Health New Zealand
Te Whatu Ora

Health New Zealand | Te Whatu Ora

My Health Account (Unified)

Privacy Impact Assessment

Date 12/06/2025

Information for the Project

Health NZ | Te Whatu Ora is the kaitiaki and steward of a significant amount of Personal Information, including highly sensitive Health Information. We **all** have a responsibility to handle it appropriately and with care.

The best time to start privacy work (and this Privacy Impact Assessment) is **at the beginning** of your Project**.** By being proactive you can implement a privacy-by-design approach, prioritising privacy of Personal Information and ensuring you're upholding our obligations under the Privacy Act 2020 and Health Information Privacy Code 2020.

HNZ Privacy is here to support you in preparing this Privacy Impact Assessment. The complexity and scale of this Privacy Impact Assessment will depend on the complexity and scale of the Project. **We strongly recommend** you allow a **minimum** of 4-6 weeks to complete this Privacy Impact Assessment. For the more complex and significant Projects you should allow longer (including time to consult with the Office of the Privacy Commissioner as per their requirements). This Privacy Impact Assessment is not a last minute legal and privacy compliance checklist.

Please check out the "Guide to Completing a Privacy Impact Assessment" for more information.

The Project

Business Unit:	Digital Services
PIA Author:	Samuel Wong
Date PIA prepared:	12 June 2025
Version number:	2.0
Project Go-live Date:	12/06/2025

Summary of Project / Change

Please **describe** the Project. This should include:

- What the purpose of the Project (or change)?
- What are the benefits and expected outcomes?
- Will it provide a solution to an existing problem?

Summary

My Health Account Unified is a feature extension of My Health Account (MHA). MHA continues to be branded as 'My Health Account' as an identity authentication service. From an MHA user perspective, the unified extension provides an additional option that allows providers of health services to add a workforce profile that allows users to log into an approved workforce digital health service.

My Health Account Workforce (MHA-W) remains unchanged. MHA-W has an existing approved Privacy Impact Assessment.

The scope of this document applies to the unified feature extension to My Health Account. Within this document, the term My Health Account will be used to describe My Health Account with the unified feature extension. To ensure appropriate context for the unified feature extension, the document will also refer to My Health Account Workforce as a separate, but related product.

Introduction

1. My Health Account is the digital health identity service originally developed by the Ministry of Health (the Ministry).

    1.1. On 1 July 2022 My Health Account became the responsibility of Te Whatu Ora – Health New Zealand[1].

    1.2. My Health Account services have previously been provided as two separate profiles using the same shared username (email) registration facility:

        1.2.1. My Health Account (MHA) which verifies the identity of health consumers to ensure appropriately access to linked digital health services which hold health consumer's own personal health information e.g. vaccination information.

        1.2.2. My Health Account Workforce (MHAW) which verifies the identity of health professionals to ensure appropriate access to connected professional health care related applications. These applications enable various administrative and healthcare related tasks such as invoicing or form completion such as submitting results of a viral RAT test done in the community. These professionals can come from across the health sector e.g. ACC.

    1.3. My Health Account (Unified) is an updated version of My Health Account that supports users to add a workforce profile to their consumer account. The current MHA release includes the unified enhancement. A PIA covers the prior MHA release. The scope of this PIA includes the prior and current MHA release.

2. The PIA outlines the move to implement a 'unified account' enhancement within My Health Account. This enhancement can support two profiles, allowing users to manage both personal and professional healthcare roles within a single account. This change is expected to streamline user experience and improve efficiency. When referencing "My Health Account" in this PIA, it includes all aspects of My Health Account including the workforce profile feature provided by the Unified enhancement. Health New Zealand aims to enhance user access to health information via digital channels. My Health Account intends to be the trusted digital health identity service that helps individuals have greater access to information about their own health by easily verifying their identity with a trusted level of confidence. This enables access to personal health information such as My Health Record and ongoing access management for the various linked digital services which hold further personal and health information.

Background

3. To allow users to access digital health services that includes personal identifiable information, Health New Zealand first needs to accurately identify users. My Health Account was stood up to enable health consumers and health workers to authenticate and confirm who they are digitally in accordance to

[1] Te Whatu Ora - Health New Zealand is a Crown agent within the meaning of section 10(1) of the Crown Entities Act 2004 and is established under the Pae Ora (Healthy Futures) Act 2021.

Identification Management Standards[2] and the trust framework for digital identity[3] where possible, and to engage with online healthcare services.

3.1. The initial use case for My Health Account was for consumers to view and confirm their identity in order to access their COVID-19 vaccination status and test results through My Covid Record. After the COVID-19 pandemic response, My Health Record was created to supersede My COVID Record to support health consumers to access more of their publicly held- digital records in a modern, safe and secure way.

Integrated Use Case

3.2. Health workers who need to view, access and collect information using digital health services, either in providing services or processing records, must first be authenticated to determine the role-by-employer they play when accessing personally identifiable. This created the need for My Health Account Workforce.

3.3. My Health Account addresses the three scenarios that have been identified for a health worker – when Realme Verified is linked to a single email that other public agency services require them to use; when a person works as an on-demand independent contractor or enrols to be a student at an educational institution; and when generic email accounts are assigned by organisations to their rostered teams, when services are needed to identify individuals for the purposes to access Personally Identifiable Information. Approximately 2500 user's profiles will be enhanced by this development, this represents less than 10% of the overall health workforce.

3.4. The My Health Account service is now integrated with several approved Digital Health Services which hold the records that My Health Account users are able to access after the identity verification provided by My Health Account is completed to an appropriate level (those current at the date of issue of this PIA are listed in Appendix 6 and latest versions updated on the My Health Account website).

4. **Privacy Assessment** Each digital health service must complete a PIA and meet the requirements of My Health Account's identification level framework, listed in Appendix 6 before being permitted credentials to use the My Health Account service. This will not change in the current My Health Account (unified) release.

5. Health New Zealand carefully balances the potential privacy risks against the public health benefits of Consumer and those with roles as health workers access to their health records using My Health Account. Consumer trust is essential to achieve widespread use of the current My Health Account release. Health New Zealand seeks to earn and retain high levels of public trust.

5.1. My Health Account intends to retain user choice, collecting only the essential personal information required to uniquely identify users online, and limit who will have access to that information. Health workers also have the option to provide what is only required for their organisation's authentication needs, balancing both health system and personal needs. The current My Health Account release does not gain, hold or retrieve information from digital health

[2] Identification Standards | NZ Digital government sighted 12.3.25

[3] Trust framework for digital identity | NZ Digital government sighted 12.6.25

services to which it is connected except for that information entirely necessary to access records, verify identity and maintain trust in a user profile.

5.2. Information about consumers and members of the health workforce who choose to use My Health Account is stored by Health New Zealand and will not be shared with any other agencies unless explicit consent is obtained, or it is authorised by law. Use of information by Service Providers will either be authorised or under legal authority (such as in compliance with the rules in the Health Information Privacy Code 2020 and other enactments that require or allow information to be used or disclosed). This may happen:

- if users have authorised this sharing
- if it is necessary for delivering care and treatment
- If there is an incident we need to investigate, or a technology issue
- for your safety or the safety of others, or
- if authorised by law.

5.3. Users are asked for their permission before My Health Account shares their information with connected digital health services. Users can view a list of all digital health services they have previously given permission to access their information. Users can remove these permissions at any time via My Health Account.

6. The Office of the Privacy Commissioner and the Government Chief Privacy Officer were consulted and provided comments on an earlier version of the Privacy Impact Assessment in respect to consumer services in Appendix 4. There have been no substantial changes since this review.

7. This Privacy Impact Assessment (PIA) is a 'living' document that will be reviewed as My Health Account continues to develop. Health New Zealand releases new functionality in My Health Account Services in phases. As new features are developed and released, the privacy impacts will be reviewed and reassessed.

What is the Health NZ **scope** for your Project? *i.e., is the Project for a single District, Region, or the whole of Health NZ?*

My Health Account is a national digital health identity service that enables users of New Zealand health-related services (both health consumers and health workforce members) to create a trusted digital health identity, are authenticated, and can interact with the information they are entitled to access.

Use of My Health Account is voluntary. People must choose to use it and can determine what Identification Level they wish to achieve based on the Digital Health Services they want and consent to access. While the service is voluntary, most services require risk-based assessment to determine the appropriate level of identification and most digital applications will require the highest identification level to be maintained to ensure legal (such as in compliance with the rules in the Health Information Privacy Code 2020 and other enactments that require or allow personal information to be used or disclosed) authorisation like consent for accessing said digital services.

Depending on the type of identity proof that the user provides, My Health Account will set a verified Identification Level as per the Consumer Health identity Standard (HISO 10046:2024) and guided by the Identification Management Standards 2020). Approved Service Providers can use the Identification Level to ensure that private information is only released to users who meet identity requirements set by the

Digital Health Service and relevant to the level of sensitivity and risk in accessing personal and health information held in that Digital Health Service.

My Health Account has developed a process so that people can make choices on an ongoing basis to connect to various and relevant Digital Health Services. Users can also choose when to revoke their access choices for Services. Users who would have previously had a Workforce account are now able to access Digital Health Services using their MHA login (with the unified enhancement). This allows access to relevant health worker Digital Health Services which enable healthcare administration.

Phases

My Health Account (unified) enhancements will be rolled out in three phases. This PIA covers phase one. Phases two and three entail having an account that allows recovery emails to support user-defined contact and login preferences, and the ability to hold multiple emails belong to multiple employers for the same account. The general principle is that you have one digital account representing who you are, and the context of identity attributes and claims that has been verified are used to enable access to your consented and approved digital health services, including auditing when accessing a record.

Will Health NZ be partnering with any individuals or agencies outside of Health NZ on this Project?
If so, who? What is each parties' role in this Project?

Identity Collection and Verification partners

Health New Zealand has contracted the use of **GBG Cloudcheck** services for verifying user identities. GBG Cloudcheck (also formerly known as Verifi Identity Services) is an approved organisation to act as an Intermediary under the Identity Information Confirmation Act 2012. They provide identity confirmation services with direct connection to the Department of Internal Affairs and New Zealand Transport Agency as authoritative source providers of New Zealand Identity Information.

We also have arrangements with the **Kiwi Access card provider** via CentraPass to verify the documents they issue. Kiwi Access Card is developed as the official provider for Identity services managed for hospitality and disability services, and to handle young adults and older people who may not be able to hold a driver licence or travel internationally.

Individuals nominate relationship associations with **employers or membership associations such** as colleges, credential issuing authorities, or international institutions in their workforce profile, which is now linked to My Health Account (previously separated). These assertions are verified with those organisations, with consent of the user. Identity verification is performed by agreement with authorised representatives of those nominated organisations if they have an existing agreement with Health New Zealand. If no agreement is in place or organisation is unreachable such as an international membership organisation, we will provide the details as self-asserted and not verified by source.

External Data Processors

Two telecommunication providers are contracted to provide communication services to end-users generated from user onboarding and account recovery workflows. **SendGrid** is used to send notifications to users by email, which is only the email and content supplied by our system. Text messages are sent through services provided by **One.NZ** gateway involving the user of the mobile number on record. Text messages are used for sending notifications and one-time-password codes for verification.

Note: Due diligence was undertaken, as part of the privacy assessment, and documented within an existing Privacy Impact Assessment (PIA) dated May 2024.

Public Agency partner users

Accident Compensation Corporation (ACC) has been provided a license, under cost-recovery, for the use of My Health Account Workforce to use the shared national digital health identity account to authenticate users into their linked digital health services. These services are provided with the name of the user, their username, account ID and their confidence levels to determine provisioning of access to their respective applications. Some applications may require the optional HPI-CPN.

Note: An assessment of the ACC relationship was also included within the May 2024 PIA.

Other agencies such as tertiary education providers with **Ministry of Education** are also using the same service when administrators placing students for training at healthcare services, and involved in accessing health systems for approved evaluation programmes. Public services have been instructed to leverage established digital identity services, with My Health Account being the most prevalent authentication service in the purposes for training or administrating healthcare services.

Note: Due diligence of the Ministry of Education was undertaken within the Student Placement System Project PIA. The PIA was signed off by the Health NZ Privacy Officer in September 2024.

Please summarise:

- What information will be collected or handled by this Project?
- Where is the information coming from?

The primary data collection is from the account user asserting their own identification details. These details are classified as self-asserted until verified by an Identity confirmation authoritative source, which may be held by:

- Health New Zealand's existing repositories (i.e. National Health Index, Health Provider Index and National Enrolment Service-held information) or by,
- externals sources such as GBG CloudCheck who supplies both Department of Internal Affairs (DIA) and New Zealand Transport Agency (NZTA) confirmation datasets
- Kiwi Access Card and asserted organisational relationship details are held by the respective issuing organisations
- DIA RealMe verified service

These authoritative sources will confirm that the details provided by the individual holding the account match known records, thereby lifting the level of confidence about the authenticity of the identity information asserted for the account.

Information collected is noted in the information flow, but primarily:

- Names
- Date of Birth
- Email
- Mobile number
- Document type/Version
- Document number
- NHI
- Parents-Child names if required to link relationships

And under Workforce profile

- HPI-CPN only for registered providers
- Employer (if required by application)
- Membership associations (if required for application)

Please **advise** if the collection, use or sharing of information in this Project affects Māori interests.

