of Health, cultural safety is a core component of both training and recertification (obtained through continuing professional development). In addition, NDMS Users will have completed all mandatory HNZ cultural competency training as appropriate for their role and function.

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

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.	☒	☐
NDMS is a platform operated within a HNZ instance of Salesforce (a customer service and case management Software as a Service (Saas)), hosted by Amazon Web Services (AWS).		

Engaging with Information Security

	YES	NO
Have you engaged your relevant information security team for this project/solution?	☒	☐
Has the relevant information security team given its approval for this Project? *If the answer is "yes", please provide a copy of this approval to HNZ Privacy*	☒	☐
Refer to Supporting Document 3: NDMS ATO (9/05/2025)		

Storage

Please describe the system and location where the information is stored?
Live NDMS data is stored in NDMS in an HNZ Instance of Salesforce, hosted by AWS (Sydney). Data will also be exported to the NPHS data warehouse instance of Snowflake at set intervals for reporting and surveillance (to be covered in a separate privacy assessment) and potentially for archiving and secure storage of non-active information (see comments in the Access subsection below).

Access

Please state the roles that will have access to the personal information

The following table covers the roles with access to NDMS and the reasons for access. See also information on access controls below. At the time of writing approximately 400 users have authorised access.

Internal HNZ access:

Roles/Team	Why access required
National Investigation Service	• Build Reports • Create List views and dashboards • Finders Service (locating hard to reach contacts)
Local, regional and national NPHS case investigators and managers (e.g. Medical Officers of Health, Health Protection Officer's, Public Health Nurses, and Contact Tracers)	• Case investigation • Contract tracing • Case and Contact management • Cluster management • Oversee Case and Contact management
National Clinical Team	• Coordinate national outbreak response
National Public Health Emergency Response Team	• Conduct response management and coordination for inter-regional outbreak
Analysts	• Operational data analytics and surveillance • Support National Focal Point notifications
System Administrators/Managers	• Maintenance, support for NDMS System

External access:

Agency – PHF Science	Purpose for Access
EpiSurv Coordinators Public Health Medicine Specialists	In line with contract for services by Ministry of Health: • Surveillance • Data quality • Outbreak response

Please describe why these roles need access to the personal information

See tables above.

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)

Extensive consideration has been given to User access and ongoing use of NDMS, with a NDMS User Framework developed. The following outlines details from that framework.

Roles and Responsibilities

DIRECTOR PROTECTION

- Overall accountability for access to NDMS
- Overall accountability for the stewardship of data in NDMS

- Responsible for decision on granting access to NDMS to additional service providers and/or agencies (outside of NPHS) including
  - scope of access
  - criteria that must be met by service providers, agencies and their Users, and
  - who can mandate individual *User* access and/or *User Approvers* (individuals with the authority to approve *Users* with access to NDMS)

REGIONAL KAITĀTAKI HEALTH PROTECTION

- Accountable for mandating *User Approvers* within their Regional Directorate or as specifically authorised by the Director Protection
- Accountable for ensuring that *User Approvers* and *Users* meet and maintain the criteria for access
- Responsible for approving or delegating approval of information request disclosures to individuals.

PROTECTION DIGITAL TEAM AND COMMUNICABLE DISEASE OPERATIONS MANAGER, PROTECTION

- Responsible for mandating *Users* and/or *User Approvers* from:
  - NPHS National directorates
  - Digital Services
  - Other service providers or agencies where specifically authorised by the Director Protection
- Responsible for ensuring that *Users* have met the criteria for access
- Responsible for maintaining oversight of the *Users* within their approval scope
- Ensures that *Users* are removed from NDMS as necessary
- Responsible for approving information request disclosures to individuals

User Approvers – Responsibilities, Criteria and Onboarding

Responsibilities	Criteria to be mandated as a *User Approver*
• Responsible for approving *Users* • Responsible for approving changes to *User* permissions within their designated scope • Responsible for ensuring that *Users* have met the criteria for access as outlined below • Responsible for maintaining oversight of the *Users* within their approval scope • Ensures that *Users* are removed from NDMS when they no longer require access e.g. they change roles or leave Te Whatu Ora • Responsible for notifying all privacy breaches through standard channels and to the national Communicable Disease Manager Note: *User Approvers* cannot approve their own access to NDMS and are not granted access by default.	• Is approved by regional Kaitātaki Health Protection or National Communicable Disease Manager with a specific scope • Uses their organisational email address • Accepts responsibility and accountability for maintaining user access according to User Access criteria

A process has been developed to mandate User Approvers that ensures each User Approver understands their responsibilities as well as the criteria they and all other NDMS Users must meet. As stated above, Kaitātaki Health Protection, the Protection Digital Team and the Communicable Disease Operations Manager are accountable for mandating User Approvers. This process is detailed in an internal User Approval Framework.

NDMS Support Desk adds *User Approver* to an internal list and informs *User Approver* and Kaitātaki Health Protection, Protection Digital Team or Communicable Disease Operations Manager of resolution.

User – Responsibilities, Criteria and Onboarding

Responsibilities	Criteria to be granted access to NDMS
Responsible for: • Accepting and adhering to NDMS Terms of Use • Adhering to the Privacy Act 2020 and the Health Information Privacy Code 2020 • Complying with their organisation's Information Security and Acceptable Use Policy • Taking all reasonable safeguards to protect health information • Ensuring they only look at health information needed to perform their role • Using NDMS for case and contact management, or reporting • Not sharing system access with another individual • Reporting all actual and suspected privacy breaches to a NDMS *User Approver* • Ensuring they stay up to date with their obligations as Users and ensuring that they are a steward for information within the system	All *Users* must meet these criteria to be granted access to NDMS: • Understands their responsibilities as a User of NDMS • Has a legitimate business reason to have access to the system • People undertaking contact tracing activities will have met the criteria outlined in the Health Act 1956 section 92ZZA • Actively requires access to identifiable case and contact information associated with notifiable diseases • Uses their organisational email address • Where the User is not an Employee or direct contractor of HNZ, the *User Approver* acknowledges that the *User's* organisation's 'Information Security and Acceptable Use Policy' is materially similar to Te Whatu Ora's • Have an awareness of Te Mana Raraunga Te Kāhui Raraunga – Māori Data Governance Model • Completes and maintains their NDMS training in a timely manner • Has completed 'Privacy of Personal Information' training or the appropriate organisational equivalent • Has completed training around ethnicity data collection and recording

Terms of Use

NDMS Users must accept the Terms of Use (see Appendix 3) prior to accessing the system. This acceptance is required for the initial log in which must be reaccepted every 3 months, when a User changes their password, or when the Terms of Use has been updated. Minor updates have been made to strengthen the Terms of Use as part of the version 3 PIA update (August 2025).

Onboarding

To be onboarded to NDMS, a User Approver and a User:

Either self identifies, or is identified as needing access to NDMS

Has their criteria for access checked (by an allocated higher tier role), with additional information to support access collected (i.e. confirmation/evidence of training completed)

Access request is processed via a dedicated support desk, which may be subject to an additional internal approval process.

Once access has been processed, communications between the support desk, allocated higher tier role and the User/Approver will confirm the arrangement.

External Agency Access to NDMS – Onboarding

Access to NDMS for users outside of HNZ is strictly controlled, with requests for access based on a clear and appropriate business need and lawful purpose to access the information.

