

# **Te Whatu Ora - Health New Zealand**

## **Aotearoa Immunisation Register**

### **Privacy Impact Assessment**

**Date 20/11/2023**

## The Project

<b>Business Unit:</b>	National Immunisation Programme
<b>PIA Author:</b>	Amelia Harris – Te Whatu Ora Privacy Consultant
<b>Date PIA prepared:</b>	20/11/2023
<b>Last revision date: if applicable:</b>	Click to enter a date.
<b>Version number:</b>	1

## Summary of Project / Change

**Please describe** the project (or change) clearly and simply. Be sure to set out:

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

### Purpose

The Aotearoa Immunisation Register (AIR) will replace the National Immunisation Register (NIR) and will supersede the COVID Immunisation Register (CIR). The purposes of AIR are twofold:

1. to act as New Zealand’s immunisation source of truth to provide timely and accurate understanding of population immunity to mitigate risks to public health, and
2. to provide an accurate and complete set of vaccination data accessible to New Zealand health providers to ensure safe and effective Consumer health care.

These purposes are further broken down and described in more detail throughout this document.

AIR will provide a mechanism for recording the offer of immunisation services and the outcome of that offer for all vaccinations (including public and privately funded). AIR will act as Aotearoa’s immunisation source of truth.

### Background

On 1 April 2022 a tactical solution was deployed in support of the Flu Vaccination Programme. Flu vaccinations were captured through the existing CIR and stored in the newly established National Immunisation Service Immunisation Service Management (NIS ISM) system. A Privacy Impact Assessment (PIA) was carried out to assess this tactical solution – the NIS MVP PIA. In June 2022 the NIS was renamed to the Aotearoa Immunisation Register (AIR).

In September 2022, the Immunisation Service Delivery (ISD) platform was rolled out to a pilot group to capture MMR vaccinations. It was extended in November 2022 to record additional vaccine types and return immunisation history information for Consumers currently available in NIR, CIR and AIR. It has also replaced ImmuniseNow which was the system used by Pharmacies to record their administered vaccinations in the NIR and to view Consumer vaccination history.

### Engagement with Privacy and the Office of the Privacy Commissioner

The AIR programme has engaged an external privacy resource who has been consulted on every major design and technical decision leading up to go-live of the solution. This resource has also been involved

with the implementation of privacy artefacts for the AIR programme, including Privacy Statements, Consumer and Health Sector communications, information brochures, website content, terms of use and business procedures. This relationship will cease with the implementation of the AIR on 22 December 2023. Te Whatu Ora Privacy will provide continued support to the AIR, any required updates to this living PIA document.

The Office of the Privacy Commissioner significant concerns around the design of the system, specifically relating to the removal of the 'opt off' option. To date, significant work has been done on implementing a 'suppression' system that will allow for the OPC's feedback to be adopted while ensuring the purposes of the AIR can still be met.

### Justification for the design of AIR as a centralised system

The NIR was established to provide a centralised record of Consumer immunisation history and address the poor quality of data on immunisation coverage across communities. However, there have been significant roadblocks in the NIR's ability to fully achieve these goals due to the inconsistencies across Vaccinator record keeping and the ability for Consumers to decline data collection.

The aim of AIR is to remedy these roadblocks and create an accurate and complete set of population vaccination data to strengthen New Zealand's public health response. Below are the key justifications that the collection of all public and privately funded vaccinations within one system would enact the purpose of AIR as set out above.

Historically, Consumer vaccination information was always collected in PMS systems, but the NIR allowed Consumers to decline having this information recorded centrally. This reflected the fragmented nature of health services provided across Aotearoa. Throughout the COVID-19 response, centralised recordkeeping was key to the health systems ability to deliver health services to those who required it. In addition, with the centralising of national health services through the implementation of Te Whatu Ora, this provides a further opportunity to ensure health care recordkeeping is improved along with the provision of health services.

Currently, the population of data into shared care systems and clinical data repositories is controlled by the consumer 'opting off' having their information transferred. The problem is that this information is not quickly transferrable if needed in an emergency or where there is a serious threat.

The decision to centralise Consumer vaccination information under the AIR while enacting a 'suppression' functionality to ensure consumer choice is enabled, ensures Te Whatu Ora complies with its legislative function under section 14 of the Pae Ora (Healthy Futures) Act 2022 (as discussed in more detail below) and its obligations under the Health Information Governance Guidelines, while still allowing healthcare professionals to respond quickly in an emergency (such as an outbreak of an infectious disease).

### Introducing a suppression process

Adjustments have been made to the AIR to introduce a system for suppression of records within the system. This process will supersede the 'opt off' process that was introduced for the NIR. A request to suppress records will only apply to future vaccinations once AIR goes live. It will not apply to historical vaccinations which have already been recorded in the NIR or CIR and were not previously subject to the 'opt off' process.

Te Whatu Ora acknowledges that consumer choice is a requirement under the Health Information Governance Guidelines, but this must be balanced against the need for complete, accurate and up to date clinical records of healthcare.

The suppression process does not inhibit all vaccination information being recorded in the AIR. However, if a consumer receives a vaccination, they can elect to have their information suppressed, which will stop the information being visible or shared to other parties outside Te Whatu Ora. This includes other health services a consumer may access that would use this information to make clinical decisions about health care e.g., emergency departments, pharmacies, occupational health services or general practice etc. After suppression, records may still be accessed in an emergency situation i.e., where a vaccine preventable

disease outbreak threatens the health and safety of our community and public health teams need to respond quickly to prevent further harm.

Individuals can request to have their records suppressed by emailing the Te Whatu Ora privacy team. A form will then be provided to the consumer outlining the impact of their decision and seeking confirmation of the decision to suppress. There is a 20-working day cooling off/ processing period, which aligns with the custom and practice of some of the other Registers managed by Te Whatu Ora that allow for opting off the register.

### Supporting justifications for the Purpose of AIR

#### *Enacting Legislative Function*

The Health Act 1956 states the Ministry of Health has the purpose of improving, promoting, and protecting public health. With the introduction of the Pae Ora (Healthy Futures) Act 2022, Te Whatu Ora was given the below legislative functions under section 14 to carry out this purpose:

- Provide or arrange for the provision of services at a national, regional and local level.
- Develop and implement locality plans.
- Undertake health workforce planning.
- Undertake and promote public health measures.
- Improve service delivery and outcomes for all people at all levels.
- Collaborate with other agencies, organisations, and individuals to improve health and wellbeing outcomes and to address the wider determinants of health outcomes.
- Evaluate the delivery and performance of services provided or funded by Health NZ.

The proposed design of AIR as both a point-of-care and shared care platform operating as a centralised immunisation register with accurate and complete data quality, will give the health workforce the greatest opportunity to fully enact the legislative functions set out above.

Principle 1 of the Privacy Act 2020 allows an organisation to collect information if it is for a lawful purpose connected with their functions and activities and the information is necessary to achieve that purpose. The AIR is a system which is being introduced by Te Whatu Ora to meet Te Whatu Ora's purpose of improving, promoting and protecting public health in connection with its functions specified in section 14 of the Pae Ora (Healthy Futures) Act 2022. Having a centralised record enables Te Whatu Ora to meet both its purpose and its functions. Fragmentally recorded or missing vaccination records inhibit the improvement of service delivery and outcomes and prevents effective locality and health workforce planning.

In addition to our legislative obligations, Te Whatu Ora is also bound by the Health Information Governance Guidelines (HIGG). Specifically, section 4.3 of the HIGG requires us to provide consumers with a choice as to what happens to their individual records. For AIR, this is realised through a 'suppression' option built into the shared care system which gives effect to the consumer's wishes to not have their information disclosed to other parties. In theory, it will also allow access by health providers through a 'break glass' mechanism in an emergency and where the patient is unable to give their direct consent.

#### *Improve Service Delivery of Vaccination Services*

Keeping medical records is a legal requirement under the Health (Retention of Health Information) Regulations 1996. AIR will be a vaccination shared care system that clinicians use to record and view Consumer vaccination records. Where a clinician uses a different system for recording vaccination data (such as PMS), this will be pulled through to AIR ensuring that AIR is maintained as the centralised immunisation record.

For those records where the person has requested that their information is suppressed, these records will still be pulled through to the AIR but will not be shared with any other parties. This means that the records may still be used for statistical and research purposes to target vaccination campaigns but not outreach campaigns targeted at the individual level.

It is important for Health professionals to work from the same set of Consumer records to provide a reasonable standard of continuity of care to the Consumer. To ensure this continuity of care, vaccination records should be centralised and not fragmented so to adequately inform a Vaccinator and avoid the risk of over or under vaccinating a Consumer. This is particularly important in cases of emergency or where

there is a serious risk to the life of the Consumer, and they are unable to provide confirmation on their vaccination status.

Understanding the level of immunity risk in the community is also key to carrying out the above functions and is an important public health interest. Without a centralised record, we would not accurately be able to understand population immunity and coverage in New Zealand, and this would affect our ability to plan and improve service delivery and outcomes.

#### *Implementing Public Health Measures*

In collecting in one location the minimum required information about population immunisation coverage, the register will act as a safety net for future public health protection. The register will provide enough information to inform the health sector of where the gaps are across population immunisation coverage, strengthening the ability of the public health response to address problem areas in the event of a widespread outbreak. The information collected via the register is the minimum amount of information needed to support other entities to take the necessary steps in managing outbreak events. This is in line with the Privacy Act requirements to only collect the information necessary to achieve the purposes of AIR.

#### *Supporting Health Workforce Planning*

The quality of health information is a product of its accuracy and completeness. In requiring the compulsory collection of all vaccinations within one central register, the design of AIR ensures that the following benefits of good quality data are realised:

- Consumers are more likely to receive safe and effective care if health providers have access to accurate and reliable information to support decision making.
- Consumers will have access to reliable information to help them decide where and when to access care, improving service delivery and outcomes.
- If the information used to support decision making is of a high quality, health care services can plan and provide for future population needs more effectively and efficiently.
- Healthcare research contributes to improved outcomes by providing evidence to support particular care processes. This research can only be relied on if it is based on good quality and complete information.

#### **Overview of the Immunisation Source of Truth Lean Data Model, Immunisation Service Delivery (ISD) and Immunisation Service Management (ISM) Portals**

The AIR is comprised of Services and Experience Layers.

The Services Layer is the Immunisation Source of Truth (ImmSoT) Data Repository held on the AWS tenancy and the Operational and Analytical Reporting functionality.

The Experience Layer is the Immunisation Service Delivery (ISD) and Immunisation Service Management (ISM) portals located on the Salesforce platform front end. These portals are used to capture vaccination event details and provide a mechanism for the health workforce to create, view and edit a Consumers vaccination history record. These portals are integrated with the ImmSoT data repository and with other existing Te Whatu Ora systems such as the NHI, HPI and NES.

ImmSoT will be collecting information from the following sources:

- Directly from the Vaccinator and Consumer at the time of vaccination via the Immunisation Service Delivery (ISD) portal or Patient Management Systems (PMS)
- Migration of historical immunisation records from the NIR and CIR
- Te Whatu Ora existing systems – such as the NHI, HPI, NES (note: information received from these systems will pass through the ImmSoT, but will not be stored there).

The ISD is the Vaccinator portal which is where all the details associated with a vaccination event will be recorded, viewed, and stored in the ImmSoT data repository.

The ISM is the administrator portal where admins will have the ability to onboard Users to the ISD and where they can view, edit, and change the vaccination record held in the ImmSoT data repository. Users

will not be able to upload data into the ISD or view the data held in the ImmSoT data repository until they are onboarded to the ISD or ISM.

### *Immunisation Source of Truth*

The ImmSoT data repository will only capture minimal vaccination event information from the ISD and PMS (NHI, DOB, gender and vaccination event information) and will not itself store all the information associated with the NHI or HPI. Instead, the relevant patient fields and health provider fields will be enriched with data from the NHI register and HPI register when a query about a vaccination record is raised by the ISD/ISM portals or PMS.

The ISD/ISM or PMS users will raise a query by inputting an NHI number into their front-end User interface. The NHI number is sent to ImmSoT which pulls all the vaccination event information associated with that NHI (including HPI) stored in ImmSoT. ImmSoT then acts as an intermediary to send the NHI and HPI numbers to their source systems – the NHI and HPI registers (via the Orchestration Service), where they are enriched with additional personal information stored on these source systems. The ImmSoT then returns the enriched vaccination event information back to the ISD/ISM or PMS. This enriched information is not retained by the ImmSoT. This Orchestration Service is discussed in more detail below.

Information flows out from the AIR will include:

- To Primary Health Organisations / General Practitioners who will be notified of the vaccination status of their patients via HealthLink. This process is discussed in more detail under the Co-Existence Broker Service section below.
- Reporting - including identifiable level reporting where required to enable providers to follow-up with Consumers, and non-identifiable reporting for resource planning and other tasks. Te Whatu Ora and the AIR programme will also require both identifiable and aggregated reporting for the purposes of improving, promoting, and protecting public health under the Health Act 1956. An analysis of the Operational and Analytical Reporting Functionalities under AIR is provided later in this PIA.

### *Immunisation Service Delivery Portal*

ISD Users can view a Consumers vaccination record by inputting their NHI number into the ISD. If they do not have the NHI number for a Consumer, the User must search the NHI register directly to get it.

Vaccinators will also record immunisation event details in the ISD. This information includes:

- Consumer identification information (such as Name, DOB, NHI),
- vaccination event information (such as vaccine type and batch number), and
- Vaccinator identification information (such as HPI and HPI FID).

Minimal information from this collection (NHI, DOB, gender, Vaccine Event Information (including HPI)) is then stored in the ImmSoT data repository (the data fields captured as Vaccination Event Information are set out in the Data Collection Table). This is due to ImmSoT operating as a lean data model, which only requires minimal identification information which is then enriched by other data sources as set out below.

### *Immunisation Service Management Portal*

The ISM is the AIR administrator portal where AIR admins can create, view and update Consumer immunisation records by querying an NHI number. AIR admins will also deal with AIR data quality issues. For example, when data is sent to the ImmSoT via the ISD, and something has gone wrong (such as the NHI being invalid), the AIR admin receives a notification via the ISM that the data quality rules determined by the business have not been met.