If so- what are those interests? How are they affected? How will you accommodate them?[4]

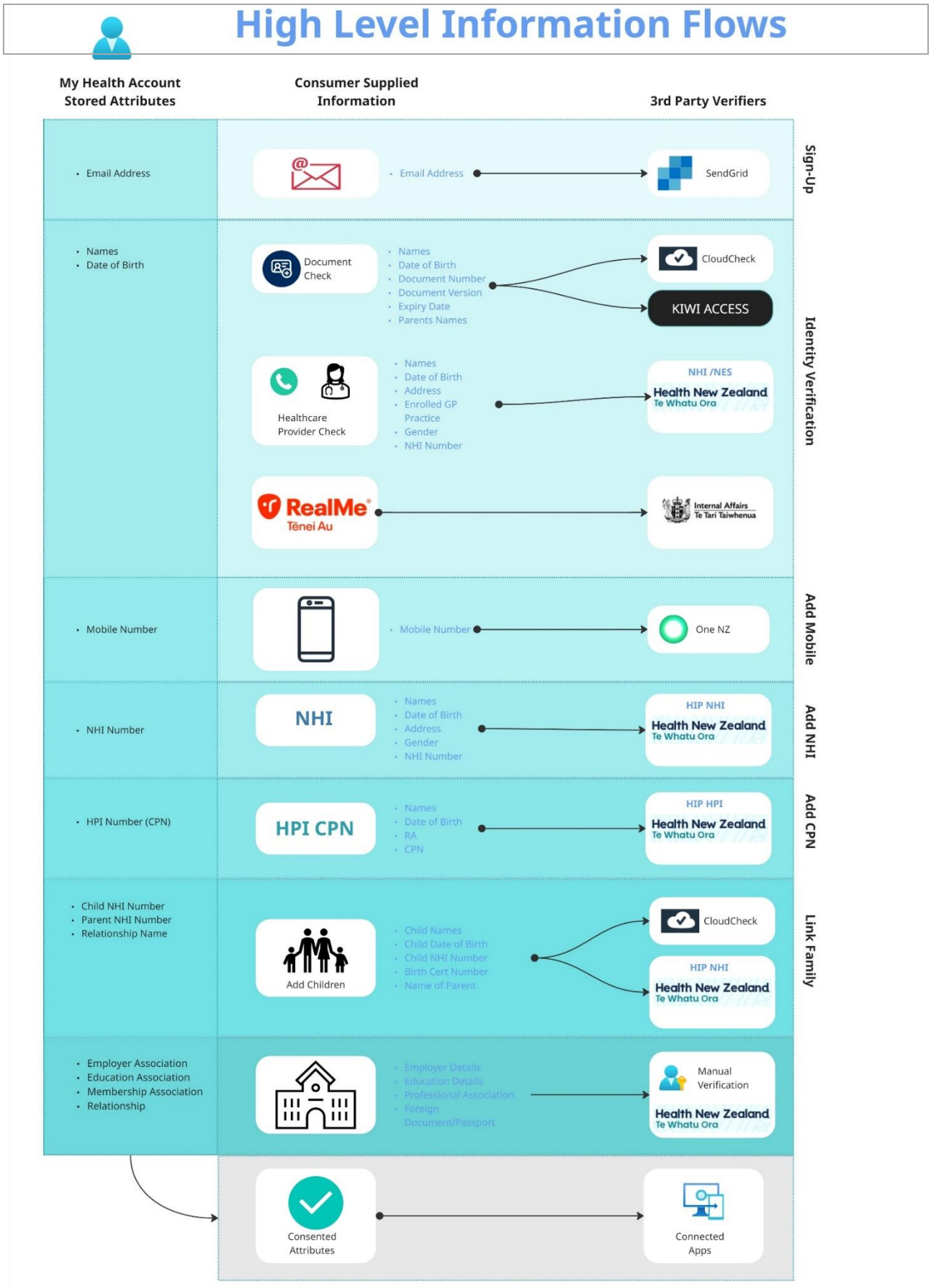
My Health Account is being provided as a population wide solution that may overlap and support Māori interests., for example, by enabling the collection of information via Māori-orientated linked digital health services, such as the national Tātai iwi affiliation collection service, which supports Tino rangatiratanga (self-determination).

A known barrier to Māori in using the My Health Account Unified service is the lack of accessible identity documents used to prove identity, with Māori having lower rates of ownership of driving licences and passports. To address this issue other options like Kiwi Access Card and in-person verified 'uplift by relationship' have been made available.

[4] It is a requirement of our Government Chief Privacy Officer that this is addressed in our Privacy Impact Assessments.

Information Flow Diagram

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



Scope of Assessment

Please define the scope of this PIA
The current assessment covers: The personal, demographic, and anonymous[5] information to be collected from the user to create a My Health Account. The prior release of My Health Account has a PIA. The current My Health Account release includes the unified enhancement. This document will supersede the PIA for the prior release of the MHA. The unified enhancement is an update to My Health Account. The enhancement provides a mechanism to allow individuals who are a health consumer but may also have a role as a provider or supplier of health-related services, to be able to self-assert their digital identity as a health worker. The unified enhancement does not collect or store any personal information in addition to that of MHA. The context within which information is collected does change. The scope of MHA now includes workforce logins which can now be used interchangeably with consumer logins.
Please describe what has been excluded from the scope of this PIA and why
This Assessment does not address: • any further digital health services or applications My Health Account may be able to interact with in future, as each of these will be addressed in subsequent service-specific Privacy Impact Assessment activity and must meet the identification level requirements set by My Health Account. • the decision-making process, approvals, or the conclusions reached about the decision to create My Health Account services. • The standalone My Health Account Workforce PIA.

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

[5] Users can choose their level of engagement with the system. At the lowest Identification Level (Level 1), users can provide pseudonymous information such as phone number, email address and “names” without this information being verified with official sources. Users who choose a lower Identification Level will not be permitted access to sensitive information (e.g. medical records) until they successfully provide further evidence of identity.

Appendix 3	Privacy statement
Appendix 4	Previous Privacy Impact Assessments
Appendix 5	Health New Zealand Identity Confidence Level Standards
Appendix 6	Approved Live Connected Digital Services

Assessment Questions

Does the project involve personal information?	YES	NO
	☒	☐

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

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

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

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

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

Principle 1:
Lawful purpose and necessary collection of personal information

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

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

Please complete the following table:

List all information collected by project	Please state why this information is needed for the purpose of this project

Patient First and Last Name (example)	Identification/verification (example)
Phone Number (example)	Identification/verification and communication (example)
Unique ID	The unique identifier for the My Health Account holder. This must be provided as a system ID for data exchange (main unique identifier used by My Health Account).
Email	The verified email address for the My Health Account holder. This must be provided as the account username
Identification Level	The Identification Level that the My Health Account holder has achieved by completing verification processes. This must be provided if any attributes other than Unique ID and Email are requested.
Mobile number	The verified mobile number as supplied by the My Health Account holder. This must be provided if used under Workforce profile
Given name	The account holder's optional given name, as recorded on the official document they supplied as evidence of identity on sign-up. Collected on accounts at Identification Level 2 and higher
Middle name	The account holder's optional middle name, as recorded on the official document they supplied as evidence of identity on sign-up. Collected on accounts at Identification Level 2 and higher
Family name	The account holder's family name, as recorded on the official document they supplied as evidence of identity on sign-up. Collected on accounts at Identification Level 2 and higher
Nickname / Preferred name	The account holder's preferred name as set on the self-service profile page of My Health Account. This is optional
Date of birth	The date of birth as recorded on the account holder's official document used as evidence of identity. Collected on accounts at Identification Level 2 and higher.
NHI number	The NHI number of the My Health Account holder. Collected on accounts at Identification Level 2 and higher.
HPI number (CPN)	The HPI number (CPN) of the My Health Account holder. Collected on accounts at Identification Level 2 and higher.
Related NHI numbers	The list of NHIs that the My Health Account holder has linked to their own NHI number. Collected on accounts at Identification Level 3N.
Alternative Names [upcoming]	My Health Account holder has linked to their own NHI number and known as alternative names. Collected on accounts at Identification Level 2/2N, particularly when they are unable to proceed to Level 3.
Relationship associations [upcoming]	Assertions of employer, association and education associations. This is optional collection subject to connected service requirements

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

My Health Account is a digital health identity service that enables users of New Zealand health-related services (both health consumers and health workforce members) to create a trusted digital health identity, so that they can interact with the health information they are allowed to access.

Use of My Health Account is voluntary. People must opt in to use it and can determine what Identification Level they wish to achieve based on the Services they want to access. While the service is voluntary, most services require risk-based assessment to determine their appropriate level of identification and most digital health services will require the highest identification level to be maintained to ensure legal (such as in compliance with the rules in the Health Information Privacy Code 2020 and other enactments that require or allow information to be used or disclosed) authorisation like consent for accessing said digital health services. Depending on the type of identity proof that the user provides, My Health Account will set an Identification Level (Consumer Health Information Standard (HISO 10046:2024)), guided by the Identification Management Standards 2020). Approved Digital Health Service Providers can use the Identification Level to ensure that private information is only released to users who meet their identity requirements.

My Health Account enables the identification of healthcare consumers and workforce in order to enable their access to health and personal information relevant to their care and treatment and/or professional environment. These activities are aligned to the functions of Health New Zealand under s14 of the Pae Ora Act 2022.

Identification Level 1

At Level 1, users only need to provide an email address to sign up and MHA will send a verification code to confirm it is an email account to which you have access. You have very limited access to work-related digital health services at this level because users still need to confirm who they are. At Level 1, My Health Account stores the following information about you:

- Your email address
- Your preferred name (if provided)
- Your mobile phone number (if provided).

Identification Level 2

At Level 2, users have provided details from one of three possible sources:

- eligible identity documents
- verification information held by the user's general practice (GP)
- Level 2 My Health Account (consumer) verification.

At Level 2, My Health Account Workforce stores the same information as Level 1, plus:

- first name, middle name/s (if applicable), and last name
- date of birth
- HPI number (CPN) if added.

To reach Level 2, one of the following sources must be used:

- identity document check
- healthcare provider check
- My Health Account (consumer) check

Any provided HPI number (CPN), will be checked and verified. Access is restricted to information asserted against the NHI or CPN, or for lower risk services using My Health Account like form submissions or viewing booking information.

Identification Level 3

At Level 3, we check the user that has created the account and that the right person has been connected to the account. At Level 3, My Health Account stores the same information as for Levels 1 and 2, plus:

- Your HPI number (CPN), if added.
- NHI, if a consumer account is present.

My Health Accounts established to Level 3 will authenticate the user to the connected application's complete capability but authorisation to specific information will still be managed by application permissions.

Uplift by Relationship

Under certain circumstances, users may be unable to access an account because they don't hold the identity documents needed to use the document verification service. This may be due to holding documents that don't meet current API standards, or that are Non-New Zealand or Australian government issued foreign identity documents and not digitally verifiable. The users may also be based overseas where their identity is not verifiable by a request to Immigration New Zealand, who holds the authority for foreign documentation.

The expectation is that anyone using My Health Account is under contract to a health providing service domiciled in New Zealand and that the contract is active and has provisions for security in New Zealand. This may include participants or supporting members in a clinical service.

Under these circumstances, the following details are collected to ensure identity validation can be undertaken using an 'uplift by relationship' process which relies on three relationship components:

1. [Responsible Verifier] The digital health service provider's key responsible person, providing us the name of the employee who is asserting that the My Health Account holder is real and that the details on their document are correct (and genuinely dated).
2. [Information Assurance] The details of the individual My Health Account holder as recorded on official documentation (Name, DOB, document type, doc reference number, issue + expiry date, version number if applicable)
3. [Legal authorisation to operate] The details of the health provider contracted in New Zealand (under Health Information Privacy Code Schedule 2 provider) that has confirmed they employ the developer providing services to NZ health sector users.

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

Please provide further information here if you're not using the minimum amount of personal information, or you could use aggregated or anonymised data
The screen flows for My Health Account have been designed to be user-friendly. My Health Account can be accessed from https://identity.health.nz. The approach Health New Zealand has taken is to balance the need to make My Health Account as easy as possible for users to sign up and provide their information, against the need for appropriate security and assurance levels to verify identity to ensure appropriate access controls to personal information are maintained. Users can sign up directly from the My Health Account website, but most accounts are created when they are referred to My Health Account to establish their identity and Identification Level. This is usually by an application or service the Consumer, or workforce member, wishes to use, such as My Health Record. Before signing up to My Health Account, users are provided links to the Privacy statement[6] and Terms of use[7]. Health New Zealand has produced standardised Privacy Statement Materials that are compliant with Rule 3 of the Health Information Privacy Code. The current version of the Privacy statement is in Appendix Three. The website also provides access to advice and guidance[8]. Before users can use My Health Account, their identity must be verified. This verification process involves several steps, and the 'Identification Level' achieved reflects the increasing assurance that can be placed on each step. The user can stop progressing through the identity verification steps when they want to, but they will not be able to access digital health services via My Health Account if they do not meet the Identification Level required for access to the digital health service in question. An identification level summary is set out in Appendix 5.

	YES	NO
Will the project be using cookies or other analytics?	☒	☐
If **yes**, please provide further information:		

[6] https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/privacy-statement

[7] https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/terms-of-use

[8] Advice on creating your My Health Account: https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/creating-your-account and advice on how to get the most from your account: https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/getting-the-most-from-your-account

Cookies

My Health Account uses temporary session cookies. The session cookies are limited to the lifetime of the session and provide support for features such as single sign-on (SSO), as well as enhancing the user experience within the My Health Account self-service portal.

My Health Account does not use third-party or 'tracking' cookies.

Statistical Information

Health New Zealand collects statistical information to help improve the Service and understand how it is being used. This will apply to both user interactions and digital platform performance across all services associated or connected with My Health Account. This includes the event type and session, timestamps, the type of device and browser being used, and the Digital Health Services being accessed. This information is aggregated and doesn't identify the User personally.

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	☒	☐	☐

- Please complete Principle/Rule 1 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 2: Collection directly from the individual concerned

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

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

- If you have answered "**No**", please answer the questions in this section

Please state why you're not collecting information directly from the individual
Some personal information is collected direct from the user, in order to set up an account and begin the verification process, such as email, first name, family name and date of birth. When undertaking the identity document check, identity document details are verified such as name, date of birth, document number, and other details (depending on the document – for example, NZ driver licence). We send the information to our document-checking partners, Cloudcheck from Verifi Identity Services (GBG) or Kiwi Access Card verification via CentraPass, for verification of a match.

Information collected directly from the user cannot just be self-asserted. Identification Management Standards stipulate the need for verification against an authoritative source, such as the identity confirmation lead agency, the Department of Internal Affairs, or their service Realme Verified.

Verifi Identity Services is a New Zealand company, now part of GBG group, that provides GBG Cloudcheck, a service to check records such as passports, driver licences, birth certificates, and other records with the Department of Internal Affairs, Waka Kotahi NZTA, and Australian authorities, on our behalf. We do record when and how you verified your identity, and the type of document you used, but do not retain the unique identifiers associated with those forms of ID.