A 'pre-approved external agencies list' and their authorised Users is maintained by the Business Owner of the system. Only the DIRECTOR PROTECTION can authorise an external agency to be added to this list. The approval shall identify who is delegated to approve individual Users (National Communicable Disease Manager, Regional Kaitātaki or a designated person within the agency).

Limitations may be placed on an external agency NDMS User such as duration of access, scope of access, and the type of access granted (permission).

External Users are subject to the same or similar criteria as an HNZ User, with oversight of these Users being the responsibility of the User Approver.

At the time of this review, PHF Science is the only external agency with access. Work has been carried out to ensure PHF Science access is consistent with the new Government Standard for providing non-government third parties with access to, or collection of, government-held personal information (introduced July 2025) and HNZ requirements introduced in relation to this. As part of an agreed Information Sharing Agreement, PHF Science also have responsibilities to ensure that their users of NDMS are appropriately informed of their obligations under the sharing agreement, are appropriately trained and their list of users is kept, regularly reviewed and can be requested by Health New Zealand where reasonably necessary.

If other agencies (for example Reach Aotearoa) are contracted to undertake work associated with NDMS (i.e. Contact Tracing in an outbreak) it is expected that they would be acting on HNZ's behalf and not have independent rights to data (i.e. an agency agreement). Contracts could address this at the time.

Access Permissions

At this time, access to NDMS records for authorised users is **not** limited. This means all users will have the ability to access all information about individuals, for all diseases regardless of where a user is located, or whether they are from an external agency (noting actual access is limited by Terms of Use – see Appendix 3). This was a considered and purposeful decision by the NPHS.

EpiSurv limits the ability to share case and contact information, which greatly limits the ability for NPHS to work as one national service. With NDMS allowing access to all information, for all Users, the system enables adaptability. This is especially important due to the frequency with which cases and contacts move to different parts of the country during their period of contact with Public Health. Having the ability within the system to delegate and reassign cases and contacts is a critical function needed for seamless delivery.

This system is appropriate for the limited diseases originally included within NDMS (COVID-19 and measles). However, with the expansion of NDMS to cover a significantly greater number of diseases, some of which have higher sensitivities,[1] consideration will need to be given as to whether open access for authorised users is a sufficient security safeguard for all diseases in this new context.

Users are already prohibited under Terms of Use from accessing records which are not relevant to their role, and access to records is auditable. Nonetheless, access controls to limit users to those strictly requiring access, at least for more highly sensitive diseases, may need to be scoped, considered and/or implemented. This is noted as a planned action in the Risks and Controls section of this PIA.

At present, there are five access permissions that can be granted to NDMS Users. The permission(s) granted are based on the requirements of a role to fulfil their duties.

[1] An initial and provisional Privacy and Clinical review identified the following diseases as of high sensitivity: Hepatitis A; Hepatitis B; Hepatitis C; Hepatitis (viral) not otherwise specified; Leprosy; Mpox; Tuberculosis.

General Access Permissions:

- Read only – users can only see data related to Cases, Disease Contacts, Exposure Events, and Exposures.
- Edit – users can edit data related to Cases, Disease Contacts, Exposure Events, and Exposures.

Optional Access Permissions

- Report creation – users can create private and public reports and can modify private reports or reports within their team folder.
- Dashboard creation – users can create private and public dashboards and can modify private dashboards or dashboards within their team folder.
- Bulk Import of Disease Contacts – permission to use automated creation of Disease Contacts.

As discussed elsewhere in this PIA, additional permissions to enable export of data out of NDMS may also be enabled subsequently as an Optional Access Permission.

Offboarding

Offboarding will occur when:

- A User leaves HNZ – their access will be revoked via EntraID (automated IT process)
- A User has been inactive in the system for ninety days – access will be revoked (HNZ Salesforce Delivery Team process)
- A User's access is no longer necessary – determined and overseen by the Regional Kaitātaki, Protection Digital Team, National Communicable Diseases Operations Manager, or external agency.

It is additionally noted that – as per the User Approval Framework – external user accounts must be associated with their work email address, so if they leave their organisation and notification is inadvertently missed, they would cease to be able to access the NDMS.

Archiving of non-active records

NDMS is primarily relevant to the management of active infectious disease cases. The treatment of older, non-active NDMS case and contact records (which nonetheless may need to be retained to meet Public Record requirements or for analytical purposes) is still being worked through. However, given wide access to records as standard (see above), this will be considered with the intent to limit access to these records where practicable. Possible solutions may include:

- Archiving records outside of NDMS in a secure environment, such as the NPHS data warehouse Snowflake environment.
- Archiving records inside NDMS, with significantly restricted user access.

Development of an archiving approach is identified as an action in the Risks and Controls section of this PIA.

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**	**NA**
Salesforce operates two factor authentication systems which has been incorporated into NDMS	☒	☐	☐

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 conduct 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.

Security Information Event Management Solution

NDMS is monitored by a Security Information Event Management (**SIEM**) solution which operates 24/7. SIEM can detect malicious external and some account user behaviour. Examples include:

External Behaviour

- **Brute force attacks –** An attacker tries to login to a user account, trying hundreds of different passwords.
- **Credential stuffing –** An attacker uses stolen or leaked credentials to user accounts on other systems.
- **Password spraying attacks –** An attacker tries to login to a range of possible user accounts using some common passwords. E.g. Amanda's LinkedIn profile says she works on a specific system and the attacker tries Password123.
- **SQL injection –** Malicious code injection.
- **Data scraping/mining –** A user goes beyond a set threshold for the amount of rows they access. E.g. 50 000 records within 6 hours.

Account Behaviour

- **Impossible travel –** For example, if a User account logs in from two distinct geographical locations that they could not have physically travelled between. E.g. 11am in Wellington 11:30am in Auckland.
- **Deviation from baseline profile –** A user normally works 10am to 6pm and then suddenly logins at 7am, or midnight. When a user reads or writes above a certain number of records in a certain time period. Such as reading 50 000 records in an hour.
- **Data ingestion –** Only relevant (expected users) will be able to perform data ingestion into the platform – ingestion behaviour will be logged.
- **Local Logon/Break Glass Account Use –** Any use of NDMS Admin account.
- **Attempts to bypass access controls**
- **Login Attempt to disabled/now unauthorised User –** A disabled/now unauthorised User tries to login, or their account is used.

The HNZ Security Team will notify the Salesforce Platform Owner who then notify NDMS Business Owner and NDMS Platform Owner in the event of any NDMS SIEM alerts.

Manual Auditing/Monitoring

Salesforce has extensive User audit and monitoring capabilities that supplements, and operates in parallel to the SIEM solution, with logs capturing all accesses, records viewed and modifications. Audit information will be retained for 2 years.

As part of weekly checks, the HNZ Salesforce Delivery Team will deactivate Users who have been inactive for ninety days to ensure only personnel who require access have access to NDMS.

A formal and standard process is yet to be scoped and developed to monitor and identify misuse of the system. This is expected to include clarification of what constitutes misuse (beyond failure to adhere to Terms of Use) and strategies for manually reviewing actions and access. Based on preliminary discussions, and subject to confirmation, this may include specific consideration of:

- Records marked by users for audit, such as records about staff, high profile individuals, or relating to high profile cases
- Records accessed by a high number of Users

- Records accessed by possibly unexpected users, e.g. records in one region being accessed by staff in another region
- Downloads of information from NDMS (if enabled)
- Random spot checks

While the details of this are still being worked through, audit records may continue to be accessed as required to ensure compliance with Terms of Use and protection of privacy.