These functionalities are possible via the following ImmSoT API's which have been developed specifically for AIR:

- Create;
- Update;
- Search;
- Read Immunisation Record;

- Read Immunisation Record Version History; and
- Search Immunisation Records with Data Quality Issues.

### *Integrations with Existing Te Whatu Ora Systems via the Orchestration Service*

Personal information will also be used by the AIR from leveraging existing integrations with Te Whatu Ora Identity Systems (NHI, NES and HPI). These integrations will occur via the Orchestration Service discussed in more detail under Principle 2 of this PIA. The NHI will be used to establish the health identity of Consumers recorded in AIR, and the HPI will be used to identify Vaccinators.

Vaccinators will not have the ability to update NHI source system details for Consumers via the ISD or PMS. If the NHI, DOB and gender recorded in the ISD for a Consumer who has received a vaccination does not match the records from the NHI source system, a data quality issue is raised and alerted to the AIR Administrators via the ISM. The AIR admins will need to facilitate the update of information in a separate application (Health UI) connected to the NHI system.

The NHI, combined with the NES can be used to identify the general practitioner or practice a Consumer is enrolled with and identify people that have no Primary Care enrolment. This will be those people who have had some contact with the health system (and have an NHI) but are not currently enrolled with a GP.

### *Patient Management Systems and Co-Existence Broker Service*

PMS systems currently communicate with the NIR through HealthLink. AIR is moving to a co-existence model where API's will be implemented between PMS systems and the AIR. These APIs will eventually be utilised by other Providers who do not have direct access to the AIR. Currently, PMS vendors need more time to effectively uptake these APIs, so the Co-Existence Broker Service is being developed to allow PMS systems and the AIR to talk to each other in the meantime. This broker service is part of HealthLink.

The main purpose of the messaging allows for a status query to be made and for recording and editing a vaccination event. Messages are archived for up to 28 days – this is a standard process which is happening now for the NIR. None of the messages themselves get stored, only logs and audits of the messages coming in and out are available. The translation is all encrypted and non-accessible.

Currently there is a standard messaging specification (such as naming rules and data exchange rules) that we have for messages sent and received by PMS vendors. For every message, there is a mapping spreadsheet which links the API field to the PMS system. At Cutover, there will be no change in the data types that AIR is sending or receiving, but some of the field lengths will have their character limit restrictions removed. This means that a couple of the fields will need to have their data truncated. The business is taking steps to make sure that there are no clinical risks associated with truncating these fields – such as truncating a long batch number.

### **Overview of Operational and Analytical Reporting Functionalities**

This PIA assesses the operational and analytical reporting functionalities for the AIR. The operational reporting functionality is accessible by approved Users via three mechanisms – the ISD and ISM portals and PowerBI. Analytical reporting will also be carried out by Te Whatu Ora staff working on the AIR Programme or District Analysts. This analytical reporting will utilize the replica data stored in Snowflake.

The Vaccinations Administered Report (attached as an Additional Appendix) will be accessed by onboarded ISD and ISM Users through the ISD and ISM portals. There are also 7 other types of operational reports (attached as an Additional Appendix) which will be available via the PowerBI reporting functionality. This functionality will also be accessed by AIR Admins through their ISM, and by Whaihua Users, PHO-General Practices and District Analysts through PowerBI directly.

### *Vaccinations Administered Report*

AIR ISD/ISM Users can access the Vaccinations Administered Report (VAR) via the ISD/ISM portals on the internal Salesforce platform. Access to the VAR will be managed by the ISD/ISM User onboarding process and all ISD/ISM users will enjoy the same access to the VAR regardless of their ISD or ISM User role. However, the VAR available to an ISD/ISM User will be limited to the facility or facilities in which the logged in ISD/ISM User works. This is governed by the ISD/ISM Sharing Rules Model within the AIR solution.

ISD/ISM Users will generate a VAR for the following use cases:

- Reconciliation of vaccinations administered to the Facility's record of vaccinations dispensed.
- Enable payment claims for vaccination services provided.
- To provide an organisation with a list of employees and contractors who have taken up the offer of privately funded vaccination (paid for by the organisation).

A sample of the VAR is attached as an Additional Appendix. It is not possible for the VAR to use de-identifiable data while meeting the requirements of the above use cases. The VAR will, by default, limit the result sent to the ISD/ISM User to vaccinations administered within the last 30 days. The ISD/ISM User may further filter or reduce the result set to a desired smaller set of vaccination administered records, appropriate to the needs of the above use cases. For example:

- Where an ISD/ISM user works for many facilities, they may use the facility filter to reduce the result set to only the facility or facilities vaccination records to reconcile facility dispensing records.
- Where an ISD/ISM user is generating a list of employees vaccinated in a workplace vaccination facility, they may reduce the result set to only those employees vaccinated on a specific date.

The AIR Programme is aware that concerns have been raised about Users generating a VAR to check whether Te Whatu Ora staff have been vaccinated. This is not an approved use case of the VAR. In all cases, the ISD/ISM User must make a request through the Immunisation Service Help Desk to export a VAR, which should provide some mitigation to the VAR being used inappropriately.

### *PowerBI Reports*

The purpose of PowerBI is to provide a comprehensive reporting system which offers a tool for tracking and reporting on immunisation activities. The PowerBI reports provide real-time insights into completed immunisations, planned events, due events, and overdue vaccinations. It has been designed to support PHOs immunisation services, Whaihua and OIS to ensure efficient data can be accessed and analysed and enable delivery of a Te Whatu Ora immunisation service. PowerBI has a user-friendly interface and interactive dashboards for stakeholders to make informed decisions from.

The National Immunisation Programme will be responsible for determining whether access to PowerBI data is justified for a particular role (such as AIR admins). When an AIR Admin logs in to the ISM, there will be a tab which provides them with a view of PowerBI reports.

For all other PowerBI Users, access to PowerBI is via single sign on access to the B2B Guest Service using their Azure Active Directory (AD) credentials. At Cutover, only PHO's who have an existing Data Sharing Agreement with Te Whatu Ora will be granted access to PowerBI. After go-live, requests will be able to be made on an ad hoc basis by any organisation wanting access to Power BI. The approval process for these Users is outlined below:

- The National Immunisation Programme will assess whether the requestor comes from an approved organisation (an approved organisation is an organisation that falls within one of the groups approved by the Data Governance Group as being a data sharing partner). If they are not, they are directed to the process to apply to be one.
- A Data Sharing Agreement (DSA) must exist between their organisation and Te Whatu Ora. If one is not in place, they are directed to the process to apply for one.
- The requestor must have a Microsoft guest account. If not, one will be requested via myHub.

Once the above checks have all passed, a ticket will be raised with Te Whatu Ora's IT service desk to create an Azure Active Directory (AD) account and to assign them to an AD group. The service desk will then close the ticket and the Immunisation Service Support Helpdesk will inform the requestor that their access has been approved.

Other third parties such as NGO's and iwi groups will be provided with data (including AIR immunisation data) through their existing data sharing arrangements with Te Whatu Ora (via entering into a Data Sharing Agreement approved by the Te Whatu Ora Data Governance Group). Where a third party has a Data Sharing Agreement with Te Whatu Ora, data will be able to be shared, but only in accordance with the requirements of the Privacy Act 2020 and the Health Information Privacy Code 2020. The Te Whatu Ora Data Governance Group will be responsible for approving all third-party access to AIR data via Data Sharing Agreements and will ensure that it is necessary for the third party to have access data to carry out one of the purposes of the AIR. It is anticipated that these third parties will eventually be able to access reporting data via PowerBI

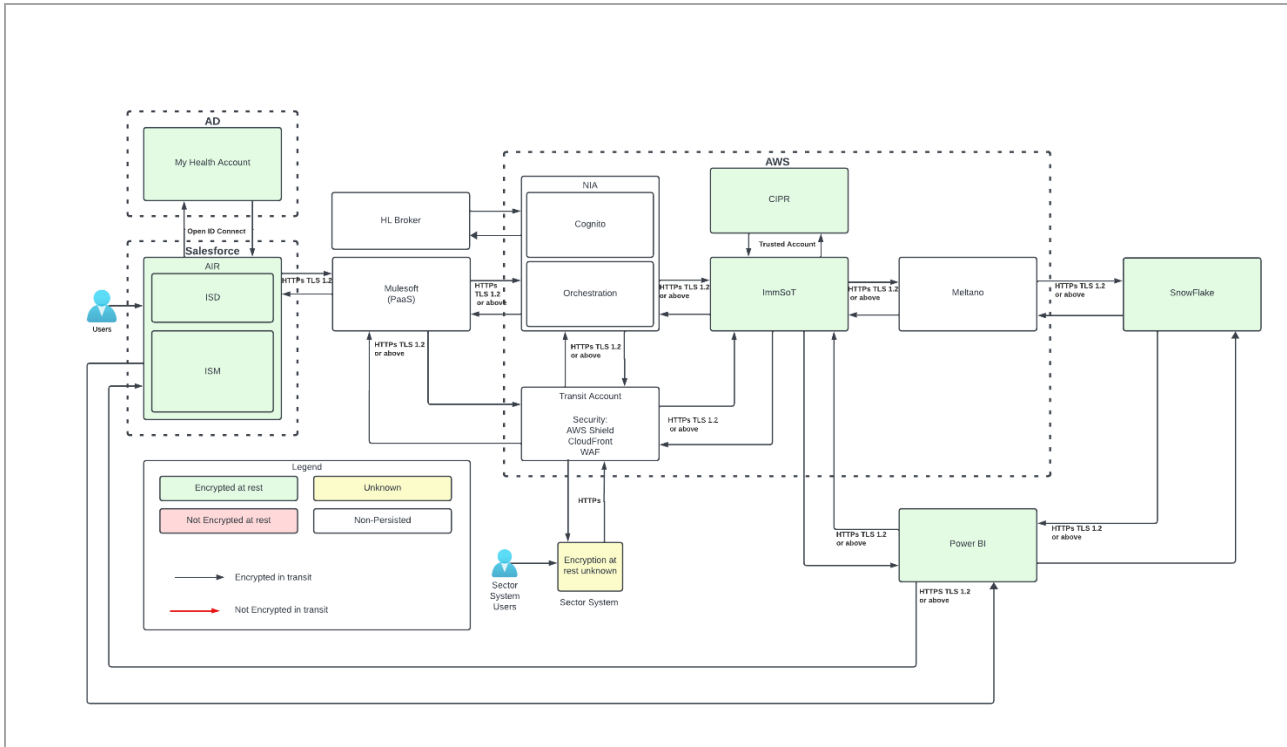


through the processes set out above, but this will be assessed in detail in future iterations of this PIA prior to occurring.

## Information Flow Diagram

Please insert a diagram (if available from project documentation) showing the end-to-end information flows relevant to this project.

The high-level end-to-end information flow is set out below. Additional information flow diagrams (including for reporting) are set out in the Appendices to this PIA.



## Scope of Assessment

Please define the scope of this PIA

This PIA assesses:

- the 'back-end' data store of the Aotearoa Immunisation Register (AIR) – known as **ImmSoT**. This assessment covers the following aspects of ImmSoT:
  - Data collected and stored.
  - Uses and disclosure of collected data.
  - Retention period and policies.
  - Integration with internal systems via the Orchestration Service.
  - Integration with external systems via API's.
  - Interaction with User interfaces.
  - Governance of data collected and stored.
- The Immunisation Service Delivery (ISD) and Immunisation Service Management (ISM) portals (also known as the Vaccinator and Administrator portals). These portals are the User interfaces which connect the health workforce to AIR and the ImmSoT data repository. This PIA will cover:

- User access to the portal including onboarding, User access controls, monitoring, and auditing processes.
- Personal information collected via the portals and the management of that information.
- Integration with AIR, existing Te Whatu Ora systems, and external third-party systems.

A previous PIA was completed for ISD Reporting in February 2023. It is intended that this PIA will replace this prior one.

3. The AIR operational and analytical reporting functionality which involves:

- A description of User groups of who can access this functionality.
- The mechanism for each User group to access the reports (via ISD, ISM or PowerBI).
- The onboarding of these User groups to their applicable access mechanism.
- The content of available reports.

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

Where ImmSoT is integrated with existing Te Whatu Ora systems (such as NHI, HPI and NES), this PIA will assess the integration points with ImmSoT via the Orchestration Service, but the systems themselves will be assessed under their own individual existing PIA's. The programme has taken steps to ensure that the data sharing arrangements will be consistent with the approved PIAs for the source systems.

The FHIR API which will connect source systems with ImmSoT via the Orchestration Service will also be assessed under its own PIA – the FHIR PIA.

My Health Record (Consumer services) and My Health Account currently have their own Privacy Impact Assessments in place. This PIA will not reassess the MHR or MHA platforms. It is assumed that those accessing the data via MHR or MHA have the proper credentials to access the information.

It also does not assess all the privacy risks associated with the PowerBI tool. Rather, it focuses on the ingestion of ImmSoT data into PowerBI and the various User groups who will access this data through the PowerBI channel. PowerBI is already in use by other programmes within Te Whatu Ora, and it has been previously assessed by the Information Security team as being secure.