CentraPass is a New Zealand company that provides a service to verify Kiwi Access Card details with Hospitality New Zealand. As with Cloudcheck, we do record when and how you verified your identity, and that you used your Kiwi Access Card, but do not retain the unique identifiers associated with your card.

Healthcare provider check

When you use the healthcare provider check, we verify your identity using details held by the general practice with which you are enrolled, which is sourced from your General Practice in the National Enrolment Service.

If you have not already added your NHI number to your account, we will check the details you give us against the NHI database to link those details to a unique NHI number.

We then check the contact details held about you by your general practice with which you are currently enrolled (if you authorise us to do so). We send you a one-time code challenge to the mobile phone number that your general practice has on their records.

If you have that mobile phone, you will be able to get and input the one-time code into My Health Account. If you do this successfully, the Identification Level of your account will be updated.

Health workforce

Health workforce members can set up a health workforce identity profile using My Health Account. This allows them to connect with digital health services in a health workforce role when they have a current registration. This includes health practitioners with a Common Person Number (CPN), otherwise known as HPI Number, or other industry-recognised identifier, if approved by My Health Account Workforce for this purpose.

We use your CPN or other approved identifier, together with the name and contact details you have given to us to give you access to health workforce-related digital health services, and to record what health workforce-related digital health services you access.

As a health workforce member, if you are still using your My Health Account to access work-related digital health services, we will not provide your NHI if it is a health workforce-related application, and we will not provide your CPN if it is a health consumer service application.

Relationship Verification

As a health workforce member, personal information relating to associated relationships provided and asserted by the user, with consent, may be verified by organisations that the user asserts to have a

relationship. This may include cases where the user claims to work for or represent an organisation, is enrolled for studies with an education provider, or holds membership with a credential issuing organisation, such as a professional association. Collection of this information is voluntary, but if the organisation has linked digital health services that requires the use of My Health Account for authentication, it may be necessary to confirm run-time authentication demonstrating verified attributes in accordance with the HISO 10046:2024 Consumer Health Identity Standards.
Please state what legislative exception applies *The legislative exceptions can be found in Principle 2 of the Privacy Act and Rule 2 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact the privacy team.*
It is not practicable or possible for individuals to independently verify their own identity. In order to confidently undertake identity verification to the Identification Management Standards 2024, a consented and transparent indirect collection must take place (IPP 2(c)) to confirm identity.

Please complete the following table:

Information collected from third parties	Who is the third party?
name, date of birth, document/card number and, depending on the type of document used, other details such as expiry date or document version. Birth certificate parent-child names	GBG Cloudcheck
name, date of birth, gender.	RealMe® Verified
name, date of birth, gender	CentraPass
names used in practice	Verifying organisations asserted by user

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)?	☒	☐	☐

- Please complete Principle/Rule 2 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 3:
Telling the individual what we are doing

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

(a) the **fact** that the agency is collecting personal information

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

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

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

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

A. How you're going to tell the individual

Please describe how will you tell the individual how the project will manage their information.
For example, will you have a consent form, information leaflet, privacy statement etc?

The current Privacy statement is contained in Appendix Three and the current Terms of use on website. The documents are published on the My Health Account website.

Both documents are linked from the initial sign-up page on My Health Account and are in the footer of the application. The Privacy Materials provided are of central importance in ensuring users have a clear understanding of what My Health Account involves, and how they may control the amount of information collected, and their interaction with services that can be accessed via My Health Account, including workforce profiles.

The Privacy statement is updated regularly as changes are made in My Health Account. Health New Zealand's website contains the most current list of connected digital health services that can be accessed via My Health Account

In addition, advice and guidance can be found on the My Health Account website, providing additional context about My Health Account features

Where will the document be made accessible?
For example, will it be published online? Link in an email? Hard copy?

Privacy statement – Health New Zealand | Te Whatu Ora

https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/my-health-account/privacy-statement

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

B. When you are going to tell the individual

Will you tell individuals before or after you have collected their information? If you're telling the individuals after you have collected their information, how long after?
Individuals are informed as part of their sign-up flow before information is collected.

C. Mandatory or voluntary collection

Please state whether the collection of information is voluntary or mandatory?
Use of My Health Account is voluntary. People must opt in to use it and can determine what Identification Level they wish to achieve based on the Services they want to access. While the service is voluntary, most services will require the highest identification level to be maintained to ensure legal (such as in compliance with the rules in the Health Information Privacy Code 2020 and other enactments that require or allow information to be used or disclosed) authorisation for accessing said digital health services. My Health Account requires users to submit an email address as a username, and for level 2 and above, the individual's name is mandatory for the functional use of the platform. My Health Account has developed a process so that people can make choices on an ongoing basis to connect to the Digital Health Services they wish. Users can also choose when to revoke consent for those Services. My Health Account will be transparent with the use of the data, to maintain and grow social licence. My Health Account always follows these principles: • The information collected will be voluntarily provided by the Consumer. • Information collected is always secured and only shared with those who need to know. • Only the minimum information that is needed is collected. • Information used temporarily (e.g. only for identity verification) is deleted once the purpose has been completed. • The Consumer can grant or deny permission to share their My Health Account information with participating digital health services. Health services will continue to be provided regardless of whether a person has a My Health Account. There are also customer support services available for those unwilling or unable to use My Health Account services.
Please state to what extent, if any, the individual can opt out of providing some or all their information
People must opt in to use My Health Account and can determine what Identification Level they wish to achieve based on the services they want to access. While My Health Account is voluntary, most services using it require risk-based assessment to determine their appropriate level of identification and most digital applications will require the highest identification level to be maintained to ensure legal (such as in compliance with the rules in the Health Information Privacy Code 2020 and other enactments that require or allow information to be used or disclosed) authorisation and consent for accessing or disclosing said digital services. Different identification levels require different types of verification, so choice is available as to which type of verification, which documents and what matching occurs. Ultimately if an individual wants or

needs their identity verified to access the records sitting behind My Health Account, they will need to submit information to the service and have this information verified. If someone wants their identity verified to access records available via MHR, for example, but refuses to use MHA, alternative methods are permissible through an application release form available on the website. However, each service will have a different and manually assessed request mechanism. For workforce this means if their employer requires them to use the application, they will have to complete the required authentication approaches to perform their roles.
Please state what happens if the individual does not want to disclose their information?
If the individual does not want to disclose their information, then they cannot have a My Health Account, and will not be able to log into applications using the My Health Account service. If they are a health worker and their employer has designated this is the method for authentication, they will be unable to perform their role. However, some employers do support more than one Identity platform provider, e.g. Realme login.

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 – Users will be informed as part of onboarding and privacy statements.
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?	☒	☐	☐

- Please complete Principle/Rule 3 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 4:
Fair and lawful collection of information

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

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

Please describe the current proposed method of information collection
If the information is not being collected fairly or lawfully, consider how the collection method could be adapted or modified to meet this Principle 4

Information about the individual is collected at the time of creating an account to assert their identity for this service. Users can assert that Identification Level to digital health services that require an identification level to use them. Depending on the type of identity proof that the user provides, My Health Account sets an Identification Level (guided by the Identification Management Standards 2024). Service Providers can use the Identification Level to ensure that private information is only released to users who meet their identity requirement, managing the risk of impersonation and inappropriate disclosure.

Customer support services are being investigated to address alternative methods of obtaining Identification Levels for those who may not have easily accessible identity documentation or may find Cloudcheck challenging to use. The RealMe identification process is available as an alternative, but it may also be a challenge to achieve for that same group of users.

An account at Identification Level 1 is potentially available to any person, irrespective of age or capacity. This enables access to general health information for notifications to expand Consumer awareness of their health choices and service availability (and how to obtain those services).

If you're collecting information from children or young people, **please state** what steps are you taking to address any power imbalance, and to obtain genuine consent for the collection (or authorisation) of their family/whānau?

Consideration has been given to the minimum age of potential account holders and those who may not have full legal capacity to act on their own behalf as My Health Account develops over time. RealMe permits individuals aged 14 years and over to create an account. Currently, My Health Account does not permit those aged under 16 years to create their own account.

Some parents can choose to establish a relationship with their child or children so that they can share in their child's or children's health and wellbeing outcomes by accessing their health information online. The current 'Add a child' feature only allows for parent-to-child / children relationships for children up to 12 years of age. However, services are generally not available for those between 12-15 years old due to risks of inappropriate disclosures on the grounds of clinical safety.

Parents wishing to establish a relationship with their child or children within My Health Account can enter information about their child, including the child's name, date of birth, and NHI number. Additional information, including the birth certificate number, is also required.

The Identification Level of the parent must be Level 3N (i.e. the most secure level, with the parent's NHI number added to the account) before they can establish a relationship with their child within My Health Account.

The Consumer-supplied information about the child is validated against the child's NHI. The Consumer-supplied information and the parent's name (as recorded against their My Health Account record) is checked against the DIA's birth registry (i.e. the child's birth certificate details), via a third-party service (Cloudcheck). If there is no match, a relationship is not established between the child and the 'parent' making the claim.

My Health Account will not store any address information related to the child nor will we make any address information for the child available via the 'Add a child' feature. This will ensure that no confidential information, such as a physical address, is surfaced through the 'Add a child' feature. It is understood that contact details of this type could, in some cases of family violence, risk compromising the privacy, safety, or security of either of the parents or child / children where a parent-to-child relationship is established through this feature. Any Digital Health Services that connect to this feature must also withhold any address or other contact details relating to the child.

If verification is successful, then the parent can choose to provide a nickname for the child or relationship. My Health Account will record the Parent's NHI number, the Child's NHI number, the child's / relationship nickname, the relationship type, and an expiry date (based on when the child will turn 12), along with verification details in line with what is described under the Identity Document Check above.

When a second parent establishes a relationship to the same child via their My Health Account, the original parent is notified by email that the other parent on the birth certificate has claimed a relationship with the same child. Within their My Health Account profile, both parents will see the first name of the other parent flagged to show them that the other parent has established a relationship with their child.

If one parent disputes the right of the other parent to access a child's or children's information, access to the child's or children's information will be immediately suspended for both parties until the matter is resolved. The information is provided on the basis that Rule 11(5) of the Health Information Privacy Code permits a parent to request health information about their child – based on section 22F of the Health Act. If one parent has been legally excluded from accessing such information about their child then evidence could be produced, and the excluded relationship removed from that parent's My Health Account. In the interim, the parties will be able to obtain information about the dependent child using existing channels with any relevant healthcare provider.

If parents have any questions about the 'Add a child' feature, they can contact the My Health Account Customer Support team on 0800 222 478 or +64 9 307 6155 during standard office hours, 8 am to 5 pm Monday to Friday or send an email to support@identity.health.nz.

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
Not applicable, this is a national digital Identity Service developed in compliance with Department of Internal affairs' Identification Management standards. Consultation on the use of My Health Account has occurred with Whānau Consumer Clinical Digital Council to ensure cultural considerations are identified and addressed.

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?	☒	☐	☐

- Please complete Principle/Rule 4 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 5: Storage and security

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

A. Cloud Computing Services

	YES	NO
Does your project/solution use any cloud-based services?	☒	☐

Cloud services are infrastructure, platforms, or software that are hosted by third-party providers and made available to users through the internet.		

Please provide a brief explanation:

My Health Account information is hosted in Australia but is held only by Microsoft Azure and Amazon Web Services (AWS) as an agent for Health New Zealand and the information may not be used by that contracted provider for its own purposes. Cloudcheck is based in New Zealand but interacts with Australian-based government APIs to check Australian documents, if requested by the Consumer. CentraPass is based in New Zealand but the services that My Health Account interact with are hosted in Australia (AWS). NZ and Australian privacy commissioners have reciprocal arrangements around notification of privacy breaches.

The My Health Account system is designed according to strict security principles and practices. The system architecture provides multiple layers of defence, and all user information is encrypted, both at rest and in transit. Moreover, any user access to their information within the system is tightly controlled, with all access being both logged and audited.

B. Engaging with Information Security

	YES	NO
Have you engaged your relevant information security team for this project/solution?	☒	☐
Has the relevant information security team given its approval for this Project? *If the answer is "yes", please provide a copy of this approval to HNZ Privacy*	☒	☐

Please provide a further information:

Storage and processing of the information on My Health Account is managed by third-party IT vendors. Authority to Operate (ATO) processes and controls are used to ensure that everything than can be reasonably done is done to prevent unauthorised use or disclosure of information.

The IT component of My Health Account has been subject to full Health New Zealand Certification and Accreditation processes, together with independent third-party testing and an Authority to Operate (ATO). Future releases of significance will be subject to this same level of security scrutiny.

Section 11 of the Privacy Act 2020 will apply to the hosting of My Health Account, as the information will be held on behalf of Health New Zealand for safe custody and processing.

All digital health services authorised to connect to My Health Account are required to provide evidence that they meet Health New Zealand Privacy and Security requirements. This includes evidence of Security Testing and completion of a Privacy Impact Assessment.

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

C. Storage

Please describe the system and location where the information is stored?

My Health Account data is held by Health New Zealand in two places – namely, the identity and analytical data stores.

The main identity store is where the system uses user data for providing account services, such as enabling users (Consumer and Health Workforce members) to use their account to log in to digital health services.

The analytical store (or data warehouse) holds an aggregated view of My Health Account information. Health New Zealand uses this store for decision-making and audits. The insights the information provides

assist in the planning of new features and functionality, as well as user profile management on deceased or inactive users.

Data maintained in the analytical store is protected by the same security controls as the main My Health Account system, with full encryption of all information and rigorous access controls.

In addition, to secure data storage the My Health Account system is also designed to be highly available, thereby allowing users (Consumer and Health Workforce members) to access their My Health Account whenever they need it.

D. Access

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

End User sign-up

Users can sign up to My Health Account by either providing an email address and password, or via an existing RealMe® or RealMe® Verified account. All users of My Health Account are required to provide a unique email address as part of their sign-up process. For those users who have signed up using an email address and password, the email address is used both to log in and for communications about the My Health Account service. For those users who have signed up using RealMe® or RealMe® Verified, the email address is used only for communications about the My Health Account service.