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 classification 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?*

Information stored within AWS is encrypted in transit and at rest.

Security classification of information: MEDICAL IN-CONFIDENCE

Regular backups of all information will be captured to permit recovery from a specified point. Recovery Point Objective for the Salesforce Platform is "Recovery point object (RPO). Failure of any system must not result in greater than a 5 minute period of data loss."

Backups and audit logs are stored in S3 buckets in the HNZ AWS tenancy.

Training

As well as specialised training for NDMS Users, all HNZ personnel are required to undertake mandatory online privacy and security training when they are initially onboarded to the organisations. Refresher training may also be completed annually, be provided on an ad hoc basis, specifically requested for departmental education sessions, grand rounds, or opportunistically (i.e. Cyber Uplift Programme exercises).

Downloading Information from NDMS

NDMS Users are not currently able to download production data from NDMS. However, this is limiting some Users from being able to effectively and efficiently play their role in managing notifiable diseases. It can also lead to workarounds which in addition to being more inefficient may have other privacy risks.

Identified example use cases include:

- bulk exporting contact details to enable multi-text functionality to alert people of their potential exposure to a notifiable disease, and
- exporting data sub-sets for operational management e.g. reviewing contacts for follow up in outbreak response meeting to support prioritisation and distribution of work.

While download capability is important to allow Users to carry out their work in an effective and efficient way, through removing data from the carefully controlled NDMS environment it does increase privacy risks. Details of data export functionality and processes are still being worked through, but privacy controls will be critical to ensure exported data is managed appropriately and privacy is protected. These might be expected to include:

- limiting functionality to a restricted User base via additional access permissions
- ability to audit data exports (i.e. if data is downloaded from NDMS, this will be captured in an audit log and downloads will be subject to appropriate regular audit)
- clearly authorised use cases, and
- simple documented guidance/requirements for Users who are granted the capability to download, outlining their responsibilities and requirements for ensuring downloaded data are well protected, particularly with reference to safe storage, retention and sharing.

Some enhancements to NDMS, particularly around integration with HNZ systems such as CPIR and AIR, have already addressed some potential use cases where downloading would previously have been required. As NDMS develops – and subject to resourcing and prioritisation – more functionality may be able to be incorporated which reduces or removes the need to export data out of the system.

System Administration Privacy and Security Training

Only HNZ staff will hold the role of System Administrator, but not all System Administrators will work in NDMS. While specific security and privacy training in relation to NDMS will not be provided to this group of personnel, they are required to complete HNZ Cybersecurity and HNZ Privacy training modules within their first 10 weeks of employment with HNZ.

Additionally, NDMS has a privacy incident response plan:

Escalation

There are two primary ways in which a privacy incident may get escalated:

1 By HNZ Security Operations Centre team if an alert is raised (via SIEMS)

2 By an NDMS User identifying, or being made aware of, an incident (via own accidental actions, or witnessed actions/concerns of others, e.g. advisement from Case/Contact that their information has been discovered where it should not be)

In order to respond as quickly as possible, a suspected or actual privacy breach is to be **IMMEDIATELY** notified to the following:

- The staff member's Manager (if applicable) and NDMS Product Owner and NDMS Platform
- HNZ Privacy – hnzprivacy@tewhatuora.govt.nz and
- HNZ Information Security at HNZInfoSec@health.govt.nz.

This escalation process is detailed in NDMS Terms of Use agreement and provided to HNZ teams who are directly involved with NDMS (i.e. NPHS, Data & Digital BA/Support Teams).

Breach Response Plan

Where a User detects or suspects there has been access, use, disclosure, alteration, loss or destruction of information without authorisation, they are required to immediately report the incident to NDMS Product Owner and NDMS Platform Owner. Users are also required to notify the HNZ Privacy (HNZPrivacy@tewhatuora.govt.nz) and HNZ Information Security (HNZInfoSec@health.govt.nz) immediately.

In accordance with privacy breach processes, NDMS Product Owner and NDMS Platform Owner will work with the Privacy Team to coordinate the response to any incident.

Consequences for Misuse/Non-compliance

Consequences for misuse are detailed in NDMS Terms of Use. Unacceptable usage, inappropriate searching of, or access to, information held within NDMS will be formally investigated.

Depending on circumstances, access to NDMS may be immediately removed, and the matter referred to the User's manager, or other legal action undertaken if appropriate.

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?*
The privacy statement for NDMS contains information for individuals on how they can access and correct information. HNZ also has general information about making access and correction requests. When requests for information are received, these will be forwarded to the applicable *Regional* (which ensures the personal information is kept localised as much as possible) Kaitātaki Health Protection person, who will coordinate the collection and release of information to the individual. These personnel are familiar with this process (i.e. validation of individual, or requestor has the authority to request, and ensuring only appropriate information is disclosed). When unsure, personnel processing these requests will contact the National Privacy Office for guidance. Instruction on how an Individual can initiate a request is included in the updated Full Privacy Statement
Please outline how you intend to ensure that it is possible to find the information about a specific individual?
Details such as a combination of First and Last Name, Address and Contact details, as well as use of NHI.

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?*
As with a Request for Information, requests for correction to information will be directed to the Regional Kaitātaki Health Protection person, who will assist in coordinating a correction, utilising the assistance of other appropriate and associated personnel where required.
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?
Details such as a combination of First and Last Name, Address and contact details, as well as use of NHI.
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?*
Where it is not agreed that NDMS information requires correction, an NDMS User will attach a statement of correction (in the form of a 'note') to the Case records of that individual. Where this disputed information is known to have been used elsewhere, the relevant area/agency will be informed of the statement of correction.

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?
Information will be sourced wherever possible directly from the individual concerned, and the information provided by that individual is expected to be accurate at that time. An individual could be a Case, Contact (or parent/guardian/authorised representative), a person associated with a Case or Contact (e.g. employer), or a person that has a location connection to a Case (e.g. event organiser). NDMS is integrated with several health information systems/databases which are considered the 'source of truth'. Relevant information is imported from these systems, into NDMS, to ensure that the information in NDMS is as accurate and up to date as possible (see Summary: Integration with Other Systems for a list of all connected systems). This information is deliberately 'point-in-time' information, as that is most relevant to NDMS decision making and the use of relevant data. It is therefore accurate and up-to-date *at a point in time.* It has been confirmed with clinical advisors that not alternatively or additionally holding live information does not pose a substantive risk to cases/contacts. Various functions/tools of NDMS are available to ensure that information is accurately captured such as self-completion forms (sent via CPIR) or in-built questionnaires for Contact Tracers to read as scripts during Case and Contact interviews. Steps undertaken to ensure information is accurate, up to date and complete: • Test results will come from an authoritative source (e.g. PHF Science/Community or Hospital laboratories). • If necessary, the Finders Services will assist with checking accuracy of contact and identification details as required. If a contact number is found to be invalid or belongs to someone else, this information will remain in NDMS record but noted as an invalid number. • When Cases and Contacts are contacted, their contact details will be confirmed and updated in NDMS if needed. • Incorrect/inaccurate information may be received from individuals – this will be managed as much as possible by Contact Tracers who will follow up ambiguities or errors where identified. • It is acknowledged that people could be incorrectly identified – the involvement of personal contact from Contact Tracers is designed to minimise the opportunity of this happening by communicating directly with the individual concerned and checking details with them.

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. Once those other legislative requirements for retention have been met, then the information should be disposed of when it is no longer needed.