## Appendices

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

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

Appendices	Information
Appendix 1	Risk and Mitigation Table
Appendix 2	Glossary
Additional Appendices – located at the link below. <a href="#">Programme Privacy Artefacts</a>	Aotearoa Immunisation Register Website Privacy Statement Information Flow Diagrams Example PHO Data Sharing Agreement ISD/ISM Authorised User Agreement Onboarding PowerBI User Disclaimer Operational Reporting – Draft Reports as at 26 October 2023 Consumer Information Sheet for Suppression Process

Assessment Questions

<b>Does the project involve personal information?</b>	YES	NO
	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

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

<b>Does the project involve personal health information?</b>	YES	NO
	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

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

## Principle 1: Lawful purpose and necessary collection of personal information

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



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

Please complete the following table:

List all information collected by the project	Please state why this information is needed for the purposes of this project
Immunisation service event information: <ul style="list-style-type: none"> <li>• Consumer NHI, DOB and gender</li> <li>• Vaccine details such as vaccine type, batch number, dilutant and needle size, dates.</li> <li>• Vaccinator HPI and Facility code where vaccination was administered (FID).</li> <li>• Related person name (person who has accompanied a Consumer under 16 years)</li> </ul>	To link the vaccination event data in ImmSoT to the correct Consumer details in the NHI to create a complete and accurate record of their healthcare services received. This will be reported to the practitioner the Consumer is enrolled with.  Vaccinators will be required to check at a minimum the name, date of birth and contact details prior to giving a vaccine to an individual (to assist with accuracy and ensuring the correct person receives the vaccine).  To enrich the Consumer health record with details of the Vaccinator who provided the vaccination and

	the organisation and facilities where the vaccination event occurred.
<p>ISD or ISM User information from My Health Account (MHA):</p> <ul style="list-style-type: none"> <li>• First Name</li> <li>• Middle Name</li> <li>• Family Name</li> <li>• Mobile Number</li> <li>• Email</li> <li>• Confidence Level</li> <li>• CPN</li> </ul> <p>ISD or ISM User information via independent verification process:</p> <ul style="list-style-type: none"> <li>• First Name</li> <li>• Middle Name</li> <li>• Family Name</li> <li>• CPN</li> <li>• ImmuniseNow Username</li> <li>• CIR login Username</li> </ul>	<p>To verify the identification and approve access of AIR Users and to allow for auditing and monitoring of User access.</p> <p>MHA can be used to authenticate onto AIR. If the following details are held by MHA these will be passed to AIR for Identity Authentication. These details will only be passed with the MHA account holder’s consent. The information will not be stored in the ImmSoT – it will only be used operationally to approve User access.</p> <p>For those that do not or cannot use MHA, at least one of the following forms of identity verification and authentication must be collected to be onboarded onto AIR – CPN, ImmuniseNow, CIR.</p>
Login details of the User accessing the reporting functionality via PowerBI such as – name, email address	To verify the identity and approve access of a User to PowerBI.
Date and time of report download or view	To allow for auditing and monitoring of User access to the reporting functionality via ISD, ISM or PowerBI.

**Please state** the lawful purpose for the collection of this personal information

The collection of the above personal information is necessary to meet clinical requirements and is consistent with the overall purpose of AIR which is to provide timely and accurate understanding of population immunity to mitigate risks to public health, and to provide an accurate and complete set of vaccination data accessible to New Zealand health providers to ensure safe and effective Consumer health care.

	YES	NO
Could the project use <b>aggregated or anonymised data</b> and still satisfy the project’s purpose?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Is the project collecting <b>the minimum</b> amount of personal information required for the purpose of the project?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**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.

	YES	NO
Will the project be using cookies or other analytics?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
If <b>yes</b> , please provide further information: Click or tap here to enter text.		

**Compliance check with Principle 1**

Does the project comply with Principle 1?	YES	NO	UNSURE
The information is collected for a lawful purpose and the collection is necessary for that purpose	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**Principle 2:  
Collection directly from the individual concerned**

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

	YES	NO
Are you <b>only</b> collecting personal information <b>directly</b> from the individual?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

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

AIR will be collecting information from the following sources:

- Directly from the Vaccinator at the time of vaccination via the Immunisation Service Delivery (ISD) portal or Patient Management Systems (PMS)
- From the AIR administrators via the Immunisation Service Management (ISM) portal
- Migration of historical immunisation records from the NIR and CIR
- Te Whatu Ora existing systems – such as the NHI, HPI, NES
- Directly from Users when they access the AIR operational reporting functionality via the ISD, ISM or PowerBI.

**Immunisation Service Delivery (ISD) Portal and Immunisation Service Management (ISM) Portal**

Personal information collected at the time of a vaccination service to identify the Consumer and record the vaccination event details will be collected by the Vaccinator or other authorised person and entered in the ISD or PMS. The Vaccinator will confirm the identity of the Consumer prior to proceeding with the vaccination event and will record the following details in the ISD or PMS:

- NHI, DOB and gender of Consumer
- Provider details such as HPI and Facility ID
- Vaccination event details such as vaccine type, batch number
- Name of Related Person who has accompanied a child under 16 years.

Additional personal information already held by Te Whatu Ora in existing health identity systems (such as the NHI, HPI and NES) will only be used to enrich the vaccination event data when a query has been called – it will not be collected or stored in the AIR. These existing health identity systems are covered by their own PIA's.

The AIR administrators can upload personal information to correct the vaccination event details for the Consumer held in ImmSoT. They can also create a new vaccination record for a Consumer within AIR – such as uploading historical or overseas vaccination history as requested and consented by the Consumer. This process will be implemented using the FHIR Questionnaires (discussed in detail in the FHIR PIA). Only AIR admins who have authorised access via their My Health Account will have access to the FHIR form and IP whitelisting will be implemented to restrict access to Te Whatu Ora IP range. There will also be a mechanism in place to allow the Programme to see which information has been uploaded via the FHIR form and by who and carry out auditing activities on this process.

### Migration of NIR and CIR Consumer Records

#### *National Immunisation Register (NIR)*

The NIR privacy statement states that the NIR was established to facilitate delivery of vaccination services and provide an accurate record of Consumer vaccination history. It provides national and regional information on population vaccination coverage and assists in achieving New Zealand's vaccination coverage targets and controlling or eliminating vaccine preventable diseases.

These purposes of the NIR are in accordance with the proposed purposes of AIR. Therefore, personal information collected for the purposes of the NIR, can be migrated to AIR under IPP1 of the Privacy Act. There will be further privacy considerations to address as part of this migration, such as ensuring that the User access to and security of this personal information in AIR is the same or better than in NIR. These will be assessed in the Privacy Impact Assessment.

Currently the NIR provides enrolled Consumers with the option to decline that the immunisation service offer outcome and delivery is recorded and retained on the system. Once a Consumer has followed the process for opting off the NIR, no future immunisation services will be recorded. This option is a consequence of the construct of the NIR, in that the record held on the NIR is not the core clinical record - these are held in Patient Management Systems (PMS) or on paper consent forms in storage.

Where a Consumer has opted off the NIR, only records obtained in NIR prior to this opt-off will be migrated to AIR. A flag will also be created against the Consumer record to signal to providers that the Consumer has opted off the NIR. This will assist the Vaccinator in their engagement with the individual, as there will be an additional requirement to ensure the Consumer understands that this opt off is no longer applicable and has been replaced with the suppression process. The project should consider the creation of a separate privacy statement or collateral for Vaccinators to provide to Consumers who have been flagged as previously opted off. This will assist in ensuring the privacy principle of transparency is met.

If a Consumer wishes to retrospectively approve an immunisation event being recorded in AIR, from a period where that Consumer was opted off in the NIR, this is an allowable action under the Privacy Act 2020. Providers will need to be trained appropriately in how to obtain and record full and informed consent from the Consumer prior to migrating their records.

#### *COVID-19 Immunisation Register (CIR)*

The COVID-19 immunisation record held in the CIR is the primary clinical record for COVID-19 vaccinations, Consumers cannot choose to not have their COVID-19 vaccination data entered in CIR. However, Consumers could choose the preferred level of communication and if they would prefer not to share their identifiable data with Te Whatu Ora data sharing partners. The CIR also records if a Consumer decides not to get a COVID vaccination, including if there are medical reasons why they don't.

The CIR Privacy Statement available on the public facing website stated: "after you information is collected as part of the vaccination process it may be used for: managing your health, planning and funding future health services and keeping you and others safe". It was noted in this assessment that "if the CIR is to be replaced by a future national immunisation register for all national programmes, an

appropriate migration plan will be developed". It can therefore be assumed that a future register like AIR was not out of scope and the migration of CIR data to this platform would be an acceptable use of the data if proper privacy safeguards were put in place.

There is a potential for some Consumers to be upset when they hear that their personal information (such as name, DOB and address) is being migrated to a national register, as they may feel that they provided their personal information for a specific purpose – being COVID – and never intended for it to be included as part of a national data set. This will likely be caused by confusion and a misunderstanding of how AIR operates i.e., personal information such as name, DOB, address is pulled from the NHI and NES rather than the CIR, and the same people who will be accessing AIR had access to the CIR. The programme will need to ensure that the communications about AIR include this information to mitigate some of the unease.

During the COVID vaccination programme, names of vaccinators were recorded in the CIR rather than their associated HPI or CPN identifier. This creates an issue for migration of CIR data to AIR as AIR has no ability to record a vaccinator name. To get around this issue, AIR is going to create codes for vaccinator names in the CIR and link these codes to a vaccinator name in a SharePoint spreadsheet. Only the codes will be migrated to AIR and when a query about a vaccination event has been raised, the requestor will be referred to the facility associated with the code (via the SharePoint spreadsheet) or the Health Workforce Team. The spreadsheet will be locked down and will only be accessible to those who have approved access to it.

### Integration with External API Feeds and Existing Te Whatu Ora Systems

#### *The Orchestration Service*

The Orchestration Service is called both for message flows that originate from HealthLink (via PMS as discussed below) and for queries that are raised through the ISD/ISM portals. Depending on the location of the request and the additional information needed, the AIR Orchestration Service makes calls to the relevant back-end systems – ImmSoT, NHI, HPI and others to retrieve the required information before sending it back to the requestor.

All messages exchanged between HealthLink and the Orchestration Service, as well as messages between the Orchestration Service and AIR are in FHIR format. A separate PIA has been completed which covers the FHIR API functionality.

ImmSoT operates as a lean data model. When a query has been made to the AIR via the ISD/ISM or PMS, the purpose of the Orchestration Service is to enrich ImmSoT data with information from the HPI, NHI and NES. AIR information is returned to the requestor fully enriched with the data from these integrated systems.

The Orchestration Service process for the ISD/ISM portals as set out above will not be delivered in time for Cutover. Until this ideal state can be realised, the Orchestration layer will be bypassed, and the queries from ISD/ISM portals will go straight to the systems themselves through MuleSoft. With this bypass option, there will be no changes to the information being sent by the ISD and ISM and no changes to the information they will be receiving back from the source systems. The MuleSoft platform has the ability to filter out the irrelevant data retrieved from the source systems so that the ISD and ISM portals only receive the information necessary. HealthLink will still be going through the Orchestration Service.

#### *The Co-Existence Broker Service*

PMS systems currently communicate with the NIR through HealthLink. AIR is moving to a co-existence model where API's will be implemented between PMS systems and the ISD and ISM. These APIs will eventually be utilised by other Providers who do not have direct access to the ISD. Currently, PMS vendors need more time to effectively uptake these APIs, so the co-existence broker service is being developed to allow PMS systems and ISD to talk to each other in the meantime. This broker service is part of HealthLink.

The main purpose of the messaging allows for a status query to be made and for recording and editing a vaccination event. Messages are archived for up to 28 days – this is a standard process which is

happening now for the NIR. None of the messages themselves get stored, only logs and audits of the messages coming in and out are available. The translation is all encrypted and non-accessible.

Currently there is a standard messaging specification (such as naming rules and data exchange rules) that we have for messages sent and received by PMS vendors. For every message, there is a mapping spreadsheet which links the API field to the PMS system. At Cutover, there will be no change in the data types that we are sending or receiving, but some of the field lengths will have their character limit restrictions removed. This means that a couple of the fields will need to have their data truncated. The business is taking steps to make sure that there are no clinical risks associated with truncating these fields – such as truncating a long batch number.

**Operational Reporting Functionality**

Information about the User accessing the AIR via the ISD, ISM or PowerBI (such as name, email address, HPI and other logon details) will be collected directly from the User at the time of logging in to the relevant system. Users will be informed of this collection prior to being onboarded and will provide their informed consent via agreement to the Authorised User Agreement, Data Sharing Agreement and Privacy Declaration (as applicable). If there are any changes to personal information being collected or how this information will be used by the AIR, this will be communicated to the Users prior to their next login via a pop-up or in the case of PowerBI, an email.

**Please state** what legislative exception applies.

*The legislative exceptions can be found in Principle 2 of the Privacy Act and Rule 2 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact your Privacy Officer.*

Rule 2 of the Health Information Privacy Code allows for the collection of information from a source other than the individual concerned where compliance would prejudice the purposes of collection. The purpose of AIR is to provide an accurate and complete set of vaccination data for healthcare providers. To achieve this purpose, AIR needs to collect information from Consumers, healthcare providers, and existing Te Whatu Ora systems and records.

It would be unreasonable to expect Consumers to provide accurate identification and historical healthcare details every time they present for a vaccination service. To deliver safe and effective healthcare services, providers need to be certain that a vaccination record can be attributed to a particular individual and contains accurate vaccination event details.

**Please complete** the following table:

What personal information is collected from third parties?	Who is the third party?
Consumer NHI, DOB and gender Vaccination event details – such as vaccine type, batch number, name of Related Person Vaccinator details – such as HPI and Facility ID	General Practices and Vaccinators or Administrator at a facility that administers vaccinations

**Compliance check with Principle 2**

Does the project comply with Principle 2?	YES	NO	UNSURE
Are you collecting directly from the individual concerned (or an exception applies)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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



### Principle 3: Telling the individual what we are doing

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

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

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

	YES	NO
Will the project be telling an individual all the matters in Principle 3?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- 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?*

A full communications package has been prepared by the AIR programme which will be provided to Vaccinators and Administrators working in the AIR, so that they can have informed conversations with Consumers who require additional information. This package includes additional resources for Consumers, resources for HealthCare Providers and Administrators, links to AIR Website Content, and a Privacy Response Letter Template to ensure consistent messaging from the AIR programme.

Individuals will be told in a variety of formats how their information will be managed, these include:

- Privacy statement on Te Whatu Ora website – AIR page.
- Privacy statement read out to the Consumer at the point of vaccination.
- Privacy statement provided during Vaccinator onboarding to ISD, ISM and PowerBI.
- AIR information leaflet.

*Privacy Statement on Webpage*

The AIR programme will have a webpage on the Te Whatu Ora website which sets out the privacy statement for AIR and provides more in-depth details about the operation of AIR and how their information will be managed. The webpage will also include links to other Te Whatu Ora webpages (such as the NHI) which will have supporting information about how these systems interact with AIR.