All email addresses are validated via a third-party service (SendGrid) by sending a Time-limited One Time Passcode (TOTP) to the supplied email address. Users have 20 minutes to enter the TOTP into My Health Account to validate that they have access to the email account.

Administrators

All account access and all account updates or changes by users will be tracked, as will all access by Health New Zealand system administrators and call centre support. This helps Health New Zealand administrators to resolve queries raised by Users and maintains a record of who has looked at or changed which details. These audit records will be maintained for a minimum of five years and are to be monitored by system administrators.

Please describe why these roles need access to the personal information

Administrators of the programme have to be able to support assisted channel services for end-users around account set up and troubleshooting of identity services.

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)

For administrators of My Health Account, group memberships within Health New Zealand EntraID are required for someone joining the programme team, usually through approval from Health New Zealand National Contact Centre or Product teams, based on specific roles.

When an administrator leaves, Health NZ has service desk deprovisioning processes on Sailpoint automatically off boards when their employment with Health NZ ends.

SailPoint is a software used by HNZ help manage and secure access to critical data and applications across its IT environments.

Will access be controlled by at least two-factor authentication? The Office of the Privacy Commissioner has said that agencies may be in breach of the Privacy Act 2020 if they do not use at least two factor-authentication where applicable.	YES	NO	NA
	☒	☐	☐

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.

My Health Account records all activity against all Consumer and Workforce accounts. System access to audit records is strictly controlled and limited to Health New Zealand staff who are responsible for maintaining security standards and resolving customer support queries.

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?

Process for Managing Information Compromise

To maintain the credibility of the My Health Account service, any suspected compromise, including any unauthorised or accidental access to, disclosure, alteration, loss, or destruction of My Health Account details, NHI details, HPI number (CPN) details, or suspected fraud will be assessed and further investigated, where necessary. As My Health Account continues to be developed, strategies and reporting will continue to be developed to identify when a suspected compromise might have occurred, along with the responsibilities for monitoring this.

- Cases where there is evidence of fraud may be passed to Police for further investigation, and evidence of an offence under the Privacy Act 2020 will be addressed with the Privacy Commissioner[9].
- Notifiable privacy breaches will be reported to the Privacy Commissioner (and affected individuals or the public, where required) as soon as practicable as required by the Privacy Act.
- A warning has been incorporated into Privacy Materials to ensure users are aware of the seriousness of misrepresenting their identity or assuming the identity of another. Users are expected to agree to Terms of use, and this is incorporated into those terms (noting that this may not be appropriate for, or applicable to, young persons).

Reverification

A user's attributes used for determining confidence levels need to be reverified at least once every five years in accordance with the Identification Management Standards. If a user fails to reverify their attributes, then access to the account may be restricted or suspended, and verified information deleted after due process.

Governance

Strong governance is in place to manage any potential risk of 'function creep' – the expansion of, use of, or access to information beyond that originally contemplated.

New, and potentially novel, uses of information may evolve over time, and My Health Account will need to be flexible to respond to those innovations. As My Health Account will be part of the wider digital health environment, a governance structure that is empowered to review, and be informed about, other interlinked services will be essential. My Health Account is not a stand-alone service.

The social licence for My Health Account is key in helping manage the features with which My Health Account will interact. Security and audit oversight is also important to enhancing trust in the various services associated with My Health Account.

It is essential that experienced governance oversight and control is retained to make sure users remain fully informed, and their information is used in a way that is acceptable to them.

Governance includes:

- Privacy Impact Assessments of all applications / Services to be associated with or use My Health Account
- Reference of any privacy-related issues to the Health New Zealand Privacy Officer
- Governance by the Digital Applications and Products Product Board for collection, management, authorised use and disclosure, and deletion of data.

Governance will continue to be reviewed periodically as part of the continued delivery of the My Health Account service to the health sector.

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?	☒	☐	☐

- Please complete Principle/Rule 5 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

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?*
It is expected that most of the information held in My Health Account will be easily viewable by the users on their own device. For information not available directly via My Health Account, the My Health Account Privacy statement outlines how to obtain access to it. They will log into their My Health Account on a unique email they had established on sign up. My Health Account only holds information related to the service it provides and will need to refer requests for information related to other services on to the agency or business unit responsible for those services. This will be managed with existing Health New Zealand processes.
Please outline how you intend to ensure that it is possible to find the information about a specific individual?
It is specific to role-based permissions based on the identity of the user at Level 2, bound to their NHI. For workforce user, it is their account ID and if they have provided an HPI-CPN.

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 Health NZ if it holds personal information about them and the individual can access that information?	☒	☐	☐

- Please complete Principle/Rule 6 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

[9] Misleading an agency by impersonating an individual, falsely pretending to be an individual or to be acting under the authority of an individual for the purpose of obtaining access to that individual's personal information or having that individual's personal information used, altered, or destroyed, is an offence under the Privacy Act – see section 212(2)(c).

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?

Users can correct some information about themselves directly within My Health Account. For other information, users can request updates to their My Health Account information by contacting Customer services for support and/or can arrange to update information on the NHI service by contacting their general practice or hospital, as per current processes. Workforce members (users) can update their own information as self-asserted, unless it is their Health Practitioner Index information. This can be corrected by contacting the HPI team.

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?

Information Updates / Correction

Users can update or correct some information about themselves directly via the My Health Account self-service pages. The information that a user can update themselves includes:

- Preferred name: (Update or Remove)
- Mobile number: (Update)
- Email address: (Update)
- Linked Child or Children NHI numbers: (Remove the relationship between the parent's and child's NHI numbers)
- Password (Update)

Users can request that other information about them is updated by contacting My Health Account customer services. In addition to the above, the information that a user can request to update is:

- NHI number: (Update or Remove)
- HPI number (CPN): (Remove)
- Linked Child or Children NHI numbers: (Suspend the relationship between the parent's and child's NHI numbers)
- Organisation relationships (Update or remove)

In future we plan to recognise the choices of children over 12 including their decision making about who can access their health information through their accounts and to what level of information. This might, for example, allow a parent to see upcoming appointments but not clinical notes on sensitive topics. This is being considered currently and may be included in a future phase.

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?

Information displayed for My Health Account is either self-asserted for verification or is recorded in National systems such as the National Enrolment Service (NES). Corrections can be made either at the

source data level, e.g. by General Practices, or by request to Health New Zealand Customer Services team. In some instances, users will be able to self-correct information through the account.

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?	☒	☐	☐

- Please complete Principle/Rule 7 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

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?

Accuracy is very important to the allocation of the unique Health Digital Identity that will be associated with each My Health Account.

Third-party processes or checking are involved in management of Identification Levels 2 and 3 (with Cloudcheck, or other approved verification partners including RealMe®) or checking against an established NES record used in the provision of healthcare to the Consumer or checking against the Health Workforce member's My Health Account (health consumer). This assists with accuracy in assigning a correct Digital Health Identity to the relevant Identification Level in the User's My Health Account. It is important that the digital health services using workforce accounts clearly understand the implications of 'accuracy' in terms of the information available in the Digital Health Identity provided by the My Health Account Workforce. For a Non-registered Workforce member, only the person's identity can be established – the fact that they are an account holder does not actually establish that they are a Health Workforce member, nor the role they might hold if they are a Health Workforce member, nor their employer. However, their employer and their relationships will be assessed through a verification process to confirm the self-asserted facts are true.

It is noted that the Health Practitioner name provided to other digital health services using My Health Account Workforce for verification mustwill be the name that matches the documented identity attributes. The Health Practitioner's name stated on their Annual Practising Certificate (APC) – i.e. the one attached to the HPI number (CPN) – may be different. Health Practitioners can use the 'Change' feature in the My Health Account Workforce profile page to update their Preferred name so that it matches the name stated on their APC. This additional 'nickname' attribute can then be shared with Digital Health Services. If a connected Digital Health Service needs the Health Practitioner's name to match the Health Practitioner's name attached to the HPI number (CPN), then they can query the Health Provider Index directly.

There is also the ability to seek manual input from the HPI team if an HPI number (CPN) does not match during the digital processes applied, including organisation associations.

The accuracy-related issues in other services that interact with or use My Health Account will need to be carefully reviewed in the Privacy Impact Assessments for those other features.

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?	☒	☐	☐

- Please complete Principle/Rule 8 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 9:
Do not keep information longer than necessary

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

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

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

Only information necessary for the effective administration of the account will be retained. If a person asks for their My Health Account to be closed (inactivated), access to the account will be removed, other than the information required for audit purposes in compliance with the Public Records Act for a period of 10 years. Information to be retained includes the email used to establish the account, the Identification Level (and related dates it was obtained), and any linked NHI or health identifier number. Information collected into Health New Zealand's data warehouse will be retained for analytics' purposes only. The account would not be able to be used to validate further activities in future.

My Health Account administrators may initiate the removal of a HPI number (CPN) from a My Health Account after the transition period to My Health Account Workforce is over and following subsequent attempts to support health practitioners to migrate their account to My Health Account Workforce.

Upon notification of the death of an account holder, their account is inactivated for a period of two years prior to archival. During that time, only authorised representatives may be able to request access to inactivated accounts, as strictly required for the purposes to settle any affairs of the deceased individual.

Note: Parent-to-child relationships are not automatically deleted when the My Health Account that established them is deleted, since the relationship is between the NHI numbers rather than tied to the My Health Account. Users can remove the relationships themselves within My Health Account before their My Health Account is closed, or by requesting the My Health Account customer services team remove the relationships either before or after their My Health Account is closed.

The My Health Account operations team may initiate the closing of an account (inactivation) and / or deletion of information not related to minimum data retention legislation, if advice is received that an account may no longer be valid or needed (e.g. on notification that the owner of the account has deceased; or in line with fraud or privacy breach escalation processes, as outlined below).

A user's attributes used for determining confidence levels need to be reverified at least once every five years in accordance with the Identification Management Standards. If a user fails to reverify their attributes, then access to the account may be restricted or suspended, and verified information deleted after due process.

Additional archival processes in relation to General Disposal Authority rules mean we keep changes in email and identity attributes so we could maintain if usernames linked to accounts were recycled or repurposed by other users who may have access, such as a family or employer-owned shared account.

Please **state** the applicable legal requirements for retention of information (if any).
For example, Health (Retention of Health Information) Regulations 1996, Public Records Act 2005, General Disposal Authority 6, Functional Disposal Authority 1.

Health (Retention of Health Information) Regulations 1996, Public Records Act 2005 – GDA6 7.1.2 Routine Audit and Audit Administration Records relating to routine audits, including audits relating to the payroll system.

Please state:

- whether all the personal information needs to be retained by the project
- whether the information needs to be retained in a form that identifies the individual (*can it be retained in a de-identified manner)*

All information must be retained for the period, as My Health Account is a source system for defining digital access for users.

Please state:

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

If a person asks for their My Health Account to be closed, access to the account will be removed, other than the information required for audit purposes in compliance to the Public Records Act for the period of 10 years. Information to be retained includes the email used to establish the account, the Identification Level (and related dates it was obtained), and any linked NHI or health identifier number. Information collected into Health New Zealand's data warehouse will be retained for analytics' purposes only. The account would not be able to be used to validate further activities in future.

My Health Account operational team is responsible for managing the long-term retention and disposal requirements with guidance of the Health New Zealand Information Management Team.

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	☒	☐	☐

- Please complete Principle/Rule 9 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

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 purpose of My Health Account is to allow users to create a trusted digital health identity, which they can use to securely access digital health services that link them with the health information they are authorised to access. This PIA does not address the use of information by approved digital health services, however:

- Digital health services must pass various security testing and compliance requirements before users can interact with them (which includes providing evidence to My Health Account of Privacy and Security due diligence)
- Digital health services are asked to provide links to their Privacy statement and Terms of use so that these can be displayed to the Consumer in My Health Account
- Users are asked for permission to share their attributes with a digital health service
- Digital health services are required by Terms of Use to advise My Health Account if their intended use of the information changes so that My Health Account can re-prompt users for their permission to share their attributes
- Users can revoke their permission to share attributes with a digital health service at any time.

Users on our privacy statement also made aware that standard uses of their health information (for example, for managing their health) will continue to be managed by service providers in accordance with their usual processes and that My Health Account will not be able to control all access to and use of their information.

Documents used for verification are not kept or maintained within Health New Zealand, once the verification steps are completed, usually with the third-party verification service provider. The only exception will be for when there is a request to bind, due to inability to use third party automated processes, and an auditable system is established for manual processing of those cases.

ACC and Health NZ share common health sector users. ACC have a scenario where these users require authenticated access to a clinical payment management application as well as other HNZ digital health services.

	YES	NO
Are the uses listed above consistent with the purposes of collection you have outlined in Principle 1?	☒	☐
If the answer is "**No**", **please state** what legislative exception applies. *The legislative exceptions can be found in Principle 10 of the Privacy Act or Rule 10 of the Health Information Privacy Code. If you're unsure if an exception applies, please contact the Privacy team.*		
Not applicable		

	YES	NO
Does the use of information by the project involve information matching or sharing?	☒	☐
If the answer is "**yes**", please provide more information here. 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.		

Identity Document Check

Users can verify identity information in My Health Account by verifying an official document, such as a Passport or Driver Licence. Users are required to provide information as recorded on the selected document type, including name, date of birth, document/card number and, depending on the type of document used, other details such as expiry date or document version.

The User-supplied information is checked against the source records (e.g. those held by DIA or Waka Kotahi) via third-party services to ensure that there is a record of an official document that matches the details provided. This check meets the requirements of Information Assurance according to the Identification Management Standards 2020.

My Health Account retains the user-supplied name and date of birth. A 'verification' details record is also kept – i.e. verification method used, verification result (valid or invalid), and the date and time of verification. The verification details are used solely for audit purposes in the event there is an apparent misuse of the verification service (e.g. in the case a person seeks to misrepresent the identity of another Consumer). It will only be accessible to select, authorised individuals from Health New Zealand (or their agents) if they are required to investigate a possible breach of the Consumer Terms of use or fraud. This role will be limited, and all access tracked.

Healthcare Provider Check

Users can choose to verify their identity using information already held about them in Health New Zealand records. Users are required to provide information about themselves including their name, date of birth, address and the General Practice or Medical Centre with which they are currently enrolled. They also have the option to provide their gender and NHI number.