Please state how long the information will be held by Health NZ

Based on previous decisions regarding Covid-19 contact tracing data and consultation with HNZ Information Management, the following disposal classes, actions, and retention periods apply to NDMS information collected from individuals. The records of individuals who **tested positive** are covered by two different disposal classes (FDA01.01.01 and FDA01.01.02). The details of others (i.e. those who **do not have a confirmed positive result**) are covered under FDA.03.04.04.

DA707 FDA01.01.01	DA707 FDA01.01.02	DA707 FDA03.04.04
Those that are over 16 years of age, must be retained for a **minimum of 10 years** from date of last action or a minimum of 10 years after death, before the information is either discharged or destroyed.	Those that are 16 years and under, must be retained for a **minimum of 25 years** from date of last action or a minimum of 10 years after death, whichever is longer, before the information is either discharged or destroyed.	Individual's contact details that do not fall into either of these categories must be retained for a **minimum of 2 years** or until administratively no longer required, whichever is longer, and then destroyed.

Duplicated Information in NDMS
Copies of information held in other systems (i.e. AIR) meet Archives NZ General Disposal Authority 7 class 1.3. Copies or duplicates of records, in the same or different format to the original, that have been created, published or distributed and used for convenience and reference purposes can be destroyed when the material is not required, or is no longer actively used and referred to.

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.

- Public Records Act 2005
- Disposal Authority 707 Functional Disposal Authority (DA707 FDAs)
- Archives NZ General Disposal Authority 7 Facilitative, transitory, and/or short-term value records (GDA7)

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)*

As per above, records are required to be retained under Public Records Act requirements. As these form part of the patient file, this requires retention of identifying details.

An analytical data set is also expected to be retained in the NPHS data warehouse, comprising at least some of the data in the NDMS. Subject to further assessment, it is expected this will be deidentified (individual details are not expected to be required for analytical purposes). Note that identity details may be masked rather than removed from these data.

Please state:
- how the information will be disposed of
- who is responsible for ensuring disposal occurs

Information and data will be disposed of in line with HNZ information and records management policy and disposal processes. The processes and mechanisms for this are still under development. For completeness, this is noted as a Risk in the Risks and Controls Table of this PIA.

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.

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.

There are specific legislative limitations on how infectious disease information collected under Part 3A of the Health Act ('Management of infectious diseases') can be used:

- Information collected by a Contact Tracer must not be used or disclosed except for the effective management of infectious diseases (section 92ZZG).
- Information collected under a direction (e.g. from a Medical Officer of Health) must not be used or disclosed except for the effective management of infectious diseases.

Note: these do not limit an individual's right to access or disclose information about themselves.

The authorised uses of information in NDMS are as follows:

- Management and surveillance of the infectious disease in accordance with Part 3A of the Health Act, including 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 communicate with contacts (to make the contacts aware that they too may be infected, thereby encouraging them to seek testing and treatment if necessary – s92ZY(b))
  - To limit the transmission of the infectious disease or suspected infectious disease – s92ZY(c).
- Reporting and statistical analysis to support management objectives in relation to infectious diseases

Nothing in this list limits auditing activity to ensure the security of, and appropriate access to, records, nor quality improvement processes for ensuring the accuracy and completeness of data.

Research purposes are not identified as an authorised use in this PIA but may be considered further for NDMS data ingested into Snowflake. Any such use – if authorised – would need to be subject to appropriate approval processes, including ethical approval where required, and consistent with legislative restrictions as above.

	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 the Privacy team.

Not applicable

	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.		
Matching Information: Multiple 'source of truth' databases and authoritative systems will be used by NDMS to ensure the most up to date and accurate details are acted on. These include NHI, NES, AIR and EpiSurv. Where it is discovered that these sources are inaccurate, NDMS will be updated, however the source system will not. This falls outside the definition of information matching in the Privacy Act. **Sharing Information:** Several Information Sharing Memorandums of Understanding (MoU) have been signed, the purpose of which are to aid the effective management of infectious diseases, where the requesting and disclosure of information between parties is necessary to prevent or lessen a serious threat to public health and safety, and potentially to the life and health of the individuals with, or exposed to, the disease. The following MoUs are currently in place relating specifically to contact tracing: • Air New Zealand (signed Sept 2024) • NZ Police (signed Oct 2024) • NZ Customs (signed Dec 2022, audit completed in 2024. Full review to be conducted when TJI direct access agreement finalised). Each of these documents sets out the information that will be shared and the controls in place to ensure that any information is used and managed in accordance with the law.		

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.

	YES	NO
Will the project disclose personal information to individuals or agencies outside of Health NZ?	☒	☐
If you answered 'Yes', please state the legal basis for disclosing personal information		
Health Act 1956 – Part 3A, subpart 5 – addresses the collection of personal information for contact tracing and source investigation, and specifically outlines the procedures and legal requirements for obtaining personal information necessary for managing infectious diseases. However, provided for clarity in regard to disclosing personal and health information during contact tracing, note s92ZZG – **Duty of confidentiality** (1) A Contact Tracer who approaches a contact under this Part or approaches a person under section 92ZZF must not, as far as practicable, disclose to the contact or that other person the identity of the individual who may have— (a) transmitted the infectious disease to the contact; or (b) exposed the contact to the risk of contracting the infectious disease. (2) Despite anything in the Privacy Act 2020, information provided or obtained by a Contact Tracer under this Part may not be used or disclosed by anyone except for the effective management of infectious diseases, but nothing in this section limits the right of an individual to access or disclose information about him or her under that Act or any other Act.		

A similar restriction to that under (2) above applies to information collected under Direction from a Medical Officer of Health.

Subject to those **critical restrictions**, disclosure relies on the following grounds under the Health Information Privacy Code, Rule 11. For information that is disclosed for the purposes of the effective management of infectious diseases:

- That the disclosure is one of the purposes in connection with which the information was obtained [1(c)]
- That the disclosure is directly related to one of the purposes in connection with which the information was obtained [2(a)]

Note: public health and safety grounds [2(d)] would also apply in many cases, as would disclosure being to the individual concerned or their representative [2(b)].

For disclosure of information that is not limited to infectious disease management use (that is information not collected by Contact Tracers or under directions, the following grounds may also apply to permit disclosure (other grounds not listed may apply on a case-by-case basis in unusual situations):

- Individual consent [1(b)]
- Deidentified, statistical or research use [2(c)] (where authorised – see comments about research use above).

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

Ministry of Health (disclosure via reporting from NDMS nominated personnel)
Health NZ will provide identifying information to the Ministry for National Focal Point reporting to sovereign nations in accordance with international agreements. De-identified information and notifiable disease data will also be provided to the Ministry for the purposes of meeting International Health Regulations (more detail in Principle 12).

Institute for Public Health and Forensic Science (PHF Science) (disclosure via direct access to NDMS)
As an Agent of the Ministry of Health contracted to support active surveillance and outbreak detection functions as well as critical quality control and system integrity functions (i.e. to ensure the data integrations are operating correctly).

NZ Police (via request by the Finders Service)
In rare circumstances where contact tracers have been unable to establish contact with cases or contacts, Health NZ will provide identifiable information to the Police for them to assist with identifying additional contact / location information for Contact Tracers to establish contact.

Air New Zealand (via request by the Finders Service)
Health NZ will disclose the minimum necessary information to obtain crew and passenger information to support contact tracing.