*Privacy Statement and Consent for Consumer*

Consumers will be read a short form privacy statement and declaration prior to receiving a vaccination service. Vaccinators will be required to tick a box confirming that the Consumer has understood the content of the privacy statement and has provided their informed consent to receive the vaccination. If Consumers require further information before providing informed consent, they will be given additional

resources (such as the AIR information leaflet) and directed to the AIR webpage and the programme's Privacy Officers details.

#### *Privacy Statement for Vaccinators*

Vaccinators and administrative staff who have access to the ISD/ISM portals will be provided with a privacy statement when they are onboarded to the portals. They will also be required to sign Authorised User Agreements which specify that the User has read and agreed to the privacy statement to be granted access.

#### *AIR Information Leaflet*

An information leaflet will be available for any Consumers who require further and more in-depth information about AIR to provide informed consent. This leaflet will contain details about who the Consumer can contact for any queries or complaints and will provide links to other online resources (such as the AIR webpage).

#### *Privacy Declaration for PowerBI Users*

Users who have access to PowerBI will also be provided with a privacy declaration which they are required to read and accept during the onboarding process. Users will not be onboarded to PowerBI without a Data Sharing Agreement in place which specifies that the User has read and agreed to the privacy declaration to be granted access.

**Where** will the document be made accessible?

*For example, will it be published online? Link in an email? Hard copy?*

As per the above, the resources will be made available online, verbally and in hard copy.

**Please** include as an **appendix** a copy of any draft document that outlines how you will manage an individual's personal information.

## **B. When you are going to tell the individual**

Will you tell individuals before or after you have collected their information?

If you're telling the individuals after you have collected their information, how long after?

Consumers will be told prior to receiving a vaccination service that their identification and vaccination event details will be collected. If individuals do not provide their informed consent, this information will not be collected.

Vaccinators and AIR Admins will be made aware of what information is collected about them when they are onboarded on to the ISM or ISD portals. They will be required to sign an Authorised User Agreement which sets out what information will be collected about them and how it will be managed. If there are any changes to their personal information being collected or how this information will be used by the AIR programme, this will be communicated to the Users at the time of their next login via a pop up.

Other Users accessing the reporting functionality via PowerBI will be informed prior to being onboarded. If there are any changes to their personal information being collected or how this information will be used by the AIR programme, this will be communicated to the Users via an email.

## **C. Mandatory or voluntary collection**

**Please state** whether the collection of information is voluntary or mandatory?

If Consumers wish to receive a vaccination service, it is necessary for the data associated with the vaccination service to be recorded in AIR. Te Whatu Ora acknowledges that consumer choice is a requirement under the Health Information Governance Guidelines, but this must be balanced against the need for complete, accurate and up to date clinical records of healthcare.

The suppression process implemented by AIR does not inhibit all vaccination information being recorded in the AIR. However, if a consumer receives a vaccination, they can elect to have their information suppressed, which will stop the information being visible or shared to other parties outside Te Whatu Ora.

Individuals can request to have their records suppressed by emailing the Te Whatu Ora privacy team. A form will then be provided to the consumer outlining the impact of their decision and seeking confirmation of the decision to suppress.

**Please state** to what extent, if any, the individual can opt out of providing some or all their information

Consumers are unable to opt out of providing any of their information if they elect to receive a vaccination service. This is a change from the operational process under the historical National Immunisation Register. Instead, the Programme has elected to implement a ‘suppression’ process as outlined above.

**Please state** what happens if the individual does not want to disclose their information?

If the Consumer wants to receive a vaccination service but does not want their information to be captured in AIR, they will be able to request that this information to be suppressed. Vaccinators and AIR Admins will be provided with resources to have informed discussions with Consumers around what it means to have their information captured within AIR. These resources will include information about the suppression process and provide additional contact information for Consumers to get in touch directly with the AIR programme if they require further information and guidance or to lay a complaint.

There is a risk that consumers will choose not to be vaccinated because of the collection of their information in the AIR. This risk will need to be weighed against the alternative risk of over vaccinating a consumer or not having a clear understanding of population immunity and coverage.

The AIR programme is very aware of this risk and is taking all possible steps to ensure that individuals are informed and understand the purposes behind AIR and the reasons for this collection. The suppression process, additional resources and informed conversations with vaccinators and other health service professionals will play a large role in educating individuals and lowering the risk threshold. This issue is discussed further in Risk 1 of the Risk Table included as Appendix 2.

Ongoing engagement with the Office of the Privacy Commissioner is also recommended to check in with complaints and queries that have been made by the public in relation to the collection of their information in the AIR.

**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?

Not applicable.

**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.

**Compliance check with Principle 3**

Does the project comply with Principle 3?	YES	NO	UNSURE
Are you telling the individual how the project will handle their personal information (either before or as soon as practicable after the information is collected) or an exception applies?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

## Principle 4: Fair and lawful collection of information

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



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

<p><b>Please describe</b> the current proposed method of information collection <i>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</i></p>
<p>Information will not be recorded by the ISD/ISM portals or PMS without informed consent being obtained first. Consumers will always have the option to decline a vaccination service if they do not consent to their information being collected by the AIR.</p> <p>ImmSoT does not have a front facing interface to collect personal information. Instead, Vaccinators and AIR Admins will record information directly in the ISD/ISM portals or Patient Management Systems (PMS). These portals then feed the vaccination event information into the ImmSoT. The existing data stored by the NHI, HPI and NES systems will be used by ImmSoT (via the Orchestration Service) to enrich the vaccination event details when a query has been made, but it will not be collected or stored in ImmSoT itself. This use of the data from the source systems is authorised as it is in accordance with the purposes for which the information was obtained (this is discussed further under Principle 2). This entire information flow is what is referred to when data is said to be collected and stored in the AIR.</p> <p>The reporting functionality does not collect personal information about Consumers itself. Rather, it utilises Consumer personal information already recorded in the AIR. Information about the User accessing the reporting functionality (such as name, email address, HPI facility ID) will be provided directly by the User at the point of logging in to the ISD/ISM portal or PowerBI. This information is not collected without the User providing their informed consent via express agreement to the terms and conditions of onboarding.</p>
<p>If you’re collecting information from children or young people, <b>please state</b> what steps are you taking to address any power imbalance, and to obtain genuine consent for the collection (or authorisation) of their family/whānau?</p>
<p>All Vaccinators will have received training as healthcare professionals on how to obtain informed consent from young people or from their legal guardians if required. Vaccinators and AIR Admins will also sign Authorised User Agreements before being onboarded to the ISD/ISM portals which set out their obligations in relation to the collection of personal information from children or young people.</p> <p>Vaccinators will also record the name of a person who has accompanied a child under 16 years old in the ISD or PMS. This name is collected and stored in ImmSoT.</p>
<p>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</p>
<p>Statistics have illustrated that Māori and Pasifika populations are disproportionately affected by infectious diseases such as Measles. The purpose of AIR as an immunisation source of truth enables the health care sector to identify areas where population immunity against a certain disease is low and allows them to take steps to contact affected Consumers.</p>

The COVID-19 response illustrated the importance of providing access to our community and iwi led organisations to assist in engaging with unvaccinated Consumers. The AIR programme intends to implement these learnings by providing for outreach activities (discussed in the Whaihua PIA) and reliance on the Te Whatu Ora Data Governance Group to enter into Data Sharing Agreements with certain community and cultural groups where it is appropriate to meet the purposes of AIR.

Decisions about sharing with community and iwi led organisations is beyond the authority of the AIR programme – this will continue to be a Te Whatu Ora led approval process. The AIR programme has also engaged with the Whanau, Consumer and Clinical Digital Council (WCCDC). The design and purposes of AIR was presented to the WCCDC, and no high-level objections or action points were raised.

The AIR programme has also engaged with Refugee Centres. These centres currently use PMS systems when carrying out a general health check for a refugee and working out an appropriate vaccination schedule for them. It is not uncommon for the refugee to lose contact with the healthcare sector once they have moved out of these Refugee Centres (given the current difficulties with obtaining enrolment at a General Practice).

The integration of PMS systems with AIR enables the refugee’s immunisation history to be collated in one source of truth location and ensures that their vaccination schedule will be followed up on by the AIR programme when required. Staff at the Refugee Centres will receive the same training and information brochures as other AIR Vaccinators and will be required to ensure that their Consumer fully understands and consents to their information being collected by the AIR prior to delivering a vaccination service.

**Compliance check with Principle 4**

Does the project comply with Principle 4?	YES	NO	UNSURE
Are you collecting information in a lawful manner and by means that are fair and not intrusive?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**Principle 5:  
Storage and security**

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

**A. Cloud Computing Services**

	YES	NO
Does your project/solution use any cloud-based services? <i>Cloud services are infrastructure, platforms, or software that are hosted by third-party providers and made available to Users through the internet.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The ImmSoT and the Orchestration Service are located on the Amazon Web Services (AWS) Cloud Infrastructure infrastructure based in Sydney, Australia. This is an existing cloud service utilised by Te Whatu Ora and has received IT Security and Privacy approvals to operate.

The information ‘held’ via AWS is personal information being held by AWS as agent for Te Whatu Ora in accordance with section 11 of the Privacy Act 2020. Data stored within AWS is encrypted. Te Whatu Ora

controls access to the encryption keys and the data. The information is not to be used or disclosed for any purposes other than those directly permitted by the AIR.

The front-end User interfaces (the ISD/ISM) are located on the Salesforce platform. This is an existing cloud service utilised by Te Whatu Ora and has received IT Security and Privacy approvals to operate.

**B. Engaging with Information Security**

	YES	NO
Have you engaged your relevant information security team for this project/solution?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Has a Security Risk Assessment (SRA) been completed by your relevant information security team?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Has a Cloud Service Provider Due Diligence Questionnaire been completed by your relevant information security team?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Please provide a further information:</p> <p>Information stored in the AIR will be covered by the NSS Data Policy, this aligns with the relevant HISO standards, including HISO 10029:2015 Health Information Security Framework, and the New Zealand Information Security Manual.</p> <p>Access to the AIR via the ISD and ISM will require multifactor authentication, via a log-in and password for registered Users. All access from Users outside Te Whatu Ora will be through the ‘immunisation community’, which is a Salesforce community that provides an application specific to the function they are performing. Access will only be permitted to the level of data required for their function – i.e., recording a vaccination and managing the patient.</p> <p>Information collected by the ISD, ISM and PMS will be encrypted in transit and all personally identifiable and clinical data is encrypted in storage in the ImmSoT. The role-based access for Vaccinators and Administrators will be able to be tracked and monitored. It is anticipated that proactive tracking and monitoring will take place, rather than it being implemented retrospectively once a risk has been realised.</p>		

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

**C. Storage**

<b>Please describe</b> the system and location where the information is stored?
The only information stored in the AIR (within ImmSoT) is the vaccination event data captured by the ISD portal and PMS. All other information is stored in existing locations (such as the NHI, HPI and NES), and is pulled straight from these systems to enrich the ImmSoT vaccination event data when a direct query has been made to the AIR. These existing locations have received their own Privacy and Information Security Risk Assessments.

**D. Access**

<b>Please state</b> the roles that will have access to the personal information and <b>describe</b> why these roles need access to the personal information
Only Users who have been onboarded to the ISD/ISM portals or PowerBI or have access to a PMS will have access to the vaccination event information stored in AIR. Users will not have access to ImmSoT directly. Instead, they will access the data by raising a query through their PMS, ISD/ISM portal or PowerBI which will pull the vaccination event information from ImmSoT and enrich it with associated information within the NHI, HPI and NES. Access to this data is required by Users to meet the purposes of AIR which is to provide timely and accurate understanding of population immunity to mitigate risks to public health, and

to provide an accurate and complete set of vaccination data accessible to New Zealand health providers to ensure safe and effective consumer health care.

Authorised Te Whatu Ora technical teams will have direct access to the data within the ImmSoT for the purposes of providing technical support and system updates.

**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)

Users are onboarded to the ISD and ISM via the same processes which were put in place to onboard Users onto the CIR. Authorised Users for accessing the ISD will be Vaccinators who are involved with the process of administering the vaccines to be recorded in the AIR. AIR Administrator (former NIR Administrator) will be given access to provide support via the ISM function.

Vaccinators and AIR Administrators will be onboarded using AIR's onboarding workflow, that includes the use of My Health Account (MHA) for some AIR Users. MHA is a digital identity tool and a way for the health workforce to access Te Whatu Ora applications securely. MHA will be used in the onboarding workflow to establish the verified identity and CPN attribute for some of AIR Users. These credentials will be used in the initial account set-up and once that has been established Users will be able to use their MHA to log into AIR.

Access to the data stored in the AIR via the ISD and ISM and PowerBI will require multifactor authentication using a unique log-on and password. Users of the ISD, ISM and PowerBI will be:

- Vaccinators administering the vaccination service.
- Administration staff with responsibility to support the vaccination services (e.g., upload of the Consumer cohort that is to be vaccinated, reporting, planning, and supporting the clinical administration of the vaccine).
- Te Whatu Ora (for non-identifiable reporting activities).
- Third Parties (such as PHO's) who require data for the effective delivery of healthcare services.

Users will only be granted the minimum amount of access to data needed to carry out their function. Access limitations will be set by the AIR programme when onboarding Users to the ISD/ISM portals or PowerBI. The role/function-based access for ISD/ISM and PowerBI Users will be able to be tracked and monitored. It is anticipated that proactive tracking and monitoring will take place, rather than it being implemented retrospectively once a risk has been realised.

The AIR programme has a procedure in place which governs the onboarding and offboarding of Users to AIR. This procedure is located on the AIR Programme's internal confluence page, which is accessed by all parties who are responsible for approving or removing User access to AIR. This confluence page has been reviewed by Privacy.

All Users of the ISD and ISM are required to read and accept the Authorised User Agreement (AUA) prior to accessing the system for the first time. The information set out within the AUA informs Users that their activities on the ISD and ISM are monitored and auditable and includes the consequences if any of the terms are breached. Similarly, all Users who are onboarded to PowerBI will be required to read and accept the Data Sharing Agreement between Te Whatu Ora and the User and the terms of the Privacy Declaration which will set out the privacy expectations and inform Users that their use of PowerBI will be monitored and auditable.