The User-supplied information is used to find and validate the user's NHI number and their patient record in the National Enrolment Service (NES). If a matching patient record is identified for the Consumer, and if the patient record includes a Mobile phone number, the Consumer can request that My Health Account send a Time-limited One Time Passcode (TOTP) to that Mobile number via SMS. The Users is shown the last four digits of the phone number on the My Health Account screen (with the other details obscured) so that they can determine if they still have access to the phone with that number.

The User must correctly input the code into My Health Account within a 20-minute period, before it expires. If the Consumer can successfully complete the TOTP challenge before it expires, it is considered a strong and direct link to the person who owns the NHI and is enrolled with the specified General Practice.

My Health Account retains the user-supplied name and date of birth (where not already stored) along with verification details in line with what is described under the Identity Document Check above.

RealMe® Verified

Users who have signed up via a RealMe® account with a 'Verified' status can choose to allow RealMe to share their 'Verified' information with My Health Account.

If a User consents for RealMe® to provide their verified attributes, then RealMe® shares information including name, date of birth, gender, and address. This information, along with a user-provided unique email address, will be used to create a My Health Account with a strengthened assurance that the person claiming the identity attributes is the owner of the identity. This gives them an account with an Identification Level of 3.

My Health Account retains the name and date of birth along with verification details in line with what is described under the Identity Document Check above.

Adding NHI Number

Users who have completed an identity verification process up to Identification Level 2 or 3, can choose to add their National Health Index (NHI) number to their account. The NHI number is a unique identifier that links an individual to their personal health information recorded in the National Health Index (NHI). This will allow them to share the number as an attribute with connected Digital Health Services, making it easier for them to be linked to their personal health information and records.

My Health Account will use the verified information (names and date of birth) stored against the Consumer's record to search for a matching NHI record. Matching NHI records are scored on uniqueness, based on a matching algorithm. If the record is not deemed to be a unique match, the Consumer is asked to provide more information. The Consumer can choose to provide their NHI number (if known), their gender and/or their address. My Health Account then re-attempts to find a uniquely-matching NHI record.

If a uniquely-matching NHI record is identified, the NHI number for the active NHI record is stored against the Consumer's My Health Account record.

If a uniquely-matching NHI record cannot be identified, or more than one matching NHI record is found, then the record is sent to the Health New Zealand NHI-matching team who will review the provided information and other Health New Zealand datasets to determine the correct NHI record to link to the My Health Account record. If no existing NHI record is identified, the NHI-matching team may create a new NHI record to be linked to the Consumer's My Health Account record.

If the Consumer has provided a gender and/or address as part of the matching process, this information is deleted from their record as soon as a successful NHI match has been completed.

An NHI number can only be linked to a single My Health Account record.

Adding HPI number (CPN)

In April 2023, Health New Zealand released My Health Account Workforce – a digital health identity service for Aotearoa New Zealand's health workforce. The service allows health workforce members to create a trusted digital health identity so that they can interact with the work-related and health information that is necessary for them to perform their work role.

Prior to the release of My Health Account Workforce, registered health practitioners who had completed an identity verification process up to Identification Level 2 or 3, could choose to add their Health Provider Index (HPI) – Common Person Number (CPN) to their My Health Account. The HPI number (CPN) is a unique identifier that is issued to certain health practitioners and links the practitioner to their record in the Health Provider Index (HPI). This allowed them to share the number as an attribute with work-related Digital Health Services, making it easier for them to be linked to their health workforce information.

My Health Account will use the verified information (names and date of birth) stored against the Consumer's record to search for a matching HPI record. Users must provide the HPI number (CPN) but can edit the name information that is used in the search, in case the name on their Annual Practising Certificate is different to the name used on their identity document.

If a uniquely-matching HPI record is identified, the HPI number (CPN) for the HPI record is stored against the Consumer's My Health Account record.

If a uniquely-matching HPI record cannot be identified, the Consumer is provided with advice on how they can try again.

If the users has provided a different name as part of the matching process, this information is not stored against their My Health Account record, unless consented for linking to another authoritative source to prove their identity.

An HPI number (CPN) can only be linked to a single My Health Account record.

Employers and relationships asserted by the users can also verified in due course to confirm identity of individuals.

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?	☒	☐	☐

- Please complete Principle/Rule 10 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

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 Health NZ?	☒	☐

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

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 the Privacy team.

The disclosure enabled via My Health Account during the verification process is signalled in advance to users, who may then choose to proceed with the disclosures (for example, to GBG Cloudcheck or other authorised third-party identity services we have licensed identity confirmation services).

The information disclosed to digital health services about users is determined as part of the onboarding process, following a Privacy Impact Assessment. Only information deemed as necessary for the services offered to the user is approved for disclosure to the digital health service.

In addition, users are required to approve the disclosure of information to the digital health service before it is shared. At any time, the user can choose to deny or revoke further disclosure of information.

Subsequent controls on disclosure that may be associated with My Health Account will need to be carefully reviewed in future releases, prior to incorporating and enabling those activities. A framework, within which other services may authorise disclosures, will need to be provided so that other 'enabling' services (such as My Health Record) fully address disclosure implications to make sure the My Health Account role is fully considered, and any authorisation matches the My Health Account Identification Levels. The risk is managed through initial certification and PIA review of any additional connected health application.

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 disclosure enabled via My Health Account during the verification process is signalled in advance to users, who may then choose to proceed with the disclosures (for example, to Cloudcheck or other authorised third-party identity services).

The information disclosed to Digital Health Services about Users is first determined as part of the Onboarding process, following a Privacy Impact Assessment. Only information deemed necessary for the digital health services about the Users are approved for disclosure to the digital health service.

In addition, Users are required to approve the disclosure of information to the digital health service before it is shared on the first occasion on which they use the digital health service. At any time, the Users can choose to deny or revoke further disclosure of information in relation to that particular digital health service.

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 Health NZ or an exception applies	☒	☐	☐

- Please complete Principle/Rule 11 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

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 Health NZ disclose personal information to a foreign person or entity?	☒	☐

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

Please state:

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

My Health Account information is hosted in Australia but is held only by Microsoft Azure and Amazon Web Services (AWS) as an agent for Health New Zealand and the information may not be used by that contracted provider for its own purposes. Cloudcheck is based in New Zealand but interacts with Australian-based government APIs to check Australian documents, if requested by the Consumer. CentraPass is based in New Zealand but the services that My Health Account interact with are hosted in Australia (AWS). Health New Zealand has taken a position of risk tolerance in terms of the gaps between equivalency in New Zealand and Australian privacy law in similar matters to date.

We expect some New Zealanders with accounts will access from overseas when travelling or having emigrated to another country. The same access applies for those overseas as within New Zealand. With workforce applications, like ACC Provider Hub, vendor developers may be based overseas and require access.

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	☒	☐	☐

- Please complete Principle/Rule 12 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Principle 13: Creation or use of unique identifiers

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

To avoid doubt, Health NZ does not assign unique identifiers when it records and uses a unique identifier so that we can communication with another agency about the individual (please see IPP13(3) and Rule 13(5).

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

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

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

Please explain:

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

The National Health Index (NHI) number is the unique identifier for patients who receive healthcare in New Zealand and 'is the cornerstone of clinical and administrative patient-related information'. It is not used as the account identifier.

My Health Account's use of the NHI number in the health sector is for the purpose of unique identification of the individual concerned. The applications / services seeking to use My Health Account NHIs should be restricted to those that comply with the requirements of the HIPC (as per Rule 13(3) (noting that the agencies approved to assign the NHI number have been updated to include the new agencies under the Pae Ora Act). Users are able to choose to include an NHI in their record or not, but most consumer digital health services are only available with the NHI linked.

All parties interacting with My Health Account (other than users) will be consistent with Schedule 2 of the HIPC.

The Health Provider Index (HPI) – Common Person Number (CPN) is the unique identifier for registered health practitioners in New Zealand and links them to the Health Provider Index. My Health Account allows individuals that had already been assigned an HPI number (CPN) to add it to their My Health Account workforce profile, in order to uniquely identify themselves to digital health services as a health

practitioner. This complies with the requirements of Rule 13(4) such that any assignment must be by a health agency (in terms of applications / services authorised to operate with My Health Account)

My Health Account uses GUID number (globally Unique 32 hexadecimal characters) for its account identifier. It is used only by consuming systems to uniquely identify the user in such a way that the user can change their email address without affecting access to that consuming system in future. It is not shared with or displayed to the user. It is not shared with any party other than consuming applications in a 'behind the scenes' manner.

Compliance check with Principle 13

Does the project comply with Principle 13?	YES	NO	UNSURE
Does the project comply with Principle 13/ Rule 13 regarding the assignment and/or use of unique identifiers?	☒	☐	☐

- Please complete Principle/Rule 13 of the Risk and Mitigation Tables (Appendix 1), summarising the actual/potential risks identified with this Principle, and outline the current controls, and/or recommendations to be implemented before continuing on to the next section.

Artificial Intelligence Initial Assessment

The Privacy Act 2020 applies to the use of Artificial Intelligence (**AI**). There is no single, universally accepted definition for AI. For the purposes of this PIA, we use the definition of the Office of the Privacy Commissioner- *"AI refers to computer systems doing tasks that seem like intelligent behaviour, such as finding patterns, putting items into categories, and triggering actions based on information", including:*

- ***machine learning systems** developed or refined by processing training data.*
- ***classifier systems** used to put information into categories (e.g., captioning images).*
- ***interpreter systems** that turn noisy input data into standardised outputs (e.g., deciding what words are present in speech or handwriting).*
- ***generative systems** used to create text, images, computer code, or something else.*
- ***automation** where computers take on tasks that people have done up until recently.*[10]

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

If you have answered '**yes'** to this question, please complete the AI row of the Risk and Mitigation Tables (Appendix 1), and then complete the "**Artificial Intelligence – Privacy Assessment"**. Please contact the Privacy team for more information.

Please note that in addition to engaging with HNZ Privacy on the use of Artificial Intelligence it is critical you also engage with other relevant stakeholders as applicable. HNZ Privacy approval of the use of Artificial Intelligence does not cover approvals from other relevant stakeholders.

Third Party Artificial Intelligence	YES	NO
Has your project been asked to **share** information that Health NZ holds (including personal or health information) with a third party to enable the third party to design, develop, train and/or deploy their own AI?	☐	☒
If Health NZ will contract with a third party for this project/ solution, do the contract terms/ Terms of Service etc allow the third party to use Health NZ information to develop, train and/or deploy their own AI?	☐	☒
If the answer is **'yes'** to either of these questions, please provide additional information:		
Not Applicable		

Once you have completed this section (Artificial Intelligence), please move on to the next section (Privacy Policies and Terms of Service).

[10] Office of the Privacy Commissioner- Artificial intelligence and the Information Privacy Principles, September 2023.

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

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

Third Party Privacy Policy/Statement	**YES**	**NO**
Has the Project reviewed the current Privacy Policy/Statement of the third party?	☒	☐
If the Project identified any privacy risks, mitigations, or controls from its review of the Privacy Policy/Statement, have these been documented and addressed in this Privacy Impact Assessment?	☒	☐
If you have answered "**no**" to either of these questions, please provide additional information:		
Not Applicable		
Terms of Service (or other contractual provisions)	**YES**	**NO**
Has the Project reviewed the relevant Privacy clauses in the Terms of Service (or other contractual provisions as applicable)?	☒	☐
If the Project identified any privacy risks, mitigations, or controls from its review of the relevant Privacy clauses in the Terms of Service (or other contractual provisions as applicable), have these been documented and addressed in this Privacy Impact Assessment?	☒	☐
Have you engaged HNZ Legal on a review of the relevant contractual provisions?	☒	☐
If you have answered "**no**" to any of these questions, please provide additional information:		
Not Applicable		

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

Review and Sign Off

Conditional Approval	YES	NO
Are you seeking **conditional approval** of this Privacy Impact Assessment? *For example, if the Project does not have an approved Authority to Operate and it needs one from Information Security, you may ask for conditional approval until such time as one is in place.*	☐	☒
If you **are** seeking conditional approval, please state why:		
No.		
If you are seeking conditional approval, please note that you **must**: - Inform HNZ Privacy as soon as the condition has been met; and - Update this Privacy Impact Assessment as required when the condition has been met		

National Privacy Office
I approve this Privacy Impact Assessment as having sufficiently and appropriately identified and assessed privacy risks and mitigations.

Name: Viv Kerr – Head of Privacy Signature: Viv Kerr	Date: 23 /06 /2025

Business Owner
I approve this Privacy Impact Assessment, accepting that:
- I am accountable for the appropriate management of Personal Information associated with this initiative/system
- I am responsible for ensuring identified mitigations are actioned, and
- I own the privacy risks associated with this initiative/system.

Name: Joel Brown – Group Manager, Health Identity & Eligibility Signature: Joel Brown	Date: 23/06/2025

Project Manager
I endorse that this Privacy Impact Assessment accurately and comprehensively describes the relevant parts of the initiative/system to be assessed and that all substantive privacy risks have been identified, along with appropriate mitigations to address these.