NZ Customs (via request by the Finders Service)
Currently, Finders Service will request details of the occupants and vessel a Case has been known to be travelling on (whilst infectious). The only personal information shared during this transaction may be the name, passport number and date of birth of a Case (or Contacts where known).

In the future, under the Information Sharing Agreement currently being drawn up with NZ Customs, Finders will be able to run a query through NDMS to access specific data from the Traveller Journey Index database using an individual's name, date of birth or vessel number and date of arrival.

Reporting to other government agencies (via legal reporting requirements)
Personal identifiable information may be disclosed to other agencies in accordance with legal reporting obligations (e.g. WorkSafe (see Section 199 of the Health and Safety at Work Act 2015), Ministry for Primary Industries (e.g. foodborne illnesses) and Ministry for Business, Innovation and Employment (e.g.

employment-related exposure) – see Communicable Disease Control Manual for further information on reporting for each disease).

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 NZ entity would; or
- B carries on business in NZ and is therefore subject to the Privacy Act 2020; or
- B's privacy laws offer comparable safeguards to the NZ Privacy Act 2020; or
- B is bound by contract or agreement to protect the information with similar safeguards to NZ 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 personal information be disclosed to a foreign person or entity?	☒	☐

- If you have answered "**Yes"**, please answer the following questions.

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?

While HNZ itself will not be disclosing information overseas, NDMS information will be provided to the Ministry of Health, which will then be disclosed by that agency for the following purposes:

- National Focal Point Reporting (identifiable information to other sovereign nations in accordance with international agreements)
- Compliance with International Health Regulations (de-identified death and notifiable disease data to the World Health Organisation)

New Zealand International Focal Point is advised when a Case or Contact has left New Zealand. The National Focal Point (NFP) is a function required in accordance with Article 44 (Collaboration and Assistance) of the International Health Regulations 2005 (IHR) to provide information to other countries. It acts as a formal single point of contact (receive/send) between countries and with the WHO to support management of all potentially serious events, such as the outbreak of a communicable disease.

- This information may include personal information, which is supplied in accordance with the International Health Regulations (IHR) 2005 and may be used or disclosed only for the purpose of assessing and managing a public health risk in accordance with and subject to the requirements of Article 45 of the IHR. The NFP is also used to provide official reports and updates to WHO.

While this information is noted for context, NDMS itself is not directly involved in overseas notifications and so this disclosure is not considered in scope of this PIA.

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 1 or more of its functions effectively.

To avoid doubt, Health NZ 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 IPP13(3) and Rule 13(5).

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

- If you have answered "**Yes"** to any one of these questions, please answer the following questions

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?

Used Unique Identifiers

National Health Index (NHI)
The NHI will be used to assist in the correct identification of individuals (i.e. avoid persons with a similar or identical name being mistakenly identified) and used to link with NES where needed to discover necessary contact details and engage with their GP if requested (not a standard part of NDMS processes).

If an NHI cannot initially be linked (as the identity of the individual is uncertain), the existing records on 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.

Health Provider Index (HPI)
The Health Provider Index is integrated with NDMS to allow the capturing of structured information on health organisations and practitioners so that NDMS Users can correlate practice/practitioner's information for analytics and reporting. It also provides Contract Tracers with an easy picklist of practitioners as opposed to free text typing practitioner details, minimising risk of error in information.

Passport Number
The passport number is the only source of independently verified legal identification available in NZTD and is useful in reliably confirming an individual's identity and when requesting further information from NZ Customs.

Provided for clarity – other Unique Numbers in NDMS, but not considered Unique Identifiers

PHF Science system generated numbers
While each test result holds an PHF Science assigned number to uniquely identify that test, recorded within NDMS, these will not be used as a unique identifier in their own right.

NDMS system generated numbers
NDMS will auto assign system generated numbers to each Case and/or Contact. This is not considered a unique identifier as it is onl3y used within the host system.

New Zealand Traveler Declaration (NZTD) – Contact ID
NZTD uses a unique identifier made for every new declaration that is created on the NZTD web and mobile applications. Travellers can create as many declarations as they like (even for the same travel journey), and each declaration is assigned a unique identifier. This will be supplied to the Traveller Journey Index via NDMS which allows Health NZ access only to the data required for a specific purpose and that Health NZ are legally authorised to access.

Artificial Intelligence Initial Assessment

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

Privacy Policies and Terms of Service (or other contractual provisions)

If the Project is engaging anyone outside of Health NZ to provide services as part of this Project, please answer the following questions:

Third Party Privacy Policy/Statement	YES	NO
Has the Project reviewed the current Privacy Policy/Statement of the third party?	☒	☐
Confirming a third-party provider's privacy policy aligns with HNZ has been included as part of the User criteria in the NDMS User Approval Framework. Data and Digital also have in place a defined process for contractors developing the system gaining access to the test and production environments.		
Terms of Service (or other contractual provisions)	**YES**	**NO**
Has the Project reviewed the relevant Privacy clauses in the Terms of Service (or other contractual provisions as applicable)?	☒	☐
Have you engaged HNZ Legal on a review of the relevant contractual provisions?	☐	☒
HNZ will only give permission to third-party providers once privacy clauses have been reviewed. This is part of the NDMS User Approval criteria for external agencies/providers. Data and Digital have in place a defined process for contractors developing the system gaining access to the test and production environments.		

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

Risk and Control Tables

This Privacy Impact Assessment has identified a number of privacy risks which have been recorded in the tables below. Only risks rated as Medium or High have been recorded.

The first table records **Privacy Risks with Outstanding Controls**, where controls are planned or in the process of having controls put in place to mitigate the risks identified. The Inherent risk rating reflects the level of risk should no control be put in place. The current risk rating reflects progress made towards reducing the risk through the controls described. The target risk rating provides a benchmark for the risk level achieved once all controls have been implemented. The summary of controls provides a brief overview of what controls are being put in place for that risk, further detail can be found in the **Summary of Privacy Controls** table.

The second risk table records **All Controls Implemented** where the target risk rating has been achieved. A summary of the controls that have been put in place to reduce risk have also been included.

For a full description of the controls summarised in each table, see the **Summary of Privacy Controls** table.