There is no ability for PowerBI users to "accept" privacy terms and conditions via a tick box when they first log in to PowerBI. Instead, PowerBI users will be sent an onboarding email when they have been approved for access to AIR data via PowerBI. This onboarding email will contain a link to PowerBI and a disclaimer statement (attached as an Additional Appendix) which states that in accessing PowerBI the user agrees to comply with the specified terms of the disclaimer. Users will not be able to reply or confirm back to this email, so their login to PowerBI will be taken as acceptance to the terms. In addition, there will be a link to the Privacy Statement and a reiteration of the email disclaimer located on the Information Tab of the PowerBI portal.

Will access be controlled <b>by at least two-factor authentication?</b>			
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.	<b>YES</b>	<b>NO</b>	<b>NA</b>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**E. Auditing Accounts**

**Please state:**

- if, and to what extent, the project can audit User access to the personal information
- what will be audited, who will 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.

Auditing mechanisms are set out in more detail in the ATO completed for the AIR programme by the Information Security team. This includes the technical processes for the AIR programme to audit User access to personal information. While the programme cannot always monitor User access to all information, flags will be raised where an account displays suspicious browsing activity (such as accessing a large amount of personal information in a short time or accessing the personal information of a “special” person). It has been recommended to the programme that proactive audits should be undertaken by the programme on a regular basis such as quarterly (rather than waiting for a complaint to be raised).

In addition, access by ISD users must be reviewed by Facility Managers on a regular basis to determine whether the access of the User is still appropriate. This includes individual users’ facility access and whether this access is also still necessary. This requirement is set out in the Terms of Use and onboarding documentation provided to Facility Managers.

**F. Any other Information**

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

**For example:**

- *Is information encrypted at rest and in transit? What other relevant safeguards are utilised during the transit of information?*
- *Is there a need for additional privacy training, new policies, processes, or contracts?*
- *How will you keep physical copies of documents secure?*
- *How will you ensure conversations are not overheard?*
- *What checks will be done to ensure you’re talking to, and sharing information with, the right person?*
- *What are the security 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?*

All information stored as part of the AIR will be marked as In-Confidence or Medical In-Confidence.

The ISD has a business continuity plan in place for when the system is offline or unavailable. If this eventuates, the Vaccinators and Administrator will default to using paper vaccination forms and their existing offline processes. The paper forms and other documentation will be manually loaded into the ISD by the Administrator once the system is back online.

All on-site physical copies of medical records are assumed to be managed and stored securely in accordance with industry best practice. The below process is an example of what best practice may look



like in this context, however ultimately it is up to the Vaccinators and Facility to implement a process which ensures they are adhering to and meeting industry best practice processes:

- All physical documentation collected at Facilities which contain patient personal information will be securely stored out of the sight of patients (e.g., a drawer), with the drawer preferably locked or in the constant presence of an authorised person (such as an Administrator, security guard or Vaccinator).

At the conclusion of the immunisation event, the documentation needs to be taken directly (no transit points) by an authorised person, to the site where the documentation will be securely held until disposed of in accordance with the applicable retention and disposal requirements.

**Compliance check with Principle 5**

Does the project comply with Principle 5?	YES	NO	UNSURE
When the project holds personal information, is it using security safeguards that are reasonable to protect against loss, access, use, modification, disclosure, or other misuse?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**Principle 6:  
Access to personal information**

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

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

**Please outline** how individuals will be able to access their information.  
*For example, will it be through existing information request processes (for example, requests for clinical records), or will a new process need to be put in place?*

Individuals will have access to their personal information through existing mechanisms for requesting access to their clinical records held in the NIR. This existing process will be leveraged by the AIR programme.

The AIR privacy statement will inform individuals of the process for requesting access to their information, and this information will also be made available on the AIR webpage. As part of their AIR onboarding training and acceptance of the Authorised User Agreement, Vaccinators and administrative staff at health care facilities will be aware of their obligation to inform individuals of how they can access their information.

Users who have access to reports containing personal information via PowerBI will be required to follow their own internal processes for providing individuals with access to the information contained in the reports that they have downloaded. These Users will need to have clear processes in place for providing individuals with access to their information and for redacting or removing information from reports that does not belong to the requesting individual. The Users will be required to confirm that they have processes for this when they enter into a Data Sharing Agreement with Te Whatu Ora. Where an individual has contacted a User and asked for access to their information contained in AIR itself (not just the reports held by the User), the User will direct the individual to the AIR programme nominated address for access requests. This information will be made available to the User via the privacy statement on PowerBI.

**Please outline** how you intend to ensure that it is possible to find the information about a specific individual?

Anyone with access to the ISD/ISM portals or PMS will be able to extract the information about a specific individual. These Users will be able to input an individual’s NHI into the portal and this will send a query to the ImmSoT data repository and Orchestration Service to return the vaccination event details and personal identification details associated with that NHI.

PowerBI Users will have access to different levels of identifiable data depending on their approved access. Where a User is only able to view aggregated and anonymised data fields, they will be unable to locate the information pertaining to a specific individual. In this instance, the individual should be directed to the AIR programme as stated above. Where Users have access to reports containing individual level data, they will be able to find the information about a specific individual by matching their provided information to the information in the report. Users will be required to have their own processes in place for collecting information from the individual (such as name, DOB, NHI etc) to carry out the matching with the data in the reports.

The reporting and query process has been tested extensively by the AIR programme technical team. As part of the UAT and reporting testing, the flow of information was tested to ensure that the API’s connected to the ISD/ISM, PMS, ImmSoT data repository and Orchestration Service returned the correct information associated with a particular individual before the system went live.

**Compliance with Principle 6**

Does the project comply with Principle 6?	YES	NO	UNSURE
Is there a process in place to ensure an individual can ask Te Whatu Ora if it holds personal information about them and the individual can access that information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**Principle 7:  
Request to ask for correction of information**

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

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

Individuals will have the ability to correct their personal information through existing mechanisms for requesting correction to their clinical records held in the NIR. This existing process will be leveraged by the AIR programme.

A Consumer can request correction of their personal information held in the AIR directly with the Vaccinator. Any changes will be auditable within the system (date, change made, User who made change). If it is a clinical record however, it is essential that the integrity of these records in maintained. A process will need to be in place to manage any such request.

Where an individual has made a request to a PowerBI User to correct their information, they should be directed to the AIR programme. The AIR privacy statement will inform individuals of the process for requesting correction of their information, and this information will also be made available on the AIR webpage. PowerBI are unable to correct any individual’s information via PowerBI, as PowerBI only generates reports using information extracted from other systems.

The AIR privacy statement will inform individuals of the process for requesting correction of their information, and this information will also be made available on the AIR webpage. As part of their AIR onboarding training and acceptance of the Authorised User Agreement, Vaccinators and administrative staff at health care facilities will be aware of their obligation to inform individuals of how they can correct their information.

**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?

Anyone with access to the ISD/ISM portals or PMS will be able to access the information about a specific individual. The Users will be able to input an individual’s NHI into the portal or PMS and this will send a query to the ImmSoT data repository and Orchestration Service to return the vaccination event details and personal identification details associated with that NHI. There will be a process in place to verify an individual’s request to correct their personal information (this will be set out in the Authorised User Agreement) and the process for adding a statement of correction to the record. This statement will form part of the individual’s clinical record.

The reporting and query process has been tested extensively by the AIR programme technical team. As part of the UAT and reporting testing, the flow of information was tested to ensure that the API’s connected to the ISD/ISM, PMS, ImmSoT data repository and Orchestration Service returned the correct information associated with a particular individual before the system went live.

**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?*

A business decision was made that notes cannot be added to the Consumer record via the ISD and ISM to record a Consumer request for their personal information to be corrected. Under the NIR the notes' function was not being used often, and where it was being used it was done poorly, resulting in unnecessary information being collected that had no purpose. In this instance, the risk of holding unnecessary and inaccurate information in a centralised system is greater than the risk of Consumers being unable to request the correction of their information within the AIR.

Instead, Consumers are still able to request for their information to be corrected at their GP via notes added to the Consumer record on the PMS system. As it is a clinical record, it is essential that the integrity of the record is maintained. However, this needs to be weighed against the Consumers right under the Privacy Act to have their request for correction noted. Allowing for notes to be added to the PMS record allows for this right to be exercised while maintaining the integrity of the clinical record within AIR.

There is no ability to attach a statement of correction to the reports generated via PowerBI.

**Compliance check with Principle 7**

Does the project comply with Principle 7?	YES	NO	UNSURE
Is there a process in place to enable an individual to request the correction of their personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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



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

### How will you ensure that only **accurate, up to date, complete and relevant** information is acted on?

There is a risk that Vaccinators may elect to still vaccinate Consumers who do not wish to be recorded on the AIR. This would put the integrity and accuracy of the AIR as a centralised immunisation source of truth at risk and reduces the health sectors understanding of population immunity and coverage. It would also increase the risk of over vaccinating the Consumer next time they present for a vaccination service or affect the programme's ability to contact a Consumer if there are issues with the vaccine batch.

Relying on contractual agreements alone is unlikely to provide sufficient compliance. The programme has put additional mechanisms in place to encourage compliance with compulsory collection – such as the development of the full communications package which will be provided to vaccinators and administrators working in the AIR, so that they can have informed conversations with Consumers who require additional information. This package includes additional resources for Consumers, resources for HealthCare Providers and Administrators, links to AIR Website Content, and a Privacy Response Letter Template to ensure consistent messaging from the AIR programme.

In addition, the future operational reporting function within AIR will ensure that providers are only being paid for the vaccinations which have been recorded in AIR. If providers choose to vaccinate an individual and not record this in AIR, then they will not receive public funding.

The Consumers data pulled from the existing integrated systems such as NHI and NES (via the Orchestration Service) will be checked with the Consumer at each vaccination event to ensure that their name and details align with the Consumer presenting for their vaccination. If the information is found to be inaccurate at this point, it will need to be updated in a separate application (Health User Interface) connected to the NHI system.

The use of the NES contact details, where available, will assist to make the information as up to date as reasonably possible at the outset. The NES information is expected to be relatively accurate, up to date, and complete in accordance with contractual obligations under the PHO Agreement – but not all individuals have a current phone or email contact on the NES. An additional operational control is that each Vaccinator will be expected to check these details directly with Consumers at each attendance as part of Standard Operating Procedures.

Technical controls will also be employed to enhance accuracy. The AIR will flag inconsistencies between the NHI information contained in the system and the details provided by the Consumer presenting for vaccination. These will need to be put into a queue for data fixing as per the processes outlined in this PIA – the User is not able to update NHI details within AIR.

The ISD and ISM will not have any free text manual entry fields to help with accuracy. The ISD will also be designed to help Vaccinator's progress through each step in a logical and nationally consistent manner.

As the reporting functionalities are pulling information from other systems and do not collect personal information themselves, they will be relying on these other systems to have processes in place to ensure the information is up to date. Where a PowerBI User is informed by an individual that the information about them in the report is inaccurate, the PowerBI User must contact the AIR programme and follow the process for correction of information.

**Compliance check with Principle 8**

Does the project comply with Principle 8?	YES	NO	UNSURE
Does the project ensure that information is accurate, up to date, complete and relevant before the information is used?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**Principle 9:  
Do not keep information longer than necessary**

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



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

<b>Please state</b> how long the information will be held by Te Whatu Ora
<p>Consumer information will be maintained within the AIR in accordance with the Health (Retention of Health Information) Regulations as it is clinical information. Audit records of access to the AIR via ISD/ISM portals, PMS and PowerBI will be retained for a minimum of two years. The Te Whatu Ora Data Governance Group will be responsible for ensuring that personal information and any other data is securely deleted once legally able to be disposed of.</p> <p>Retention is also likely to be aligned to national dataset collections and may be retained indefinitely (as implications for individuals into the future may require retention of a full record of what immunisation was provided and when).</p> <p>User generated reports will not be stored within the reporting functionalities. Users will generate real time reporting via the functionality and will then download the report if a copy is required. Users who have downloaded a report will be responsible for always complying with the requirements of the Privacy Act and the Health (Retention of Health Information) Regulations, particularly around the storage and retention of these downloaded reports. The Users will agree to these obligations when entering into the Data Sharing Agreement which provides them with access to PowerBI, or when they have accepted the Authorised User Agreement as part of onboarding to the ISD or ISM.</p>
Please <b>state</b> the applicable legal requirements for retention of information (if any). <i>For example, Health (Retention of Health Information) Regulations 1996, Public Records Act 2005, General Disposal Authority 6, Functional Disposal Authority 1.</i>
As per the above.
<b>Please state:</b>
<ul style="list-style-type: none"> <li>• whether all the personal information needs to be retained by the project</li> <li>• whether the information needs to be retained in a form that identifies the individual (<i>can it be retained in a de-identified manner</i>)</li> </ul>

Users will only be able to generate reports with the level of identifiable information allowable pursuant to their use cases and function. This will be determined by Te Whatu Ora when onboarding the Users to ISD/ISM and PowerBI.

**Please state:**

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

As per the above.

**Note:** We also recommend:

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

**Compliance check with Principle 9**

Does the project comply with Principle 9?	YES	NO	UNSURE
Subject to satisfying any records management requirements, personal information is only retained for as long as it is required for the purposes of the project	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**Principle 10:**  
**Limits on use of personal information**

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



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

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

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

The AIR Privacy Statement will clearly describe for Consumers the purposes for which the information collected by the AIR may be used. These uses are in line with the purpose of AIR and include the following:

- Managing Consumer health
- Keeping Consumers and others safe
- Planning and funding future health services
- Carrying out authorised research
- Training health care professionals
- Preparing and publishing statistics
- Improving publicly funded health services
- Enabling broader health and social support services

Third parties will be provided with access to the information within AIR if they require access to carry out one or more of the above functions. Function creep is a risk that the AIR must guard against. Access will be restricted so that they can only view the minimum amount of identifiable information needed to carry out their function. Key controls to prevent this function creep are as follows:

- the implementation of a Data Governance Group that will be responsible for overseeing and approving access to any party and ensuring that Data Sharing Agreements are entered into which set out clearly defined expectations,
- an AIR data governance strategy that will require oversight of any proposed changes to uses of the information held by AIR or the expansion of Users, and
- technical controls, such as limiting ISD, ISM and PowerBI Users, or controlling the features that can be accessed via these mechanisms (such as non-identifiable reporting for third parties except where identifiable information is essential).