Name: Samuel Wong, Manager, Channels Identity & Access Signature: Samuel Wong	Date: 23/06/2025

Appendix 1: Risk and Mitigation Tables

- The risk and mitigation tables aim to help 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.
- If there is more than one identified risk for a Principle/Rule, copy the relevant Principle/Rule ROW, and paste under the copied row and amend Reference No's. (see 'Guide for Completing a Privacy Risk Assessment' for examples)

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
R.01	Nil	Change of process/ functionality after go-live and throughout the life of the Project, affecting the PI/HI involved.	National Privacy Office PIA/PTA Library	Low	The project will review and update this Privacy Impact Assessment whenever there is a chance to how personal information is collected, stored, accessed, used, disclosed, or otherwise handled. The Project team will proactively review this PIA every 12 months after the month of go-live, to ensure it is still accurate and up to date.	Rare	Minimal	Low		Every 12 months following project go live

R.02	**Principle/Rule 1** Collection is for a lawful purpose, and is necessary for that purpose		*Purpose* My Health Account's purpose is to enable user to verify their identity information to the level required to access the digital health services with which they wish to engage. *Necessary* My Health Account has analysed the minimum identity information that can reliably be used for identification at different identification levels. A summary of the Identification Levels is contained in Appendix 5. My Health Account has endeavoured to balance the amount of information necessary to meet identification requirements with the risk posed by incorrectly assigning an identification level that could enable the wrong person to access sensitive information. There is an initial level of access to generic health information (Identification Level 1), which can be enabled by providing a verified email address only. This does not need to be linked to the user in any identifiable way. To access services that require a higher Identification Level, it is necessary for users of My Health Account to supply additional information that can then be verified against other sources of information. The base information that needs to be verified is: • Name* (including given and family names) • Date of Birth* In addition, depending on the verification method or process selected, Users may need to provide additional information, such as: • Document type* • Document number • Expiry Date • Parent's names • Enrolled GP practice • Address • Gender • NHI number* • HPI number (CPN)* • Child's name • Child's Date of Birth • Child's NHI*	Low		Unlikely	Minimal	Low		

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
			• Employer information [upcoming] • Education provider information [upcoming] • Membership association information [upcoming] Of the above information, only those with an asterisk (*) next to them are retained along with verification method and the result of the verification (i.e. success / failure). Adding an NHI number or HPI number (CPN) to a My Health Account is optional, but necessary if users wish to engage with connected Digital Health Services that do not have the ability to locate those identifiers themselves . Adding a mobile number is an option for user if they prefer to receive second-factor authentication challenges via SMS rather than email, and if they would like to share that contact method with Digital Health Services.							

R.03	**Principle/Rule 2** Information is collected directly from individual		• My Health Account is an 'opt-in' service with the user (unless under 16 years old), supplying most information directly to My Health Account themselves, except for: • The NHI number, which the Consumer authorises My Health Account to search for and match to their verified information • Information related to background processing, such as results of verification processes (i.e. success / failure), including: • Document Identity checking • Healthcare Provider checking • NHI number matching • HPI number (CPN) matching • The mobile number used in the Healthcare Provider Check, which needs to be sourced from the National Enrolment Service (NES) to complete the verification process • The details from RealMe that populate My Health Account (after express authorisation from the Consumer within the RealMe application). • Any additional names and relationships self-asserted may be verified on agreement. • Users must provide the HPI number (CPN) but can edit the name information that is used in the search, in case the name on their Annual Practising Certificate is different to the name used on their identity document. • If a uniquely-matching HPI record is identified, the HPI number (CPN) for the HPI record is stored against the Consumer's My Health Account record. • If a uniquely-matching HPI record cannot be identified,	Low		Select.**Rare**	SelectMinimal	SelectLow		

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
			the Consumer is provided with advice on how they can try again. • If the users has provided a different name as part of the matching process, this information is not stored against their My Health Account record, unless consented for linking to another authoritative source to prove their identity. • An HPI number (CPN) can only be linked to a single My Health Account record. Provided the Privacy Materials that accompany My Health Account remain appropriate and consistent with the expressed intent, Rule 2(2)(a) will apply – the individual authorises collection of the information from someone else.							

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
R.04	**Principle/Rule 3** Individual is aware of collection		The current Privacy statement is contained in Appendix Three. The documents are stored on the My Health Account website. Both documents are linked from the initial sign-up page on My Health Account and are in the footer of the application. The Privacy Materials provided are of central importance in ensuring users have a clear understanding of what My Health Account involves, and how they may control the amount of information collected, and their interaction with services that can be accessed via My Health Account. The Privacy statement is updated regularly as changes are made in My Health Account. Health New Zealand's website contains the most current list of connected digital health services that can be accessed via My Health Account In addition, advice and guidance can be found on the My Health Account website, providing additional context about some My Health Account features.	Low	Updated online privacy statement to reflect Appendix 3's version. https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/my-health-account/privacy-statement To be completed before end of month of go-live of MHA-U.	Select.**Possible**	SelectMinor	SelectMedium	Samuel Wong	30 June 2025

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
R.05	**Principle/Rule 4** Collection is done in a lawful, fair and unintrusive way	Collection is generally conducted at source for end users unless approved identity confirmation service is used for verifications.	Consideration has been given to the minimum age of potential account holders and those who may not have full legal capacity to act on their own behalf as My Health Account develops over time. RealMe permits individuals aged 14 years and over to create an account. However, My Health Account is only permitted for those aged over 16 years to create their own account unless exception given on participating in an approved medically supervised programme. The Privacy statement and Terms of use confirm a parent or legal guardian may bind to a child's account before they turn 12 years old. However, services are generally not available for those between 12-15 years old due to risks of inappropriate disclosures on the grounds of clinical safety. Customer support services has escalation processes to address alternative methods of obtaining Identification Levels for those who may not have easily accessible identity documentation or may find Cloudcheck challenging to use. Kiwi Access Card, and RealMe Verified identification process is available as an alternative, but it may also be a challenge to achieve for that same group of users. Uplift by relationship, using several confirmation sources, is permitted under exceptional policy managed by Health New Zealand. An account at Identification Level 1 is potentially available to any person, irrespective of age or capacity. This enables access to general health information to expand users awareness of their health choices and service availability (and how to obtain those services).	Low		Select.**Rare**	Minor	Low		

R.06	**Principle/Rule 5** Storage and Security of information		Storage and processing of the information on My Health Account is managed by third-party IT vendors, and My Health Account will use its Authority to Operate (ATO) processes to ensure it has done everything reasonably in its power to prevent unauthorised use or disclosure of information. The IT component of My Health Account has been subject to full Ministry of Health and Health New Zealand Certification and Accreditation processes, together with independent third-party testing and an Authority to Operate (ATO). Future releases of significance will be subject to this same level of security scrutiny. Section 11 of the Privacy Act 2020 will apply to the hosting of My Health Account, as the information will be held on behalf of Health New Zealand for safe custody and processing. All services authorised to connect to My Health Account are required to provide evidence that they meet Health New Zealand Privacy and Security requirements. This includes evidence of Security Testing and completion of a Privacy Impact Assessment. For the 'Add a child' feature, access to the child's address and other contact details by either parent must be limited or excluded through design and onboarding controls. It is a recognised risk in a family violence situation that disclosure of address or contact details may enable one parent to locate the other, without the consent of that other parent. All account access and all account updates or changes by users will be tracked, as will all access by system administrators and call centre support. This helps Health New Zealand administrators to resolve queries raised by end-users and maintains a record of who has looked at or changed which details. These audit records will be maintained for a minimum of 10 years and are to be monitored by system administrators.	Low		Select.**Rare**	SelectMinimal	SelectLow		
R.07	**Principle/Rule 6** Individual can access their information		It is expected that most of the information held in My Health Account will be easily viewable by the users on their own device. For information not	Low		Select.**Rare**	SelectMinimal	SelectLow		

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
			available directly via My Health Account, the My Health Account Privacy statement outlines how to obtain access to it. My Health Account only holds information related to the service it provides and will need to refer requests for information related to other Services on to those services. This will be managed with existing Health New Zealand Privacy team processes.							
R.08	**Principle/Rule 7** Information can be corrected if requested		Users can correct some information about themselves directly within My Health Account. For other information, Users can request updates to their My Health Account information by contacting Customer services for support and/or can arrange to update information on the NHI service by contacting their general practice or hospital, as per current processes.	Low		Select.**Rare**	SelectMinimal	SelectLow		

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
R.09	**Principle/Rule 8** Information is accurate, relevant etc before use/disclosure	HPI-CPN for registered health workforces are used to verify their current association with a responsible authority, e.g. Medical council. Exact name match is required to determine it is the person associated with their account and drive access management considerations on connected clinical applications which require only approved users to access.	Accuracy is very important to the allocation of the unique digital health identity that will be associated with each My Health Account. Third-party processes or checking are involved in management of Identification Levels 2 and 3 (with Cloudcheck, or other approved verification partners including RealMe verified) or checking against an established national enrolment services record used in the provision of healthcare to the Consumer. This should assist with accuracy in assigning a correct identity to the relevant My Health Account. It is noted that the user's name provided to other services using My Health Account for verification will be the name that matches the documented identity attributes, not the NHI name, if there is a difference between the two. This is likely to align the legal identity of the users with the results produced via use of My Health Account as the NHI need not record the Consumer's legal name. This should enhance accuracy of the display produced. Users also have the option of specifying a Preferred name on their profile, which can be shared with Digital Health Services. There is also the ability to seek manual input from the specialist NHI team if an NHI number does not match during the digital processes applied. Health practitioner Index – common person number is available as an option for workforce users to state (and verify) their scope to access clinical information. Exact name match is required to what is on their registration body records to ensure accuracy. The accuracy-related issues in other services that interact with or use My Health Account will need to be carefully reviewed in the Privacy Impact Assessments for those other features.	Low		Select.**Possible**	SelectMinimal	SelectMedium		

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
R.10	**Principle/Rule 9** Information is not kept longer than necessary		Only information necessary for the effective administration of the account will be retained. A summary of the information retained is recorded in IPP1. If a My Health Account is closed by the user (or because of an administration process – e.g. on notification that a Consumer is deceased) a record of the fact that there was an account, the email used to establish the account, the Identification Level (and related dates it was obtained), and any relevant linked NHI or health identifier number is retained. These details will be required as an audit record of authorisation for activity related to their files. A user's verified attributes need to be reverified at least once every five years, as required by the Identification Management Standard. If a user fails to reverify their attributes, then access to the account may be restricted or suspended, and verified information deleted after due process, including when no longer required for business purposes and legal requirements.	Low	Consumer account is dominant account due to consumer access is a universal service. Workforce profiles can be deactivated if no longer in use, if the user leaves contract or association as a health worker.	Select.**Rare**	SelectMinimal	SelectLow	Samuel Wong	June 2026

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
R.11	**Principle/Rule 10** Information is used for the purpose it was collected		The purpose of My Health Account is to allow users to create a trusted digital health identity, which they can use to securely access Digital Health Services that link them with the health information they are authorised to access. This PIA does not address the use of information by Digital Health Services, however: • Digital Health Services must pass various security testing and compliance requirements before Users can interact with them (which includes providing evidence to My Health Account of Privacy and Security due diligence) • Digital Health Services are asked to provide links to their Privacy statement and Terms of use so that these can be displayed to the Consumer in My Health Account • Users are asked for permission to share their attributes with a Digital Health Service • Digital Health Services are required by Terms of Use to advise My Health Account if their intended use of the information changes so that My Health Account can re-prompt Users for their permission to share their attributes • Users can revoke their permission to share attributes with a Digital Health Service at any time. Users also need to be made aware that standard uses of their health information (for example, for managing their health) will continue to be managed by service providers in accordance with their usual processes and that My Health Account will not be able to control all access to and use of their information.	Low		Select.**Rare**	SelectMinimal	SelectLow		

R.12	**Principle/Rule 11** Disclosure of information	Inappropriate disclosures causing harm.	The disclosure enabled via My Health Account during the verification process is signalled in advance to Users, who may then choose to proceed with the disclosures (for example, to Cloudcheck or other authorised third-party identity services). The information disclosed to Digital Health Services about users is determined as part of the onboarding process, following a Privacy Impact Assessment. Only information deemed as necessary for the services offered to the user is approved for disclosure to the Digital Health Service. In addition, users are required to approve the disclosure of information to the Digital Health Service before it is shared. At any time, the Consumer can choose to deny or revoke further disclosure of information. Subsequent controls on disclosure that may be associated with My Health Account will need to be carefully reviewed in future releases, prior to incorporating and enabling those activities. A Framework, within which other services may authorise disclosures, will need to be provided so that other 'enabling' services (such as Shared electronic health record and My Health Records) fully address disclosure implications to make sure the My Health Account role is fully considered, and any authorisation matches the My Health Account Identification Levels. The 'Add a child' feature, enabling access by some parents to some information about their young children under 12 years old, will need to be monitored to ensure that address and contact details remain masked so that there is no risk of stalking or locating a former partner via this service. This will include interactions with other Digital Health Services that may inadvertently free up access to this information. There is a business process in place to suspend a parent-to-child relationship if a legitimate concern is raised with the My Health Account Customer Service team. It is also important that the 'Add a child' feature is controlled so that a parent is not able to gain access to a child's full health records via connected Digital Health Services. This is needed to avoid the disclosure of	Medium	No information access available from 12-15 years old users unless on approved medically supervised programme. Only 16 years and above can create their own accounts. Health workers must be using level 3 accounts and have strict role and audit controls on approved connected digital health services before they can request access to search for consented consumer records. Adolescent led controls to address 12-15 year old access to services being explored but requires inter-agency policy agreement.	**Possible**	Minor	Medium	Samuel Wong	30 June 2026

Reference No.	Privacy Principle or Rule	Risk Description	Current Controls	Current Risk Rating	Recommendations to further mitigate risk	Target Risk Rating			Owner	Date
	Principle or Rule being assessed	**Description of potential/actual risk**	**Controls currently in place which mitigate the risk**	**Risk Rating**	**Recommendation to mitigate residual risk**	**Probability**	**Consequence**	**Risk Rating**	**Role/area responsible for implementing**	**Date recommendation to be implemented by**
			any family violence allegations (which may then inadvertently alert the perpetrator). It is recommended that Onboarding controls are applied to connected Digital Health Services, so this risk is mitigated.							
R.13	**Principle/Rule 12** Disclosure outside of New Zealand		My Health Account information is hosted in Australia but is held only by Microsoft Azure and Amazon Web Services (AWS) as an agent for Health New Zealand and the information may not be used by that contracted provider for its own purposes. Cloudcheck is based in New Zealand but interacts with Australian-based government APIs to check Australian documents, if requested by the Consumer. CentraPass is based in New Zealand but the services that My Health Account interact with are hosted in Australia (AWS). There will be no disclosure of information made outside New Zealand except for users who must support the system under the rules identified in Rule 12 for My Health Account. Policies enforced on the platform includes geo-fenced location access and impossible travel policies on the platform to determine user access locations.	Low		Select.**Rare**	SelectMinimal	SelectLow		