Privacy Risks with Outstanding Controls

Risk Ref No.	Description of Privacy Risk identified through PIA	Inherent Risk Rating	Current Risk Rating	Summary of Controls (Planned, in Progress or Implemented) Note: almost all controls listed as still to be implemented are partially implemented	Target Risk Rating
PR.01	**Risk/Source of Risk:** Inappropriate over collection of personal and/or health information by NDMS, because data fields in NDMS have not considered necessity of information, or the implications of sensitive diseases added to NDMS is not considered before these diseases go live in the system.	High (16) Probability: Likely Consequence: Moderate	Medium (11) Probability: Unlikely Consequence: Moderate	PC.01 – PIA Review/Update (Implemented to date) PC.02 – Governance	Medium (11) Probability: Unlikely Consequence: Moderate
PR.02	**Risk/Source of Risk**: An authorised User gains access to information not required for their role as there are insufficient access controls	High (16) Probability: Likely Consequence: Moderate	Medium (12) Probability: Possible Consequence: Moderate	PC.02 – Governance PC.05 – Role Based Access Controls PC.06 – User Approval PC.07 – NDMS Terms of Use (Implemented) PC.13 – Archiving PC.14 – Downloading Policy Controls	Medium (11) Probability: Unlikely Consequence: Moderate
PR.03	**Risk/Source of Risk**: An authorised User inappropriately accesses, misuses, steals, modifies, discloses, or otherwise mishandles information.	High (16) Probability: Likely Consequence: Moderate	Medium (12) Probability: Possible Consequence: Moderate	PC.02 – Governance PC.04 – Privacy Training (Implemented) PC.05 – Role Based Access Controls PC.06 – User Approval PC.07 – NDMS Terms of Use (Implemented) PC.08 – Audit Logs (Implemented) PC.09 – Active Monitoring PC.13 – Archiving PC.14 – Downloading Policy Controls PC.15 – Audit Button	Medium (11) Probability: Unlikely Consequence: Moderate
PR.04	**Risk/Source of Risk**: Insufficient cyber threat security controls make system vulnerable to access, misuse, theft or unauthorised disclosure of information by external threat actor.	High (18) Probability: Possible Consequence: Major	High (18) Probability: Possible Consequence: Major	PC.10 – Security Assessment PC.13 – Archiving (solution dependent)	Medium (13) Probability: Rare Consequence: Major
PR.05	**Risk/Source of Risk**: Lack of disposal process results in information being retained for longer than is lawfully required.	High (16) Probability: Likely Consequence: Moderate	High (16) Probability: Likely Consequence: Moderate	PC.12 - Retention and Disposal Processes PC.14 – Downloading Policy Controls	Low (6) Probability: Rare Consequence: Moderate
PR.06	**Risk/Source of Risk:** Insufficient oversight leads to NDMS information being used for a purpose other than what it was collected for.	High (16) Probability: Likely Consequence: Moderate	Medium (12) Probability: Possible Consequence: Moderate	PC.02 – Governance PC.07 – NDMS Terms of Use (Implemented) PC.16 – NPHS data warehouse Snowflake Instance	Medium (11) Probability: Unlikely Consequence: Moderate

PR.07	**Risk/Source of Risk:** Insufficient oversight leads to information provided to NPHS data warehouse Snowflake Instance being used for purposes for which it was not collected or which are not authorised/unlawful.	High (17) Probability: Almost Certain Consequence: Moderate	Medium (12) Probability: Possible Consequence: Moderate	PC.02 – Governance PC.16 – NPHS data warehouse Snowflake Instance	Low (6) Probability: Rare Consequence: Moderate
PR.08	**Risk/Source of Risk:** The use of CPIR by NDMS is not privacy assessed, leading to impacts on the privacy of individuals.	Unknown		PC.17 – NDMS Use of CPIR	Low (6) Probability: Rare Consequence: Moderate

Privacy Risks – All Controls Implemented

Risk Ref No.	Description of Privacy Risk identified through PIA	Summary description of Controls implemented	Residual Risk Rating	Date achieved
PR.09	**Risk/Source of Risk**: Privacy Statement is insufficient in detail and/or has not been recently reviewed or updated, misleading individuals as to how their information is being used.	**PC.03 – Privacy Statement** **PC.11 – Access and Correction Requests Process** The Privacy Statement has been updated to include detail on NDMS and how an individual's information will be handled, including how to request access to their personal information. A process for individuals to access or request changes to their personal information has been established.	Low (4)* Probability: Rare Consequence: Minor *as this risk is rated Low, will be removed from next iteration of PIA	Publication date of PIA
PR.10	**Risk/Source of Risk:** 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.	**PC.06 – User Approval** **PC.07 - NDMS Terms of Use** All NDMS Users undertake mandatory HNZ privacy training, or their agency's equivalent. Users also agree to the NDMS Terms of Use which stipulates that they will not knowingly access or disclose any personal or health information about any individual(s) unless such information is essential for the User to properly and efficiently perform the duties and obligations of their role. The User Approver will ensure both these criterial are met before approving a User's access.	Medium (11) Probability: Unlikely Consequence: Moderate	November 2024
PR.11	**Risk/Source of Risk**: Individual (or authorised representative) is unable to access or correct their information as there are no processes in place.	**PC.11 – Access and Correction Requests Process** A process whereby individuals may contact their local public health service to access or correct their personal information is in place. Appropriate responsibility for overseeing and approving this disclose is outlined in the User Approval Framework.	Low (6)* Probability: Rare Consequence: Moderate *as this risk is rated Low, will be removed from next iteration of PIA	Publication date of PIA
PR.12	**Risk/Source of Risk**: Authorised Users are not aware of their obligations when dealing with information leading to that User accessing, using or disclosing information for unauthorised purposes.	**PC.04 – Privacy Training** **PC.07 – NDMS Terms of Use** **PC.08 – Audit logs** To ensure Users are aware of their obligations, they must have undertaken mandatory privacy training, have indicated what access they will require for their role and read and agreed to the Terms of Use before being granted access to NDMS. User Approval ensures these controls have been completed prior to access being granted.	Medium (13) Probability: Rare Consequence: Major	November 2024

Privacy Controls

Control Ref No.	Control Name	Control Description	Status Planned, In Progress or Implemented	Owner Name, Role & Business Unit	Due Date
PC.01	PIA Review/Update	To ensure the information required for the newly onboarded diseases is justified and captured in the PIA appropriately and correctly and that any other major NDMS changes are considered and assessed. Consideration may need to be given to Privacy Act changes expected in May 2026, but as these have been anticipated in version 3 of this PIA, an update may not be required.	Implemented/ Ongoing	Toby Regan – National Manager, Major Projects, Protection, NPHS	September 2027 or earlier if significant changes occur before then
PC.02	Governance	Interim NDMS Governance is currently in place while the system is being built. This Governance includes oversight by various governance groups and committees to ensure the system operates effectively and in compliance with relevant laws and regulations. The interim governance is responsible for compliance with Retention of Information Policy, monitoring audit logs and reviewing compliance with processes (with consequences for non-compliance) and oversight of provision of appropriate training to Users (with updates as required when new functionality or new issues arise). However, an enduring governance must be established well in advance of the expected project completion date (March 2026) to ensure a smooth continuance of operations. This shall include assignment of responsibility for ensuring the July 2025 Government Standard for providing non-government third parties with access to, or collection of, government-held personal information is complied with when granting external agencies access to NDMS.	Planned	Toby Regan – National Manager, Major Projects, Protection, NPHS	December 2025
PC.03	Privacy Statements	Short privacy scripts are conveyed to individuals when they are contacted and a full privacy statement is available in handout form, as well as on the HNZ website. Last updated August 2025.	Implemented	Toby Regan – National Manager, Major Projects, Protection, NPHS	
PC.04	Privacy Training	In addition to mandatory privacy training for all NDMS Users, a knowledge article has also been produced to support Users.	Implemented	Toby Regan – National Manager, Major Projects, Protection, NPHS	
PC.05	Role Based Access Controls	This control is largely implemented: NDMS has Role Based Access Controls determined by interim NDMS Governance. HNZ NDMS Users will have access to all information in the system, regardless of where they are located, however the permissions granted to a User will be based on the role requirements (e.g. Read only access). External Agencies granted NDMS User privileges, will be subject to limits associated with their access requirements (i.e. time limited period, what can be accessed, and the permissions granted). Additional Role Based Access Controls may need to be implemented to limit access to some diseases and/or to enable and appropriately limit access to download functionality. This is still to be scoped and confirmed.	Planned (TBC)	Toby Regan – National Manager, Major Projects, Protection, NPHS	March 2026
PC.06	User Approval	This control is largely implemented: NDMS User Framework has been developed which includes the criteria a requestor must meet, prior to being granted access to NDMS. The framework also establishes processes in relation to allowing external agencies access, and the responsibilities of User Approvers, who will be approving user access. This Framework, and associated artefacts such as access request forms, may need to be updated if access to some diseases is limited and/or if downloading functionality is introduced. This is still to be scoped and confirmed.	Planned (TBC)	Toby Regan – National Manager, Major Projects, Protection, NPHS	March 2026
PC.07	NDMS Terms of Use	NDMS Users must accept a (revised) Terms of Use prior to accessing the system. This acceptance is required for the initial log in which must be reaccepted every 3 months, when a User changes their password, or when the Terms of Use has been updated.	Implemented	Toby Regan – National Manager, Major Projects, Protection, NPHS	
PC.08	Audit Logs	Audit logs are captured within the system and available for proactive and reactive review. Proactive system monitoring (SIEM) is implemented.	Implemented	Toby Elliott – Product Manager	
PC.09	Active Monitoring	A formalised and standard process is yet to be scoped and developed to monitor and identify user misuse of the system. Options need to be assessed, and a decision made on which options can be practically implemented.	Planned	Toby Elliott – Product Manager	February 2026