	YES	NO
Are the uses listed above consistent with the purposes of collection you have outlined in Principle 1?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If the answer is “No”, please state what legislative exception applies. <i>The legislative exceptions can be found in <u>Principle 10</u> of the Privacy Act or <u>Rule 10</u> of the Health Information Privacy Code. If you’re unsure if an exception applies, please contact your Privacy Officer.</i>		
Not applicable.		

	YES	NO
Does the use of information by the project involve information matching or sharing?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If the answer is “yes”, please provide more information here. <i>Please consider any additional issues that may arise (for example, the need for agreements to enable and regulate matching and sharing). Please annex any relevant documents to this PIA.</i>		
The ImmSoT, and ISD and ISM portals will collect unique identifiers (such as NHI and HPI) to match the vaccination event against the Consumer records and Vaccinator information held in the existing NHI, HPI and NES source systems. This is an approved use of the unique identifiers which have been implemented by Te Whatu Ora.  Information is shared with third parties for reporting purposes. As discussed throughout this PIA, third parties will only receive the information it needs to effectively carry out its function. Its function must be related to one of the purposes of collection set out in the ImmSoT PIA.		

**Compliance check with Principle 10**

Does the project comply with Principle 10?	YES	NO	UNSURE
Will the personal information only be used for the purpose it was obtained or an exception applies?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

## Principle 11: Limits on disclosure of personal information

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



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

	YES	NO
Will the project disclose personal information to individuals or agencies outside of Te Whatu Ora?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

**Please state** the basis for disclosing personal information  
*The grounds can be found in Principle 11 of the Privacy Act or Rule 11 of the Health Information Privacy Code. If you’re unsure if an exception applies, please contact your Privacy Officer.*

AIR will rely on Rule 11(1)(c) of the Health Information Code which allows for an agency that holds health information to disclose the information if the disclosure of the information is one of the purposes in connection with which the information was obtained.

Information is shared with third parties for reporting purposes. As discussed throughout this PIA, third parties will only receive the information it needs to effectively carry out its function. Its function must be related to one of the purposes of AIR as set out in this PIA. This is an allowable disclosure under Clause 1(a) of Information Privacy Principle 11 - that the disclosure of the information is directly related to one of the purposes in connection with which the information was obtained.

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
- outline what safeguards will be put in place to ensure that the information is secure once it has been shared with the third party

The project will share personal information collected in AIR with third parties where they are an agency that provides a health care service (or a service connected to health care) and the information shared is only the minimum amount necessary for the agency to carry out that service. As stated above, this is an allowable share under the Health Information Privacy Code.

Prior to disclosing this information to a third party, a Data Sharing Agreement will be required to be entered into between Te Whatu Ora and the third party. This Data Sharing Agreement will be put in place by the National Immunisation Programme Data Governance Group (or equivalent group set up to be responsible for governing the use and disclosure of data collected under the AIR programme). The Data Sharing Agreement will set out the purpose for the third-party access to the data and include parameters around use and disclosure.

### Compliance with Principle 11

Does the project comply with Principle 11?	YES	NO	UNSURE
--	-----	----	--------



Personal information is not disclosed to an individual or agency outside of Te Whatu Ora or an exception applies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--	-------------------------------------	--------------------------	--------------------------

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

## Principle 12: Disclosure of information outside of New Zealand

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

- The individual authorises it in situations where B may not be able to protect the information to the same degree as a 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 Te Whatu Ora – Health New Zealand disclose personal information to a foreign person or entity?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

**Please state:**

- The foreign entities or persons that we will be disclosing personal information to
- Where the foreign entities or persons are based (i.e., which jurisdiction)
- Why the foreign entity or person needs to have the personal information
- what evidence you have that the foreign entity receiving information has the same safeguards available to protect the information as are provided under the Privacy Act 2020.
  - If the foreign entity cannot provide the same safeguards, indicate whether that has been explained to the individual, what has been explained and whether the individual consents to the sharing of their information with the foreign entity. Please provide evidence of that consent.
- Provide details on what safeguards have been put in place to protect the individual’s information (such as a contract or an agreement with the foreign entity).
- Has an ethics or research committee, such as Health and Disability Ethics Committee, approved overseas disclosure?

Not applicable.

### Compliance check with Principle 12

Does the project comply with Principle 12?	YES	NO	UNSURE
Personal information is not disclosed outside of New Zealand, or it is authorised under Principle 12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**Principle 13:**  
**Creation or use of unique identifiers**

**Principle 13** of the Privacy Act 2020 says an agency may only **assign** a unique identifier to an individual if that identifier is necessary to enable the agency to carry out 1 or more of its functions effectively.

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

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

	YES	NO
Will the project <b>assign</b> unique identifiers?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Will the project <b>use</b> unique identifiers?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

**Please explain:**

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

AIR will use existing NHI (National Health Index) and HPI (Health Practitioner Identifier) numbers to identify Consumers and health practitioners and assign AIR records accordingly. It will also use HPI-FID (Health Provider Identifier Facility Identification) codes to identify the facility that a vaccination was given. Providers will be required to take reasonable steps to ensure accuracy of NHI and CPN details submitted to the Register. Unique identifiers will be displayed in the reports generated by Users via the reporting functionalities.

The AIR will take reasonable steps to make sure unique NHI identifier is only assigned to an individual whose identity is clearly established (Rule 13(6)) – the AIR will catch entries that are not consistent with the NHI record held and these will be put into a queue for data fixing, before being collected by the datastore.

These existing unique identifiers have previously been assigned by the Ministry of Health and are now governed by Te Whatu Ora. The proposed use of these identifiers by AIR falls within the purposes and use cases for which they were originally created.

AIR will not create or assign any other new unique identifiers.

**Compliance check with Principle 13**

Does the project comply with Principle 13?	YES	NO	UNSURE
Will the project be using or assigning unique identifiers?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

## Artificial Intelligence

There is no single, universally accepted definition for Artificial Intelligence (AI). For the purposes of this PIA, we use the definition for AI from New Zealand's AI Forum - *“advanced technologies that enable machines to reproduce or surpass abilities that would require intelligence is humans were to perform them. This includes technologies that enable machines to learn and adapt, to sense and interact, to reason, predict and plan, to optimise procedures and parameters, to operate autonomously, to be create, and to extract knowledge from large amounts of data”*<sup>1</sup>.

Use of Artificial Intelligence at Te Whatu Ora	YES	NO
Does your project/solution involve the design, development, deployment, and/or use of any form of AI?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

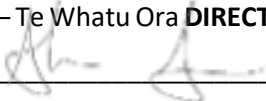
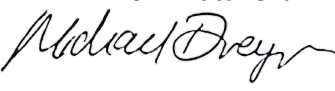
If you have answered 'yes' to this question, please complete the **“Assessment- Artificial Intelligence at Te Whatu Ora”**. Please contact your Privacy Officer/ Privacy team for more information.

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

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

<sup>1</sup> As defined by AI Forum in The New Zealand AI Impacts Research Project, May 2018.

**Review and Sign Off**

<b>Privacy Officer</b>	
Name: <b>VIV KERR</b> – Te Whatu Ora <b>INTERIM HEAD OF PRIVACY</b> Signature: <u>Viv Kerr</u>	Date: <u>3</u> / <u>12</u> / <u>2023</u>
<b>Director Prevention</b>	
Name: <b>ALANA EWE-SNOW</b> – Te Whatu Ora <b>DIRECTOR PREVENTION</b> Signature: <u></u>	Date: <u>1</u> / <u>12</u> / <u>2023</u>
<b>Director Sector Digital Channels</b>	
Name: <b>MICHAEL DREYER</b> – Te Whatu Ora <b>DIRECTOR SECTOR DIGITAL CHANNELS</b> Signature: <u></u>	Date: <u>1</u> / <u>12</u> / <u>2023</u>

## Appendix 1: Risk and Mitigation Table

- This risk and mitigation table aims to help you identify, describe, and mitigate actual and potential privacy risks involved in your project.
- For “**privacy risk description**”, please identify each vulnerability associated to the Privacy Principle you are assessing. There may be more than one actual or potential risk for each Privacy Principle/ Rule.

Risk Reference Number	Privacy Principle or Rule	Privacy Risk Description	Existing Controls (preventative or detective)	Assessment of current residual risk	Recommended mitigations or privacy enhancements	Revised risk rating	Risk and mitigation owner	Date of implementation
	<i>Which Privacy Principle (under the Privacy Act 2020) or Rule (under the Health Information Privacy Code 2020) you are assessing the risks for</i>	<i>Please provide a description of the potential and actual privacy risk identified</i>	<i>Document the existing systems and safeguards in place that act to minimise the privacy risk identified</i>	<i>Assess the risk with the existing safeguards and systems in place</i>	<i>Specify recommendations for how the residual risks can be removed, managed to ensure the individual is protected</i>	<i>Assess the risk when the new safeguards to be implemented</i>	<i>Please specify who is responsible for implementing the privacy mitigations or enhancements</i>	<i>Please specify the date by which the privacy mitigations or enhancements are to be implemented</i>
R.01	IPP1, IPP3 & IPP4	<p><b>The change from ‘opt off’ to ‘suppression’ of information may become a barrier to the offer of vaccination services being accepted by consumers.</b></p> <p><b>Risk:</b> There is a risk that consumers will choose not to be vaccinated because of the collection of their information in the AIR. This risk will need to be weighed against the alternative risk of over vaccinating a consumer or not having a clear understanding of population immunity and coverage.</p> <p><b>Cause:</b> An insufficient understanding of the purposes of AIR and what ImmSoT stores and how it collects personal information from other sources.</p> <p><b>Effect:</b> Individuals may feel a loss of control over and be distressed about the mandatory collection of their health information.</p>	<p><b>Privacy Statement</b> The AIR Privacy Statement will provide information to individuals about what personal information will be collected, how it will be managed and when it may be used or disclosed to other parties. It will also provide individuals with details of who they can contact for any privacy queries or complaints.</p> <p><b>AIR Communication Pack</b> A full communications package has been prepared by the AIR programme which will be provided to vaccinators and administrators working in the AIR, so that they can have informed conversations with Consumers who require additional information. This package includes additional resources for Consumers, resources for HealthCare Providers and Administrators, links to AIR Website Content, and a Privacy Response Letter Template to ensure consistent messaging from the AIR programme.</p>	<p><b>Probability: Possible</b> <b>Consequence: Major</b> <b>Risk rating: High</b></p>	<p>Due to the design of AIR requiring the collection of vaccination information, if an individual does not wish to provide their information, they will choose not to receive a vaccination.</p> <p>The programme is very aware of this risk and is taking all possible steps to ensure that individuals are informed and understand the purposes behind AIR and the reasons for this collection. Collateral is being developed and updated to reflect the move to ‘suppression’ of information in the AIR.</p> <p>Additional resources and informed conversations with vaccinators and other health service professionals will play a large role in educating individuals and lowering the risk threshold.</p> <p>Ongoing engagement with the Office of the Privacy Commissioner is also recommended to check in with complaints and queries that have been made by the public in relation to the compulsory collection of their information in the AIR.</p>	<p><b>Probability: Possible</b> <b>Consequence: Major</b> <b>Risk rating: Medium</b></p>	Alana Ewe-Snow – Director Prevention	

R.02	IPP8	<p><b>Providers may elect to still vaccinate individuals who do not wish to be recorded on AIR.</b></p> <p><b>Risk:</b> Providers vaccinate consumers without recording the details of the vaccination event within the AIR.</p> <p><b>Cause:</b> Vaccinators do not agree with the design of AIR and the mandatory collection of consumer health information to provide a vaccination service.</p> <p><b>Effect:</b> The purposes of the AIR programme are not met. There is a risk of over vaccinating the consumer next time they present for a vaccination service and reduces the sectors understanding of population immunity and coverage.</p>	<p><b>Contractual Agreements</b> Contractual Agreements between Te Whatu Ora and third parties to provide Users with access to AIR will set out the requirements of the third parties and their Users when accessing AIR, including the requirement to read and accept the AIR Authorised User Agreement and Onboarding Disclaimers and Terms of Use. In signing the Contractual Agreement, the third party will be accepting and acknowledging their obligations under the Privacy Act 2020 and Health Information Privacy Code. The Regional Area Managers will be responsible for managing and monitoring the contractual performance of the third parties.</p> <p><b>Privacy Statement</b> The AIR Privacy Statement will provide information to individuals about what personal information will be collected, how it will be managed and when it may be used or disclosed to other parties. It will also provide individuals with details of who they can contact for any privacy queries or complaints.</p> <p><b>AIR Communication Pack</b> A full communications package has been prepared by the AIR programme which will be provided to vaccinators and administrators working in the AIR, so that they can have informed conversations with Consumers who require additional information. This package includes additional resources for Consumers, resources for HealthCare Providers and Administrators, links to AIR Website Content, and a Privacy Response Letter Template to ensure consistent messaging from the AIR programme.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>Relying on contractual agreements alone is unlikely to provide sufficient compliance. The programme will therefore need to have additional mechanisms in place to encourage compliance with compulsory collection.</p> <p>The future operational reporting function within AIR will ensure that providers are only being paid for the vaccinations which have been recorded in AIR. If providers choose to vaccinate an individual and not record this in AIR, then they will not receive public funding.</p>	<p>Probability: <b>Unlikely</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p>Alana Ewe-Snow – Director Prevention</p>	
------	------	---	--	---	--	--	---	--