R.14	**Principle/Rule 13** Using/assigning unique identifiers	Use of NHI, HPI and account IDs for managing identification of accounts.	The National Health Index (NHI) number is the unique identifier for patients who receive healthcare in New Zealand and 'is the cornerstone of clinical and administrative patient-related information'. It is not used as the account identifier. My Health Account's use of the NHI number in the health sector is for the purpose of unique identification of the individual concerned. The applications / Services seeking to use My Health Account NHIs should be restricted to those that comply with the requirements of the HIPC (as per Rule 13(3) (noting that the agencies approved to assign the NHI number have been updated to include the new agencies under the Pae Ora Act). All parties interacting with My Health Account (other than users) will be consistent with Schedule 2 of the HIPC. The Health Provider Index (HPI) – Common Person Number (CPN) is the unique identifier for registered health practitioners in New Zealand and links them to the Health Provider Index. My Health Account initially allowed individuals that have already been assigned an HPI number (CPN) to add it to their My Health Account, in order to uniquely identify themselves to Digital Health Services as a health practitioner. This complies with the requirements of Rule 13(4) such that any assignment must be by a health agency (in terms of applications / Services authorised to operate with My Health Account). This feature is to be phased out from April 2023, when the new My Health Account Workforce becomes operational. My Health Account uses GUID number (globally Unique 32 hexadecimal characters) for its account identifier. It is used only by consuming systems to uniquely identify the user in such a way that the user can change their email address without affecting access to that consuming system in future. It is not shared with or displayed to the user. It is not shared with any party other than consuming applications in a 'behind the scenes' manner.	Medium		Select.**Unlikely**	SelectMinor	SelectMedium		
R.15	**AI** Use of AI within the project	Not applicable as no AI is used.				Select.	Select	Select		

Te Whatu Ora
Health New Zealand

Target Risk Rating Table

Consequence	Rare	Unlikely	Possible	Likely	Almost Certain
Severe	Medium - 11	High - 16	High - 20	Extreme - 23	Extreme - 25
Major	Medium - 7	Medium - 12	High - 17	High - 21	Extreme - 24
Moderate	Medium - 4	Medium - 8	Medium - 13	High - 18	Extreme - 22
Minor	Low - 2	Medium - 5	Medium - 9	High - 14	High - 19
Minimal	Low - 1 **RO1,**	Low - 3	Medium - 6	Medium - 10	High - 15

Probability

Probability Descriptions:

Rare	Event not occurred and is not expected to occur <5% chance of occurring
Unlikely	Event could occur but may not have occurred before 5-20% chance of occurring
Possible	There is evidence this event has occurred before 21-50% chance of occurring
Likely	Event has occurred several times, likely to occur again in near future 51-91% chance of occurring
Almost Certain	This event is expected to occur imminently >95% chance of occurring

Consequence Descriptions:

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

Target Risk Rating Calculation:

Low	<80% of risks are GREEN
Medium	50-80% of risks are YELLOW and/or GREEN

High	20-50% of risks are YELLOW, ORANGE and/or RED
Extreme	>20% of risks are allocated as RED
Unknown	Risk table cannot be completed

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
HNZ	Health New Zealand | Te Whatu Ora
Consumer	Health Consumer who is using for personal-related use cases
Health Workforce	A provider of health-related services including those who may provider administrative functions that is not regulated
HISO	Health Information Standards Organisation
Linked Digital Health Services	Linked Digital Health Services are applications or platforms that integrate with My Health Account or My Health Account Workforce. These services rely on verified identity attributes to provide users with access to personal or professional health information, based on user consent and identification level.
User	Refers to healthcare consumers accessing MHA and workforce accessing MHA-W or MHA-U.

Appendix 3: Privacy Statement

Privacy statement

Effective 12 June 2025

My Health Account is a digital health identity service operated by Health New Zealand | Te Whatu Ora. Find out what personal information is collected if you use My Health Account, where it's kept, and who can access it.

My Health Account (with the Unified enhancement) is an updated version of My Health Account, that supports users to add a workforce profile to their consumer account. This Privacy Statement refers to 'My Health Account' as covering all aspects of My Health Account including the workforce aspect in My Health Account Unified.

About My Health Account

At My Health Account, we know how important privacy is to all people in Aotearoa New Zealand. This Privacy statement explains how we collect and use your personal information for a My Health Account ('Account').

It's voluntary for you to sign up for an Account.

My Health Account is designed to make it easy for you to access your health information, and to connect with New Zealand digital health services.

If you are 16 years or older, you can create your own My Health Account.

Some parents aged 16 years and over may also access some information about their child or children aged under 12 years if they use the 'Add a child' feature to establish a relationship between their NHI number and the NHI number of their child or children.

If one parent disputes the right of the other parent to access a child's or children's information, access to the child's or children's information will be immediately suspended for both parties until the matter is resolved.

The information and services you can access and share via your Account are limited by the level at which you have verified your identity.

You can read more about this in our Privacy Impact Assessment(external link) (PIA).

What information is collected

We collect information you provide to us as part of confirming who you are. The information you provide and how you verify your identity sets up an 'Identification Level' for your account. This enables you to connect with digital health services that match your Identification Level. The higher your Account Identification Level, the surer we can be about who you are, and the more services you can access.

Identification Level 1

At Level 1, you only need to provide an email address to sign up. You have very limited access to digital health services at this level because you still need to confirm who you are. At Level 1, My Health Account stores the following information about you:

Your email address

Your preferred name (if provided)

Your mobile phone number (if provided).

Identification Level 2

At Level 2, you have entered your details from one of the eligible identity documents or you have used information held by your general practice (GP) to verify who you are. At Level 2, My Health Account stores the same information as Level 1, plus:

Your first name, middle name/s (if you have them), and last name

Your date of birth

Your HPI number (CPN) if you have added it.

You must use either the identity document check or the healthcare provider check to reach Level 2.

Identification Level 3

At Level 3, we check that it is really you that has created the account and that the right person has been connected to the account. At Level 3, My Health Account stores the same information as for Levels 1 and 2, plus:

Your HPI number (CPN) if you have added it.

To reach Level 3, you must use:

your RealMe® Verified(external link) account, or

the combination of the identity document check and the healthcare provider check.

Identification Level 2N or 3N

Your account will be upgraded from Level 2 to 2N or Level 3 to 3N if you decide to add your NHI number to your account. This allows you to access your health information and digital health services related to your NHI information. At Levels 2N and 3N, My Health Account stores the same information as for Levels 1, 2, and 3 plus:

Your NHI number

Your address, temporarily (if provided)

Your gender, temporarily (if provided). '

Identity document check

When you use the identity document check, we verify your identity document details provided such as your name, date of birth, document number, and other details (depending on the document – for example, your NZ driver licence).

We send the information you give us to our document-checking partners, Cloudcheck from Verifi(external link) or Kiwi Access Card(external link) Verification via CentraPass(external link), for verification that the document matches the details you provide.

Verifi is a New Zealand subsidiary to GBG company that provides Cloudcheck, a service to check records such as passports, driver licences, birth certificates, and other records with the Department of Internal Affairs, Waka Kotahi NZTA, and Australian authorities, on our behalf. We do record when and how you verified your identity, and the type of document you used, but do not retain the unique identifiers associated with those forms of ID.

CentraPass is a New Zealand company that provides a service to verify Kiwi Access Card details with Hospitality New Zealand. As with Cloudcheck, we do record when and how you verified your identity, and that you used your Kiwi Access Card, but do not retain the unique identifiers associated with your card.

Healthcare provider check

When you use the healthcare provider check, we verify your identity using details held by the general practice with which you are enrolled.

If you have not already added your NHI number to your account, we check the details you give us against the NHI database to link those details to a unique NHI number.

We then check the contact details held about you by your general practice with which you are currently enrolled (if you authorise us to do so). We send you a one-

time code challenge to the mobile phone number that your general practice has on their records.

If you have that mobile phone, you will be able to get and input the one-time code into My Health Account. If you do this successfully, the Identification Level of your account will be updated.

Health workforce

Health workforce members can set up a health workforce digital identity account using My Health Account. This allows them to connect with digital health services in their health workforce role when they have a current registration. This includes health practitioners with a Common Person Number (CPN), otherwise known as an HPI Number, or other industry-recognised identifier, if approved by My Health Account for this purpose.

We use your CPN or other approved identifier, together with the name and contact details you have given us to give you access to health workforce-related digital health services, and to record what health workforce-related digital health services you access.

Health NZ has developed a digital health service for health workforce members called My Health Account Workforce.

My Health Account is an updated service that supports Health providers who are not provided a unique email, or are involved in multiple employers, to use their preferred email to add workforce profile(s) into their My Health Account.

As a health workforce member, if you are using your My Health Account to access work-related digital health services, we will not provide your NHI if it is a health workforce-related application, and we will not provide your CPN if it is a health consumer service application.

How we use your information

Your My Health Account information is used to:

respond to your requests and inquiries made through or about your Account

protect against and identify fraud and other criminal activity. **Note:** it is an offence under section 212(2)(c) of the Privacy Act 2020 to falsely pretend to be an individual or falsely claim to be acting under their authority to obtain access to that individual's personal information

comply with and enforce applicable legal requirements, relevant standards, and our policies, including this Privacy statement

enable us to prepare reports of statistical information about how services are used (you will not be identified in the reports produced) so that we can monitor and improve the performance of My Health Account and monitor interactions with participating third-party applications and services using My Health Account.

The Account allows you to connect with and use participating third-party apps and services:

You need to review relevant information from those other services before you sign up to them, and grant permissions to sharing your information with those other services at the time you first access the services.

We disclose to those participating apps and services your documented identity attributes, such as your first name, middle name, preferred name (if one is provided), last name, date of birth, email address, mobile phone number, NHI number, HPI number (CPN), related family member NHI numbers (if applicable), and identification level associated with your account.

Attributes will only be shared with digital health services as necessary for that service. If the details are not necessary for operation of the application, they will not be supplied.

The list of which attributes digital health services can receive is agreed upon and configured during the application onboarding process. My Health Account will ask you to grant permissions when first accessing the service and those permissions will be displayed to you as part of the Account services.

You can also choose to stop sharing your information within your My Health Account to an application if you have previously given permission. They may retain any information supplied about you while the permission was granted but will not be able to access your Account information in future.

Some services that require My Health Account verification apply age restrictions. If your date of birth is outside the permitted age range, you will be refused access to those services.

Some services may require relationships to be asserted, and confirmed for you to access those services. If you do not provide those details, you may be refused services relevant to those requirements.

Visit our Connected digital health services page(external link) on our website for details of how these services use Consumer information.

Your email address

To help keep your Account secure, we may email you a verification code to use when you log in. This can also be used to help maintain your Account, for example, when you change your password. The email address must be one that is unique to you, and that you have control over, and cannot be already linked to another Account. We will use this email address to contact you and may email you with updates to the My Health Account Privacy statement, and services and applications that you can access via My Health Account.

Your mobile number

We can communicate with you via SMS (text message), rather than email, for 'One-Time Passwords' (OTPs). We will verify your mobile number with you before we send a text message. Your mobile phone number details held within My Health Account may be shared with digital health services that are authorised and linked to the My Health Account service. These digital health services may display your stored mobile phone number from My Health Account to allow you to give permission for that digital health service to communicate with you via text message.

How we protect your privacy

We take your privacy seriously.

We have discussed the My Health Account service with the Office of the Privacy Commissioner(external link) and the Government Chief Privacy Officer(external link). We continue to take their advice as we develop the service further.

A Privacy Impact Assessment [PDF, 783 KB] (PIA) has been completed. The PIA is updated to reflect new My Health Account features and functionality as they become available.

How we secure your information

Your personal information is held and managed in accordance with the Privacy Act and Health Information Privacy Code(external link).

Information you share with Te Whatu Ora – Health New Zealand may be shared with other Government agencies with your permission or as authorised by law. This may happen:

if you have authorised this sharing

if we think it is necessary for your care and treatment

If there is an incident we need to investigate, or a technology issue

for your safety or the safety of others, or

if authorised by law.

We may provide information to other government agencies where the account is used by both agencies, such as ACC ProviderHub. In these instances, we would share information to authenticate your account, identify you, help you access your account or to troubleshoot any account issues identified by us or the agency using the account. We may also provide your information to the Ministry of Health and other government agencies that require us to provide information for administrative, legal, contractual, statistical, research or public health purposes.

Information you choose to share with us will be held securely in compliance with Health NZ standards. Security measures are in place to protect your information from unauthorised access.

We use Microsoft Azure Services in Australia to deliver the Service. Use of other third-party services is detailed in the current Privacy Impact Assessment [PDF, 783 KB](PIA).

We use Google reCAPTCHA v3 as a security measure to defend My Health Account against bots. reCAPTCHA collects information such as IP address, hardware and software information, and device and application data. This information is only used to provide, maintain, and improve reCAPTCHA and for general security purposes.

How long we keep your information

Once a My Health Account is created, the following information is retained: Applicant name, date of birth, preferred name, email, mobile phone number, and supplied and verified NHI number or HPI number (CPN). Related child NHI numbers are also retained until the relationship is removed (not when the My Health Account that established the relationship is deleted). These details are supplied to authorised services connecting to the My Health Account service as identified in the PIA for each of those services (and as approved by the My Health Account service).

You can ask for your account to be closed by calling the Contact Centre on 0800 222 478 or +64 9 307 6155. Once closed, your account is not able to be used for any further activities and all details, other than those required for audit activity, will be deleted. The email associated with the account, the Identification Level obtained, and the related dates and the NHI number and / or CPN (if added) are retained.

Tips to keep your My Health Account secure

Do not share your account details with other people.

Keep your password safe.

We recommend using a screen lock on your device.

If you believe your password may have been compromised, please change it. If you believe your account has been compromised, please call the Contact Centre on 0800 222 478 or +64 9 307 6155 as soon as you can.

Viewing or changing your information

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

The Privacy Officer
Health New Zealand | Te Whatu Ora
PO Box 793
Wellington 6140
Email: hnzprivacy@health.govt.nz

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

When you contact us for help, your communications, including any information you provide regarding your identity and the matter you're contacting us about, are collected.

Giving feedback

Feedback is important and is used to evaluate and improve My Health Account. If you provide feedback by email, that feedback is sent to the appropriate Health NZ staff. This could include your email address and other identifying information that you have provided.