PC.10	Security Assessment	An Approval to Operate (ATO) has been updated to reflect new functionality and signed out, with a number of identified controls which are currently being worked on. The initial rating is MEDIUM, with an overall target risk rating of MEDIUM.	Implemented	Toby Elliott – Product Manager	
PC.11	Access and Correction Requests	A process is in place where access and correction requests are forwarded to and coordinated by the Regional Kaitātaki Health Protection person. Details of how an individual can initiate an access request/correction to information is included in the full Privacy Statement.	Implemented	Toby Regan – National Manager, Major Projects, Protection, NPHS	
PC.12	Retention and Disposal Processes	Expiry time periods have been identified for the removal of information and aligns with the HNZ Information and Records Management Policy. However, how the information is to be disposed of at the determined expiry dates (i.e. 2 years, 10 years and 25 years) is yet to be documented and evidenced.	Planned	Toby Elliott – Product Manager	February 2026
PC.13	Archiving Process (inactive records)	A process to be developed for identifying when records in NDMS are no longer operationally required for active management of disease, and a solution implemented to make these records unavailable to those users who only require access for those purposes. This may involve archiving within NDMS or removal from NDMS for archiving in a secure location (e.g. NPHS data warehouse Snowflake Instance).	Planned	Toby Regan – National Manager, Major Projects, Protection, NPHS	February 2026
PC.14	Downloading Policy Controls	If downloading capability is enabled in NDMS rules and guidance is likely to need to be developed to lower privacy risks arising from data being held outside the NDMS controlled environment.	Planned (TBC)	Toby Regan – National Manager, Major Projects, Protection, NPHS	February 2026
PC.15	Audit Button	A button or other means of flagging records will be added to the system, to allow users to tag a record for proactive audit.	Planned	Toby Regan – National Manager, Major Projects, Protection, NPHS	July 2026
PC.16	NPHS Data Warehouse Snowflake Instance	A privacy assessment detailing how NDMS information in Snowflake can be used is planned. This will ensure data is not used for any purpose other than what it was collected for.	Planned	Toby Elliott – Product Manager	October 2025
PC.17	NDMS Use of CPIR	A privacy assessment detailing how NDMS will utilise CPIR, and for what purposes is in progress.	In Progress	Toby Regan – National Manager, Major Projects, Protection, NPHS	October 2025

Target Risk Rating Table

Likelihood	Minimal	Minor	Moderate	Major	Severe
Almost Certain	Medium - 8	High - 15	High - 17	Extreme - 23	Extreme - 25
Likely	Medium - 7	Medium - 10	High - 16	High - 19	Extreme - 24
Possible	Low - 3	Medium - 9	Medium - 12	High - 18	High - 22
Unlikely	Low - 2	Low - 5	Medium - 11	Medium - 14	High - 21
Rare	Low - 1	Low - 4	Low - 6	Medium - 13	Medium - 20

Consequence

Probability Descriptions:

Rare May occur in known or exceptional circumstances / no known history
<10% chance of occurring

Unlikely Not expected but could occur in some circumstances / has happened infrequently
10-30% chance of occurring

Possible Might occur in some circumstances / has happened occasionally
31-60% chance of occurring

Likely Has happened / probably will occur in most circumstances
61-90% chance of occurring

Almost Certain Regularly happens / expected to occur in most circumstances
>90% chance of occurring

Project and programme risks are evaluated based on the project or programme timeline.

Strategic and Operational risks are evaluated based on a 3-year timeframe i.e. what is the chance of the event arising in a 3-year planning period.

Consequence Descriptions:

Please refer to the Risk Management Process document here (page 18) for specific Domains (i.e. Clinical/Patient Safety), and their associated consequence descriptions. If you are unable to access the framework, it can be provided to you by the National Privacy Office.

Review and Sign off

Business Owner

I approve this Privacy Assessment, accepting that:

- I am accountable for managing personal and/or health information for this initiative
- I own the privacy risks associated with this initiative and am responsible for ensuring any controls to mitigate risks are actioned
- I understand this assessment is a living document and must be reviewed and updated periodically.

Name: Matt Hannant – Deputy National Director, National Public Health Service

Signature:  Date: 7 November 2025

Project Manager

I confirm this Privacy Assessment accurately describes the initiative, how it will be implemented and utilised in HNZ, and identifies all substantive privacy risks, along with appropriate controls.

Name: Toby Regan – National Manager, Major Projects, Protection Directorate, NPHS

Signature:  Date: 1 October 2025

National Privacy Office

I have reviewed this privacy assessment and, based on the documented content, am satisfied that the privacy risks and controls for this initiative have been sufficiently and appropriately identified.

Name: Viv Kerr – Head of Privacy

Signature:  Date: 1 October 2025

Privacy Officer Comment

Appendix 1: Finders Service

Purpose

The Finders Service is a part of the National Investigation Service (NIS) and has responsibility for enhancing the efficiency and effectiveness of contact tracing efforts where there may be limited information. The service seeks contact details from reliable sources, focusing on phone and email information.

A 'Finder' is a specialised NIS staff member, who has been trained to perform key investigation activities when Contact Tracers have been unable to promptly identify or locate an individual. This is essential for ensuring Cases and Contacts receive timely information and instructions to mitigate the spread of a disease, to keep themselves and others safe.

It should be noted that the service does not verify contact information received from external sources before adding to NDMS. If a contact number is found to be invalid or belongs to someone else, this information will remain in NDMS record but noted as an invalid number.

Finders Service – Initial Search Process

If the individual being sought is unable to be readily contacted, or their identity needs to be further clarified, it is not reasonably practicable in some circumstances to source the information from the individual. See Principle 2: Source of Information for the legal basis for collection of information from other sources which applies to the Finders Service.

The intention of the Finders process is to proceed from the least sensitive information sources, only looking further when the individual has been unable to be identified or contacted.

If an NHI can be linked, an NES search may produce the necessary contact details. Where contact details are discovered and contact is successfully made, the Contact will be passed back to the local public health service for follow up. If no contact can be made from the available details (or there are no current details) the Finders Service will progress to look at further options.

If an NHI cannot initially be linked, the Contact and Exposure Event files on NDMS are reviewed to look for any additional identification or contact details in those locations. If unsuccessful, the Finders Services will look at other alternative information sources.