<p>R.03</p>	<p>Non-compliance with the Health Information Governance Guidelines</p>	<p><b>Consumer information is unable to be accessed in an emergency situation.</b></p> <p><b>Risk:</b> Healthcare professionals are unable to access information necessary to provide care to an individual.</p> <p><b>Cause:</b> Current suppression functionality means that individuals' information is suppressed for everyone, and a distinction cannot be made between an everyday situation and an emergency situation.</p> <p><b>Effect:</b> The individual does not receive the healthcare they need in a given emergency situation. Additionally, there is a risk of over vaccinating the consumer.</p>	<p><b>Privacy Statement</b> The AIR Privacy Statement will provide information to individuals about what personal information will be collected, how it will be managed and when it may be used or disclosed to other parties. It will also provide individuals with details of what suppression of their records practically means for them – such as the inability for an emergency department to access their immunisation history in situations where they are incapacitated.</p> <p><b>AIR Communication Pack</b> A full communications package has been prepared by the AIR programme which will be provided to vaccinators and administrators working in the AIR, so that they can have informed conversations with Consumers who require additional information about the recording of information in AIR and the suppression process. This package includes additional resources for Consumers, resources for HealthCare Providers and Administrators, links to AIR Website Content, and a Privacy Response Letter Template to ensure consistent messaging from the AIR programme.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Major</b> Risk rating: <b>High</b></p>	<p>The AIR Programme should implement a 'break the glass' mechanism to allow for additional access to records within AIR for an emergency – such as where a Consumer presents to an emergency department in an incapacitated state.</p>	<p>Probability: <b>Unlikely</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p>Alana Ewe-Snow – Director Prevention</p>	
-------------	---	---	---	--	---	--	---	--

R.04	IPP 1, 5, 10 & 11	<p><b>Inappropriate employee browsing of records via ISD/ISM, PMS and PowerBI.</b></p> <p><b>Risk:</b> Users with access to the AIR via the front-end interfaces may use this access to view personal information at a level they have no justifiable purpose to view.</p> <p><b>Cause:</b> Improper access is granted to individuals or login details are shared with individuals who are not authorised or do not have an approved purpose to access the information.</p> <p>Users do not comply with the Authorised User Agreement or Declaration they have agreed to prior to gaining access to the system.</p> <p><b>Effect:</b> Breach of IPPs 1, 5, 10 &amp; 11. Loss of public trust in the AIR Programme and consumers no longer want their personal information recorded in AIR.</p>	<p><b>Training and Education and Awareness</b> Te Whatu Ora staff and healthcare sector workers are required to complete mandatory privacy training on the appropriate management of sensitive health information. All users who are accessing AIR will receive guidance on gathering consumer consent, including the obligation to effectively communicated to consumers about what information needs to be collected about them and why.</p> <p><b>Authorised User Agreements or Terms of Use/Disclaimer</b> Users will be required to read and accept the Authorised User Agreement and/or Privacy Disclaimer prior to accessing the AIR via their approved user interface. These artefacts will set out the users' obligations under the AIR programme to meet the requirements of the Privacy Act 2020 and Health Information Privacy Code 2020.</p> <p><b>Privacy Statement</b> The AIR Privacy Statement will provide information to individuals about what personal information will be collected, how it will be managed and when it may be used or disclosed to other parties. It will also provide individuals with details of who they can contact for any privacy queries or complaints.</p> <p><b>Privacy Breach Management Process</b> There is a formal procedure for Breach Management that is known to all HNZ staff and third-party Users who are accessing the AIR. This process is communicated to Users prior to accessing the AIR via staff training and onboarding documentation including the AIR Privacy Statement and Authorised User Agreements.</p> <p><b>Monitoring and Auditing Process</b> Checks are carried out to ensure that personal information is being accessed appropriately. The effectiveness of the relationship between Te Whatu Ora Air Programme and users accessing the AIR will be monitored on an ongoing basis. The Regional Area Managers and Immunisation Service Delivery Helpdesk will play a large role in this monitoring as part of their usual work duties.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>The project is unable to reduce the risk of employee browsing further in any meaningful way. The health sector historically has a known issue with employee browsing, and this risk has largely been accepted by Te Whatu Ora as a consequence of making health care records accessible and efficient for health care service providers.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>Alana Ewe-Snow – Director Prevention</p>	
------	-------------------	--	--	---	---	---	---	--

			<p><b>Access Management</b> Only authorised users will be provided with access to AIR systems that hold personal information. This access will be approved on a case-by-case basis by the Regional Area Managers and AIR Administrators. These roles will be responsible for ensuring that access is appropriate to the user’s function under the AIR programme.</p>				
R.05	IPP 5, 8, 9, 10 & 11	<p><b>Lack of communication between different Te Whatu Ora Programmes who touch the AIR.</b></p> <p><b>Risk:</b> Te Whatu Ora system integrations with the AIR in relation to sharing, collecting, and storing personal information are changed and no longer meet the requirements outlined in the AIR Privacy Risk Assessment.</p> <p><b>Cause:</b> Changes made to the AIR programme are not communicated to other impacted programmes of work or vice versa.</p> <p><b>Effect:</b> Information is not available when it needs to be or is available in the incorrect system, leading to a breach of the Privacy Act.</p>	<p><b>Standard Operating Processes and Business Rules</b> Business requirements provide Te Whatu Ora staff members who are involved with AIR programme with information and guidance on how to manage design and programme changes.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p><b>Engagement with Te Whatu Ora Privacy Team</b> The project needs to maintain a relationship with the Te Whatu Ora Privacy Team. If possible, there will be a dedicated contact person within the privacy team who will be responsible for engaging with the AIR programme on a consistent basis. This will ensure the privacy team have oversight over any new changes happening with AIR that could impact on the risks outlined in the Privacy Risk Agreement.</p> <p><b>AIR Programme Steering Group</b> Ideally there will also be a group dedicated to overseeing the AIR programme and engaging with other business units who are responsible for the systems which are integrated with AIR. This will ensure that any updates to the AIR or integrated systems are communicated to the affected programme early on and issues can be identified and mitigated as appropriate.</p>	<p>Probability: <b>Unlikely</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	Alana Ewe-Snow – Director Prevention

R.06	All IPPs	<p><b>Third parties do not have the required level of privacy maturity to access or record data in the AIR via their nominated front-end user interface (PowerBI, ISD/ISM portal or PMS).</b></p> <p><b>Risk:</b> Te Whatu Ora grants a third-party access to the data within AIR with a lack of transparency over the third party's privacy practices and compliance with the Privacy Act 2020 resulting in a breach of one or more of the Information Privacy Principles.</p> <p><b>Cause:</b> Ineffective onboarding process for third parties accessing the AIR data or third parties do not fully understand or appreciate their obligations when accessing or recording sensitive and personal information via the ISD/ISM portals, PMS or PowerBI.</p> <p><b>Effect:</b> Breach of all IPP's.</p> <ul style="list-style-type: none"> <li>• Privacy Breach – information within AIR is accidentally or maliciously disclosed outside the purpose of why access was provided.</li> <li>• Reputational risk/media scrutiny on Te Whatu Ora where it can be identified the AIR Programme did not carry out reasonable due diligence before granting a third-party access to the data within ImmSoT.</li> <li>• Loss of public trust in the AIR Programme and consumers no longer want their personal information recorded.</li> </ul>	<p><b>Contractual Agreements</b> Contractual Agreements between Te Whatu Ora and third parties to provide Users with access to AIR will set out the requirements of the third parties and their Users when accessing AIR, including the requirement to read and accept the AIR Authorised User Agreement and Onboarding Disclaimers and Terms of Use. In signing the Contractual Agreement, the third party will be accepting and acknowledging their obligations under the Privacy Act 2020 and Health Information Privacy Code. The Regional Area Managers will be responsible for managing and monitoring the contractual performance of the third parties.</p> <p><b>Training and Education and Awareness</b> Te Whatu Ora staff and healthcare sector workers are required to complete mandatory privacy training on the appropriate management of sensitive health information. All users who are accessing AIR will receive guidance on gathering consumer consent, including the obligation to effectively communicated to consumers about what information needs to be collected about them and why.</p> <p><b>Authorised User Agreements or Terms of Use/Disclaimer</b> Users will be required to read and accept the Authorised User Agreement and/or Privacy Disclaimer prior to accessing the AIR via their approved user interface. These artefacts will set out the users' obligations under the AIR programme to meet the requirements of the Privacy Act 2020 and Health Information Privacy Code 2020.</p> <p><b>Privacy Statement</b> The AIR Privacy Statement will provide information to individuals about what personal information will be collected, how it will be managed and when it may be used or disclosed to other parties. It will also provide individuals with details of who they can contact for any privacy queries or complaints.</p> <p><b>Privacy Breach Management Process</b> There is a formal procedure for Breach Management that is known to all HNZ staff and third-party Users who are accessing the AIR. This process is</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>The project has taken all reasonable steps to ensure that third parties who are accessing the AIR are aware of their obligations under the Privacy Act 2020 and Health Information Privacy Code 2020. Without the AIR programme having constant oversight over these third parties and their use of the AIR data, it is not reasonable to expect the AIR programme to foresee and mitigate all privacy breaches.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>Alana Ewe-Snow – Director Prevention</p>	
------	----------	--	--	---	---	---	---	--

			<p>communicated to Users prior to accessing the AIR via staff training and onboarding documentation including the AIR Privacy Statement and Authorised User Agreements.</p> <p><b>Monitoring and Auditing Process</b> Checks are carried out to ensure that personal information is being accessed appropriately. The effectiveness of the relationship between Te Whatu Ora Air Programme and users accessing the AIR will be monitored on an ongoing basis. The Regional Area Managers and Immunisation Service Delivery Helpdesk will play a large role in this monitoring as part of their usual work duties.</p>				
R.07	IPP 1	<p><b>Unnecessary personal information may be collected and stored within the AIR because of inadequate systems, processes, or form design.</b></p> <p><b>Risk:</b> Unnecessary personal information may be collected and stored in AIR due to the design of the user interfaces and integration functionalities.</p> <p><b>Cause:</b> Systems and forms collect personal information that isn't required to meet the purposes of the AIR Programme and/or systems and forms overuse mandatory information fields and free text fields.</p> <p><b>Effect:</b> Collecting unnecessary personal information may result in a breach of the Privacy Act IPP1. There is a risk to Te Whatu Ora's reputation and organisation accountability if the AIR Programme collects and holds data that it does not have a purpose to collect.</p>	<p><b>Standard Operating Procedures/Business Roles</b> Business requirements provide Te Whatu Ora staff members who are involved with AIR programme with information and guidance on how to manage design and system changes to maintain privacy compliance.</p> <p><b>Monitoring and Auditing Process</b> Checks are carried out to ensure that personal information is being accessed appropriately. The effectiveness of the relationship between Te Whatu Ora Air Programme and users accessing the AIR will be monitored on an ongoing basis. The Regional Area Managers and Immunisation Service Delivery Helpdesk will play a large role in this monitoring as part of their usual work duties.</p> <p><b>Training and Education and Awareness</b> Te Whatu Ora staff and healthcare sector workers are required to complete mandatory privacy training on the appropriate management of sensitive health information. All users who are accessing AIR will receive guidance on gathering consumer consent, including the obligation to effectively communicated to consumers about what information needs to be collected about them and why.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p><b>Engagement with Te Whatu Ora Privacy Team</b> The project needs to maintain a relationship with the Te Whatu Ora Privacy Team. If possible, there will be a dedicated contact person within the privacy team who will be responsible for engaging with the AIR programme on a consistent basis. This will ensure the privacy team have oversight over any new changes happening with AIR that could impact on the risks outlined in the Privacy Risk Agreement.</p> <p><b>AIR Programme Steering Group</b> Ideally there will also be a group dedicated to overseeing the AIR programme and ensuring that any updates the AIR system design or the design of systems integrated with AIR do not create any additional privacy risk around the collection and storage of personal information.</p>	<p>Probability: <b>Unlikely</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p>Michael Dreyer – Director Sector Digital Channels</p>

R.08	IPP 5	<p><b>Third Parties are provided with more information than is necessary to achieve their functional purpose.</b></p> <p><b>Risk:</b> Third parties are provided with more personal information than is needed to perform their specific administrative or reporting function under the AIR Programme.</p> <p><b>Cause:</b> Inadequate role-based access controls are implemented meaning user views are not restricted to the minimum amount of information necessary.</p> <p>AIR administrators accessing the information via the ISM portal now have a national level view of vaccinations administered. Previously they were only given a regional view.</p> <p><b>Effect:</b> There is a risk to Te Whatu Ora's reputation and organisation accountability if the AIR Programme shares data with third parties that do not have a purpose to use it.</p>	<p><b>Standard Operating Procedures/Business Roles</b> Business requirements provide Te Whatu Ora staff members who are involved with AIR programme with information and guidance on how to manage the disclosure of AIR information to third parties.</p> <p><b>Monitoring and Auditing Process</b> Checks are carried out to ensure that personal information is being accessed appropriately. The effectiveness of the relationship between Te Whatu Ora Air Programme and users accessing the AIR will be monitored on an ongoing basis. The Regional Area Managers and Immunisation Service Delivery Helpdesk will play a large role in this monitoring as part of their usual work duties.</p> <p><b>Training and Education and Awareness</b> Te Whatu Ora staff and healthcare sector workers are required to complete mandatory privacy training on the appropriate management of sensitive health information. All users who are accessing AIR will receive guidance on gathering consumer consent, including the obligation to effectively communicated to consumers about what information needs to be collected about them and why.</p> <p><b>Data Governance</b> Prior to the disclosure of information to any third party, approval will need to be authorised by the Te Whatu Ora Data Governance group responsible for overseeing the sharing of information held by Te Whatu Ora (including AIR). Data Sharing Agreements will be entered into between Te Whatu Ora and a third party which set out whether the information is shared at the individual or aggregate level as appropriate to meet the third party's function. Approval to disclose information will not be granted where the third-party's function does not meet the purposes of AIR and is not authorised under the Privacy Act 2020, the Health Act 1956, and Health Information Privacy Code</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>Te Whatu Ora Data Governance procedures will play a key role in protecting the disclosure of an individual's personal information to a third party. The Data Governance Group will be responsible for ensuring that disclosure is only permitted in circumstances which meet the purposes of the AIR programme as communicated to individuals via the AIR privacy statement and communication channels. It is recommended that the group develop a term of reference specific to the AIR programme which also have a register in place which records all Data Sharing Agreements providing access to AIR so that this is easily accessible and identifiable. clearly documents the process for approving third party access.</p>	<p>Probability: <b>Unlikely</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p>Michael Dreyer – Director Sector Digital Channels</p>	
------	-------	---	---	---	---	--	--	--

R.09	IPPs 3 & 4	<p><b>Informed consent is not obtained from individuals prior to collecting and sharing their personal information.</b></p> <p><b>Risk:</b> Individuals are not fully aware of what information is collected by the AIR Programme and how it will be managed, used, and disclosed to third parties. This is particularly an issue when the individual is under 16 years of age or is unable to provide informed consent.</p> <p><b>Cause:</b> Individuals have an insufficient understanding of their information being collected and how it will be managed and used.</p> <p><b>Effect:</b> Breach of IPPs 3 &amp; 4 and public trust and confidence in the AIR Programme and Te Whatu Ora is undermined.</p>	<p><b>Privacy Statement</b> The AIR Privacy Statement will provide information to individuals about what personal information will be collected, how it will be managed and when it may be used or disclosed to other parties. It will also provide individuals with details of who they can contact for any privacy queries or complaints.</p> <p><b>Authorised User Agreements or Terms of Use/Disclaimer</b> Users will be required to read and accept the Authorised User Agreement and/or Privacy Disclaimer prior to accessing the AIR via their approved user interface. These artefacts will set out the users' obligations under the AIR programme to meet the requirements of the Privacy Act 2020 and Health Information Privacy Code 2020.</p> <p><b>Training and Education and Awareness</b> Te Whatu Ora staff and healthcare sector workers are required to complete mandatory privacy training on the appropriate management of sensitive health information. All users who are accessing AIR will receive guidance on gathering consumer consent, including the obligation to effectively communicated to consumers about what information needs to be collected about them and why,</p> <p><b>Business Processes and Rules</b> Business requirements provide Te Whatu Ora staff members who are involved with AIR programme with information and guidance on how to manage the collection of personal information from individuals.</p> <p><b>AIR Communication Pack</b> A full communications package has been prepared by the AIR programme which will be provided to vaccinators and administrators working in the AIR, so that they can have informed conversations with Consumers who require additional information. This package includes additional resources for Consumers, resources for HealthCare Providers and Administrators, links to AIR Website Content, and a Privacy Response Letter Template to ensure consistent messaging from the AIR programme.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>The project has taken all reasonable steps to ensure that vaccinators, administrators, and health care service providers are fully aware of their obligations to obtain informed consent from individuals prior to collecting their personal information in the AIR. Information about the AIR will be widely and publicly available for consumers.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>Alana Ewe-Snow – Director Prevention</p>	
------	------------	--	---	---	--	---	---	--

R.10	IPP 9	<p><b>Information is retained by the AIR programme or third parties for longer than is needed resulting in a breach of the Privacy Act.</b></p> <p><b>Risk:</b> Misuse of personal information is more likely if information is retained for longer than its required purpose, resulting in inaccurate and out of date information being used.</p> <p><b>Cause:</b> Te Whatu Ora have no control over how long downloaded reports are retained by third parties.</p> <p><b>Effect:</b> Breach of IPP9 which requires organisations to delete personal information once it is no longer needed. Reputational risk/media scrutiny on Te Whatu Ora for their management of the AIR Programme and the granting of access to third parties.</p>	<p><b>Privacy Breach Management Process</b> There is a formal procedure for Breach Management that is known to all HNZ staff and third-party Users who are accessing the AIR. This process is communicated to Users prior to accessing the AIR via staff training and onboarding documentation including the AIR Privacy Statement and Authorised User Agreements.</p> <p><b>Training and Education and Awareness</b> Te Whatu Ora staff and healthcare sector workers are required to complete mandatory privacy training on the appropriate management of sensitive health information. All users who are accessing AIR will receive guidance on retaining health information.</p> <p><b>Authorised User Agreements or Terms of Use/Disclaimer</b> Users will be required to read and accept the Authorised User Agreement and/or Privacy Disclaimer prior to accessing the AIR via their approved user interface. These artefacts will set out the users' obligations under the AIR programme to meet the requirements of the Privacy Act 2020 and Health Information Privacy Code 2020.</p> <p><b>Business Processes and Rules</b> Business requirements provide Te Whatu Ora staff members who are involved with AIR programme with information and guidance on how to manage the retention of personal information within the AIR.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p>The project has taken all reasonable steps to ensure that the AIR programme and users who are accessing data under the AIR are aware of their obligations under the Privacy Act 2020 and Health (Retention of Health Information) Regulations. Without the AIR programme having constant oversight over these third parties and their storage of the AIR data, it is not reasonable to expect the AIR programme to foresee and mitigate all privacy breaches.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p>Alana Ewe-Snow – Director Prevention</p>	
------	-------	--	--	--	--	--	---	--



R.11	All IPPs	<p><b>Third parties cause a privacy breach which is not effectively managed to reduce harm to the individuals affected.</b></p> <p><b>Risk:</b> A privacy breach is not identified, or where it is identified, it is not managed effectively potentially causing more harm than the breach itself and resulting in further breaches of a similar nature.</p> <p><b>Cause:</b> Lack of or inadequate training on an AIR Programme privacy breach management plan.</p> <p><b>Effect:</b> Loss of trust and confidence in the AIR Programme and Te Whatu Ora. Reputational harm to Te Whatu Ora and public and media scrutiny.</p>	<p><b>Privacy Breach Management Process</b> There is a formal procedure for Breach Management that is known to all HNZ staff and third-party Users who are accessing the AIR. This process is communicated to Users prior to accessing the AIR via staff training and onboarding documentation including the AIR Privacy Statement and Authorised User Agreements.</p> <p><b>Contractual Agreements</b> Contractual Agreements between Te Whatu Ora and third parties to provide Users with access to AIR will set out the requirements of the third parties and their Users when accessing AIR, including the requirement to read and accept the AIR Authorised User Agreement and Onboarding Disclaimers and Terms of Use. In signing the Contractual Agreement, the third party will be accepting and acknowledging their obligations under the Privacy Act 2020 and Health Information Privacy Code. The Regional Area Managers will be responsible for managing and monitoring the contractual performance of the third parties. Education and Awareness Programme.</p> <p><b>Authorised User Agreements or Terms of Use/Disclaimer</b> Users will be required to read and accept the Authorised User Agreement and/or Privacy Disclaimer prior to accessing the AIR via their approved user interface. These artefacts will set out the users' obligations under the AIR programme to meet the requirements of the Privacy Act 2020 and Health Information Privacy Code 2020.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p>The project has taken all reasonable steps to ensure that third parties who are accessing the AIR are aware of their obligations under the Privacy Act 2020 and Health Information Privacy Code 2020. Without the AIR programme having constant oversight over these third parties and their use of the AIR data, it is not reasonable to expect the AIR programme to foresee and mitigate all privacy breaches.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	Alana Ewe-Snow – Director Prevention	
------	----------	---	---	---	---	---	---	--

R.12	IPPs 10 & 11	<p><b>Inadequate Data Governance by Te Whatu Ora</b></p> <p><b>Risk:</b> Decisions about information sharing with third parties and use and management of information are not carefully considered or follow a clear process that implements Te Whatu Ora’s obligations under the Health Act and Privacy Act.</p> <p><b>Cause:</b> There is no Data Governance Steering group established which is accountable for approving Data Sharing Agreements between Te Whatu Ora and third parties. Or there is a Data Governance Group in place, but they do not have appropriate or effective processes for managing data sharing arrangements under AIR.</p> <p><b>Effect:</b> Breach of IPPs 10 &amp; 11 – use and disclosure of personal information. Reputational risk/media scrutiny on Te Whatu Ora for their management of the AIR Programme and the granting of access to third parties.</p>	<p><b>Business Processes and Rules</b> Business requirements provide Te Whatu Ora staff members who are involved with AIR programme with information and guidance on how to manage requests from third parties for access to AIR data.</p> <p><b>Contractual Agreements</b> Contractual Agreements between Te Whatu Ora and third parties to provide Users with access to AIR will set out the requirements of the third parties and their Users when accessing AIR, including the requirement to read and accept the AIR Authorised User Agreement and Onboarding Disclaimers and Terms of Use. In signing the Contractual Agreement, the third party will be accepting and acknowledging their obligations under the Privacy Act 2020 and Health Information Privacy Code. The Regional Area Managers will be responsible for managing and monitoring the contractual performance of the third parties.</p> <p><b>Data Governance</b> Prior to the disclosure of information to any third party, approval will need to be authorised by the Te Whatu Ora Data Governance group responsible for overseeing the sharing of information held by Te Whatu Ora (including AIR). Data Sharing Agreements will be entered into between Te Whatu Ora and a third party which set out whether the information is shared at the individual or aggregate level as appropriate to meet the third party’s function. Approval to disclose information will not be granted where the third-party’s function does not meet the purposes of AIR and is not authorised under the Privacy Act 2020, the Health Act 1956, and Health Information Privacy Code.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Moderate</b> Risk rating: <b>Medium</b></p>	<p><b>Engagement with Te Whatu Ora Privacy Team</b> The project needs to maintain a relationship with the Te Whatu Ora Privacy Team. If possible, there will be a dedicated contact person within the privacy team who will be responsible for engaging with the AIR programme on a consistent basis. This will ensure the privacy team have oversight over any new changes happening with AIR that could impact on the risks outlined in the Privacy Risk Agreement.</p> <p><b>AIR Programme Steering Group and Term of Reference</b> Ideally there will also be a group dedicated to overseeing the AIR programme and engaging with other business units who are responsible for the systems which are integrated with AIR. This will ensure that any updates to the AIR or integrated systems are communicated to the affected programme early on and issues can be identified and mitigated as appropriate.</p> <p>It is recommended that the group also develop a term of reference specific to the AIR programme which also have a register in place which records all Data Sharing Agreements providing access to AIR so that this is easily accessible and identifiable. clearly documents the process for approving third party access.</p>	<p>Probability: <b>Unlikely</b> Consequence: <b>Moderate</b> Risk rating: <b>Low</b></p>	<p>Alana Ewe-Snow – Director Prevention</p>	
------	--------------	---	--	---	--	--	---	--

R.13		<p><b>Relationship breakdown with OPC due to removal of consumer choice</b></p> <p><b>Risk:</b> There is a risk that if the AIR programme goes live without a consumer choice option, the OPC will investigate the programme and publicly question the validity of AIR.</p> <p><b>Cause:</b> Removal of the 'opt off' option without a viable alternative process.</p> <p><b>Effect:</b> Te Whatu Ora's reputation is publicly brought in the question by the Regulator and there is a loss of trust and confidence in our ability to protect information while delivering health services, leading to fewer people seeking care when they need it.</p>	<p><b>Implementation of the suppression option</b> Te Whatu Ora has developed a 'suppression' process that enables individuals to request that their information is suppressed in the AIR. This process is still being worked through, but a basic version is outlined in the <b>AIR Communications Pack</b> and in the <b>Privacy Statement</b>, which will be available on Te Whatu Ora's website.</p> <p><b>Ongoing engagement with OPC</b> A summary paper is being developed that outlines how we have dealt with their feedback and implemented a suppression option to replace the 'opt off' process. The Te Whatu Ora Privacy Team is managing the relationship with the OPC.</p>	<p>Probability: <b>Possible</b> Consequence: <b>Major</b> Risk rating: <b>High</b></p>	<p><b>Implementation of the suppression option</b> Once the suppression process design has been completed it will be implemented.</p> <p><b>Ongoing engagement with OPC</b> A summary paper is being developed that outlines how we have dealt with their feedback and implemented a suppression option to replace the 'opt off' process. The Te Whatu Ora Privacy Team is managing the relationship with the OPC.</p>	<p>Probability: <b>Unlikely</b> Consequence: <b>Major</b> Risk rating: <b>Medium</b></p>	Alana Ewe-Snow – Director Prevention	
------	--	---	---	--	--	--	---	--

## Appendix 2: Glossary

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

Term	Definition, description, relationship, and business rules
<b>AIR</b>	Aotearoa Immunisation Register
<b>Administrators</b>	AIR Users who access the ISM
<b>ATO</b>	Authority to Operate – Prepared by Information Security
<b>AWS</b>	Amazon Web Services
<b>Broker Service</b>	The co-existence broker service developed to allow PMS systems to talk to the ISD before PMS vendors are ready to uptake the APIs
<b>CIR</b>	COVID-19 Immunisation Register
<b>Consumer</b>	A person who has or will receive a vaccination service
<b>CPN</b>	Consumer Practitioner Number
<b>Cutover</b>	The first big release of all components of the Aotearoa Immunisation Register scheduled for 25 November 2023
<b>Health UI</b>	A Web Based User interface for the NHI, used in a swivel chair fashion
<b>HNZ</b>	Te Whatu Ora – Health New Zealand
<b>HPI</b>	Health Practitioner Index
<b>ImmSoT</b>	Immunisation Source of Truth – the data repository for AIR where immunisation event information is stored
<b>ISD</b>	Immunisation Service Delivery – the portal accessed by Vaccinators
<b>ISM</b>	Immunisation Service Management – the portal accessed by Administrators
<b>MHA</b>	My Health Account – a Ministry of Health service that connects you to your health information and online health services
<b>NES</b>	National Enrolment System to a General Practitioner
<b>NHI</b>	National Health Index – this is the unique identifier that is assigned to every person who uses health and disability support services in New Zealand
<b>NIR</b>	National Immunisation Register
<b>Orchestration Service</b>	The service layer which enriches ImmSoT data with information from the HPI, NHI and NES
<b>PHO</b>	Primary Health Organisation
<b>PMS</b>	Patient Management System – used by General Practitioners to record and view Consumer information
<b>PowerBI</b>	The reporting tool used to generate AIR operational reports
<b>Provider</b>	The term related to an entity providing vaccination services
<b>Third Parties</b>	Parties external to Te Whatu Ora – such as PHO's and community groups
<b>Users</b>	All Users who have been onboarded to the AIR user interfaces – ISD, ISM and PowerBI
<b>Vaccinators</b>	Users who access the AIR via the ISD portal
<b>Vaccination Record</b>	Refers to the actual vaccination record, which is realised as either an entry from ISD, ImmuniseNow or GP. A vaccination event is the act of giving a vaccination