Use of General Practice Sources

General practitioners may be contacted by the Finders Service, if an NHI has been identified, to find up-to-date contact details of a Case or Contact (and only as a last resort obtain Next of Kin/Emergency Contact details).

Finding household members of Contact to reach Contact

Phone numbers can be changed with some frequency by some individuals. If HNZ internal databases do not hold a current contact phone number for a Contact, it may be that another person living at the same location with the same surname may be identified. In this situation, a call may be made by the Finders Service to that other person with a request made to provide the Contact's phone number.

Use of Social Media

In extenuating circumstances, social media may be used, however Privacy will be engaged at this time.

Collaboration with External Agencies

In the event that the Finders Service has not located the individual in question after following the relevant processes noted above, there are a number of external sources that may be contacted (see Summary: Agency Collaborations).

Also see *Appendix 2: Exposure Events* for additional detail on how the Finders Service will engage with collaborating external Agencies and Third Parties in such circumstances.

Training of Finders Service

Training undertaken by the Finders Service includes awareness of the obligations of s92ZZG which requires that the identity of the individual who may have transmitted or created a risk of exposure is not identified (as far as is practicable).

All processes are supported by extensive training and reference documentation.

Appendix 2: Exposure Events

An Exposure Event is any location and time that has been identified by a Case Investigator or Contact Tracer as a high risk for people to have been exposed to a disease.

Flight related Exposure Events

As referenced in Principle 11, The New Zealand Customs Service has an Information Disclosure Agreement under section 316 of the Customs and Excise Act with Health New Zealand. Section 316 of the Customs and Excise Act 2018 specifies that the following dataset may be disclosed to HNZ (in accordance with the Agreement). This will enable identification of all arrivals on a flight or vessel arriving into New Zealand:

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

For exposure events on international flights, Customs will be approached for flight details.

For exposure events on internal flights, the Finders Service will approach the airline carrier with a request for information or request via NFP.

All Other Exposure Events

Other Exposure Events can be any location, where there may be a risk that the public have been in contact with a Case, such as restaurants, bars, supermarkets or gyms.

If an event had bookings there may be a list of attendees available along with contact details. In instances where this is not the case, such as a Friday night attendance at a bar, then it can be more challenging to obtain the necessary information on any potential Contacts.

Contact can be made with relevant organisations, and if required, assistance can be compelled via section 92ZZF of the Health Act (by Contact Tracers appointed under s92ZZA of the Health Act). This can include an individual's employer, an educational institution attended by the individual, a business or organisation that the individual has dealt with or an event co-ordinator or person likely to have a list of who attended an event.

The organisation may be requested to look through their own information (such as CCTV footage, and bank records) to report back identified Contacts. The organisations will be requested to release the findings back to the Finders Service or directly to the relevant Contact Tracer.

New Information Sharing Memorandums of Understanding have since been signed with agencies, as described in the Summary: Agency Collaborations to assist with the rapid identification and location of Contacts.

Appendix 3: NDMS Terms of Use

NDMS: Terms of Use and Confidentiality Requirements

Welcome new or returning user

Terms of Use

Terms last updated on 27/08/2024

Prior to accessing the Notifiable 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 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 NDMS or any information related to NDMS.
- You must take care of NDMS information and keep it secure and confidential.
- You will not share, disclose, or publish information in a manner that could reasonably be expected to identify an individual.
- You will not try to (re)identify any individual where information is provided in a deidentified format.
- 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 look yourself up on the system if you are a case, contact or involved in a notifiable disease exposure event.
- You will notify any potential conflicts of interest to your manager immediately and take advice on managing these, for example if assigned tasks require you to access the records of family members or close associates.
- You will not share your access credentials with anyone or let anyone else use yours.
- You will not download, copy or otherwise extract personal information from NDMS unless needed to perform your role and clearly authorised.
- You will only access 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 will not use any information available in NDMS to develop, train or otherwise use artificial intelligence tools without HNZ approvals.
- You understand that all access to NDMS by you will be logged and may be monitored.
- You will let your manager and HNZ Privacy/HNZ Information Security Teams 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.
- If you are a manager who has been informed there has been or is about to be a privacy or security breach, you will inform NDMS Product Owner, NDMS Platform Owner and HNZ Privacy Team and/or HNZ Information Security Team.
- You understand your account will be disabled after 90 days of inactivity to meet security, privacy, and licensing requirements.

User requirements

In your role you are to be authorised as a user of NDMS. You will have access to personal and health information, and in your interactions with individuals. Each user is a trusted part of the 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 NDMS (or further accessing NDMS if they are amending their password for access).
- Complete any training offered to them in relation to 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 NDMS may be removed, and the matter may be referred to the user's employer, or other legal action may be undertaken if appropriate.

Application of these Terms

The Terms apply to all users of this Service.

Continued access to this Service is contingent upon ongoing compliance with these Terms (as amended by HNZ from time to time).

If you do not comply with the Terms, your access to this Service may be immediately removed, the matter referred to your employer, or other legal action 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 NDMS and will not download any information from 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/ as a supervisor I will inform NDMS Product Owner, NDMS Platform Owner and HNZ Privacy/HNZ Information Security 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 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 NDMS or the information on it.
- I understand that my access to 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**

Appendix 4: Summary of NDMS-relevant Mandated Collection in the Health Act 1956

Key sections in Part 3 (including Part 3A) of the Health Act 1956 which mandate collection or allow the mandating of collection include (note: this list is not exhaustive):

Section	Summary
Reporting	
74	Health practitioners required to give notice of notifiable disease to a Medical Officer of Health in prescribed form
74AA	Medical laboratories to give notice of notifiable disease (via a test result) to a Medical Officer of Health in prescribed form, and to notify the health practitioner for whom test was undertaken
Cases and contacts	
92I	Subject to overarching principles in Part3A, Subpart 1 and other relevant sections, a Medical Officer of Health may make directions for any person that poses a public health risk, which may include requiring information from that person.
92J	Subject to overarching principles in Part3A, Subpart 1 and other relevant sections, a Medical Officer of Health may make directions for contacts of any person that poses a public health risk, which may include requiring information.
Note: Sections 92I and 92J do not specify any particular information collection, but allow for a Medical Officer of Health to "take specified actions to prevent or minimise the public health risk posed by the individual" which could include information provision if required.	
92ZZC	Where contact tracing is deemed required, a case or suspected cases (who may be contacts of other cases) must provide – if required by a contact tracer – information about people they have been in contact with and/or the circumstances in which they believe they may have contracted or transmitted the infectious disease. With respect to contacts the person may be required to provide, for each contact: name, age, sex, address and other contact details, or any other information required by regulations made under the Health Act.
Others	
92ZZF	For the purposes of identifying contacts, a specified range of organisations and individuals may be required to provide a contact tracer with the names and addresses of contacts.
Confidentiality – to note	
92U 92ZS 92ZZG	Confirms that information obtained under Part 3A can only be used for the purpose of effective management of infectious disease.

See also the Health (Infectious and Notifiable Diseases) Regulations 2016. Schedule 3 details the minimum information requirements for notice of notifiable disease by medical laboratory, which in relation to the patient/NDMS comprise:

- the patient's name
- national health index number (if known)
- address
- date of birth
- date of death and cause of death (if applicable)
- sex ethnicity (if known), and
- details of the disease and tests
- name of the health practitioner ordering the test and his or her phone number, address, and email address.