Phone: 0800 222 478 or +64 9 307 6155 during standard office hours, 8 am to 5 pm Monday to Friday

Email: support@identity.health.nz

Statistical information

We may collect statistical information to help us improve the Service and understand how it is being used. In summary, this includes the event type and session, timestamps, and the type of device being used. This information is aggregated and doesn't identify you personally. Full details about the statistical information collected is addressed in our Privacy Impact Assessment [PDF, 783 KB].

Your My Health Account details (including NHI number, and related attributes of age, address (suburb, town, and postcode and relevant Health New Zealand district), ethnicity, gender, New Zealand citizenship / residency status) may be used for statistical reporting on the performance of My Health Account to enable performance monitoring and service improvement. It may also include interactions with integrating applications, such as My Health Record, to identify usage statistics. Your personal information will remain securely contained in our systems and only aggregated information (without your name details, NHI number, or contact details) will be used in reports created, to preserve individual privacy for reporting purposes.

My Health Account uses temporary session cookies. The session cookies are limited to the lifetime of the session and provide support for features such as single sign-on (SSO), as well as enhancing the user experience within the My Health Account self-service portal. My Health Account does not use third-party or "tracking" cookies.

If you have a privacy concern

Please contact us by email: hnzprivacy@health.govt.nz.

If you are not satisfied with the response to any privacy concern, you can contact the Office of the Privacy Commissioner(external link).

Updates to this privacy statement

This Privacy statement may be updated to let you know about changes in how we collect and process your information in the Services or changes in related laws. The date when the document was last updated is shown at the top of this Privacy statement.

My Health Account

Privacy Impact Assessment

Date: 4 April 2024

Te Whatu Ora
Health New Zealand

Document Approval

	Name/Title	Sign-off date
Approved by Senior Responsible Officer	Samuel Wong	
Approved by Chief Privacy Officer, Te Whatu Ora	Viv Kerr	

The author of this document is the Data & Digital Directorate, Te Whatu Ora – Health New Zealand.

Disclaimer

Every effort has been made to ensure that the information contained in this report is reliable and up-to-date. This Privacy Impact Assessment (PIA) represents the current expectations of the way My Health Account services will operate.

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

Contents

SECTION ONE – EXECUTIVE SUMMARY 76

SCOPE OF ASSESSMENT 77
ASSESSMENT CONTENT 77
RECOMMENDATION SUMMARY 77

SECTION TWO – MY HEALTH ACCOUNT 80

BACKGROUND 80
MY HEALTH ACCOUNT 80
INFORMATION FLOWS INVOLVED IN MY HEALTH ACCOUNT PROCESSES: 82
INFORMATION COLLECTED 83
SIGN-UP 83
IDENTITY DOCUMENT CHECK 83
HEALTHCARE PROVIDER CHECK 83
REALME® VERIFIED 84
ADDING NHI NUMBER 84
ADDING HPI NUMBER (CPN) 85
PARENT-TO-CHILD / CHILDREN RELATIONSHIPS 86
OTHER PERSONAL INFORMATION 87
COOKIES 87
STATISTICAL INFORMATION 87
AUDITING 87
INFORMATION STORAGE 87
INFORMATION UPDATES / CORRECTION 88
INFORMATION USE AND SHARING 88
ONBOARDING DIGITAL HEALTH SERVICES 88
CONSENT AND SHARING ATTRIBUTES 89
ANALYTICS AND REPORTING 89
INFORMATION DISPOSAL 90
PROCESS FOR MANAGING INFORMATION COMPROMISE 90
GOVERNANCE 91

SECTION THREE – PRIVACY ANALYSIS 92

APPENDIX ONE – IDENTIFICATION LEVELS 98

APPENDIX TWO – RETENTION OF PERSONAL INFORMATION 99

APPENDIX THREE – MY HEALTH ACCOUNT PRIVACY STATEMENT 101

APPENDIX FOUR – CONSUMER TERMS OF USE 108

APPENDIX FIVE – ATTRIBUTES THAT CAN BE REQUESTED BY DIGITAL HEALTH SERVICES VIA MY HEALTH ACCOUNT 111

GLOSSARY 112

Section One – Executive Summary

8. My Health Account is the digital health identity service originally developed by the Ministry of Health (the Ministry).
   8.1. Post 1 July 2022 My Health Account was transferred to and is now operated by Te Whatu Ora – Health New Zealand[11].

9. Te Whatu Ora aims to enhance users' access to their health information via digital channels. My Health Account intends to be a trusted digital health identity service that helps individuals have greater access to information about their own health.

10. To allow users to access these digital health services, Te Whatu Ora first needs to accurately identify the users. My Health Account enables health consumers and health professionals to confirm who they are digitally and engage with online healthcare services.

    10.1. The initial use case for My Health Account means users can view and confirm their COVID-19 vaccination status and test results with My Covid Record.

    10.2. It now integrates with several approved Digital Health Services (those current at the date of issue of this PIA are listed on the My Health Account website).

11. Each digital health service must complete a PIA and meet the requirements of My Health Account's identification level framework before being allowed to use the My Health Account service.

12. Te Whatu Ora carefully balances these potential privacy risks against the public health benefits of letting Users access their health records using My Health Account. User trust is essential to achieve widespread use of My Health Account. Te Whatu Ora is working hard to earn and retain high levels of public trust.

    12.1. Te Whatu Ora intends to retain Consumer choice, collecting only the essential personal information required to uniquely identify users online, and limit who will have access to that information.

    12.2. Information about users who choose to use My Health Account Services is stored by Te Whatu Ora and will not be shared with any other agencies (Government or otherwise) unless explicit Consumer consent is obtained, or it is authorised by law. Use of information by Service Providers will either be authorised by users or under legal authority (such as in compliance with the rules in the Health Information Privacy Code 2020 and other enactments that require or allow information to be used or disclosed).

    12.3. Users are asked for their permission before their information is shared via My Health Account with connected digital health services. Users can view a list of all digital health services they have previously given permission to access their

[11] Te Whatu Ora - Health New Zealand is a Crown agent within the meaning of section 10(1) of the Crown Entities Act 2004 and is established under the Pae Ora (Healthy Futures) Act 2021.

information. Users can remove these permissions at any time via My Health Account.

13. The Office of the Privacy Commissioner and the Government Chief Privacy Officer were consulted and provided comments on a draft Privacy Impact Assessment. The comments were considered by the Ministry and Te Whatu Ora, then included as Te Whatu Ora saw appropriate.

14. This Privacy Impact Assessment (PIA) is a 'living' document that will be reviewed as My Health Account continues to develop. Te Whatu Ora releases new functionality in My Health Account Services in phases. As new features are developed and released, the privacy impacts are reviewed and reassessed.

Scope of Assessment

15. The current Assessment covers:

    15.1. The personal, demographic, and anonymous[12] information to be collected from the Consumer to create a My Health Account.

    15.2. My Health Account's identity confirmation role for connected digital health services or applications.

16. This Assessment does not address:

    16.1. any further digital health services or applications My Health Account may be able to interact with in future, as each of these will be addressed in subsequent service-specific Privacy Impact Assessment activity and must meet the identification level requirements set by My Health Account.

    16.2. the decision-making process, approvals, nor the conclusions reached about the decision to create My Health Account services.

Assessment content

17. Section Two contains the Description of the Service and Information Flows.

18. Section Three contains the Privacy Analysis.

Recommendation Summary

19. My Health Account is a digital health identity service, enabling individuals to opt in to have access to, and some control over, their personal health information as users. Individual users can choose the identification level they wish to apply to their account.

    19.1. My Health Account is a 'doorway' to approved digital health services and applications. Te Whatu Ora carefully oversees how My Health Account

[12] Users can choose their level of engagement with the system. At the lowest Identification Level (Level 1), users can provide pseudonymous information such as phone number, email address and "names" without this information being verified with official sources. Users who choose a low Identification Level will not have access to sensitive information (e.g. medical records) until they successfully provide further evidence of identity.

controls are managed within other services (via its onboarding process) and how Consumer control can be retained from within their My Health Account.

19.2. There is a danger of function creep if other services, access, or authorities are enabled that are not directly subject to easily-manageable Consumer control within My Health Account. Only limited exceptions will be permitted by Te Whatu Ora under narrow use cases (e.g. services required to be provide to certain groups with ambiguous legal status).

19.3. Privacy risks associated with My Health Account are successfully managed by Consumer-applied controls, security measures, and strong governance oversight.

20. Te Whatu Ora will work to ensure it obtains, and then maintains, Consumer trust in its operation of My Health Account and related services.

Recommendations:

21. The following recommendations apply to any future changes to My Health Account (or any significant changes arising from associated digital health services):

	My Health Account – Privacy Impact Assessment (PIA)	Planned Date for completion
PIA-01	Complete any Te Whatu Ora security assessment requirements including Certification and Authorisation, and independent security testing. This has occurred prior to each release to date. If any risks are identified, they will be resolved or mitigated to ensure appropriate security is applied to all aspects of the service. It is important that security measures are applied across the end-to-end services available via My Health Account to maintain trust in the service, as it is a gateway to those other services. Users can reasonably expect that Te Whatu Ora will maintain oversight of all interconnected services (via the onboarding process), and not offer them unless security is assured. These matters, however, will be potentially outside the direct control of My Health Account so communications and oversight must remain strong with other interconnected projects, such as Hira and My Health Records.	Ongoing - Prior to go-live of any new feature release of substance
PIA-02	Clear Privacy Statement Materials are developed and made available via My Health Account. The current version is attached in Appendix Three. This Statement includes reference to connected digital health services permitted to integrate with My Health Account and includes full service details on a separate My Health Account web page (linked from the Privacy statement to prevent the length of the Privacy statement becoming unwieldy). Te Whatu Ora is planning to modernise providing future updates to Privacy statement materials – whether by banner notification within the My Health Account application or by direct email to all email addresses verified by My Health Account processes.	To be finalised in each case prior to any go-live of a new release (each updated Privacy Statement to change the Effective Date recorded at the top of the Privacy statement on the website)
PIA- 03	The Onboarding process will be reviewed to ensure that the applications will operate at an identification level appropriate with My Health Account settings.	To be finalised prior to go-live in each case of

	Any connected digital health services must also incorporate a relevant Privacy statement for those services as part of the Consumer onboarding processes.	additional services
PIA-04	Service Providers permitted to interact with My Health Account must also be bound to appropriate Terms of use that confirm the permitted purposes for use of any information accessed, to ensure Service Providers are clear about expectations for use, and limitations on use of this personal information.	Prior to service providers being permitted to interact with My Health Account
PIA-05	As Hira develops, and access to more detailed identifiable records potentially become available through My Health Records and other connected services, then My Health Account and Hira processes will need to be carefully considered in relation to the accounts of the 12 to 15-year-olds who may initially have had parental assistance to set up their accounts. Te Whatu Ora will need to develop a process and safeguards to ensure if / when parents assist a child to create an account (and hold credentials to access the child's account) that there is regular review, and the subsequent opportunity for the children (particularly as they age) to control access to their own information.	Policy work is underway with an intended completion by June 2024 – prior to any expanded access to clinical records being made available
PIA-06	Strong governance is required to ensure that My Health Account and any connecting digital health services remain consistent with the My Health Account expectations set out in this Privacy Impact Assessment. The transition to Te Whatu Ora was monitored to ensure that the governance options available under the Ministry of Health were either transitioned or replaced with appropriate bodies to ensure continuity of governance.	Ongoing governance oversight
PIA-07	A particular feature to be monitored is the 'Add a child' feature, which enables some parents to establish a relationship between their NHI number and the NHI number of their child or children. Access to the child's address and other contact details by either parent must be limited or excluded through design and onboarding controls. It is a recognised risk in a family violence situation that disclosure of address or contact details may enable one parent to locate the other, without the consent of that other parent.	To be finalised prior to go-live in each case of additional services

Section Two – My Health Account

Background

My Health Account is a digital health identity service that enables users of New Zealand health-related services (both health consumers and health workforce members[13]) to create a trusted digital health identity, so that they can interact with the health information they are allowed to access.

Use of My Health Account is voluntary. People must opt in to use it and can determine what Identification Level they wish to achieve based on the Services they want to access. While the service is voluntary, most services will require the highest identification level to be maintained to ensure legal authorisation for accessing said digital services.

Users can assert that Identification Level to Digital Health Services that require an identification level to use them. Depending on the type of identity proof that the Consumer provides, My Health Account sets an Identification Level (guided by the Identification Management Standards 2020). Service Providers can use the Identification Level to ensure that private information is only released to users who meet their identity requirements.

My Health Account has developed a process so that people can make choices on an ongoing basis to connect to the Digital Health Services they wish. Users can also choose when to revoke that consent for those Services.

My Health Account will be transparent with the use of the data, to maintain and grow social licence. My Health Account always follows these principles:

- The information collected will be voluntarily provided by the Consumer.
- Information collected is always secured and only shared with those who need to know.
- Only the minimum information that is needed is collected.
- Information used temporarily (e.g. only for identity verification) is deleted once the purpose has been completed.
- The Consumer can grant or deny permission to share their My Health Account information with participating digital health services.

Health services will continue to be provided regardless of whether a person has a My Health Account. There are also customer support services available for those unwilling or unable to use My Health Account services.

My Health Account

The screen flows for My Health Account have been designed to be relatively self-explanatory for users when creating a My Health Account. My Health Account can be accessed from https://identity.health.nz.

[13] Noting that the health workforce facility will be removed in the near future when the new My Health Account Workforce is released.

The approach Te Whatu Ora has taken is to balance the need to make My Health Account as easy as possible for users to sign up and provide their information, against the need for appropriate security and assurance levels.

Users can sign up directly from the My Health Account website, but most accounts are created when an application or Service the Consumer wishes to use, such as My Covid Record, refers them to My Health Account to establish their identity and Identification Level.

Before signing up to My Health Account, users are provided links to the Privacy statement[14] and Consumer Terms of use[15]. Te Whatu Ora has produced standardised Privacy Statement Materials that are compliant with Rule 3 of the Health Information Privacy Code. The current version of the Privacy statement is in Appendix Three. The website also provides access to advice and guidance[16].

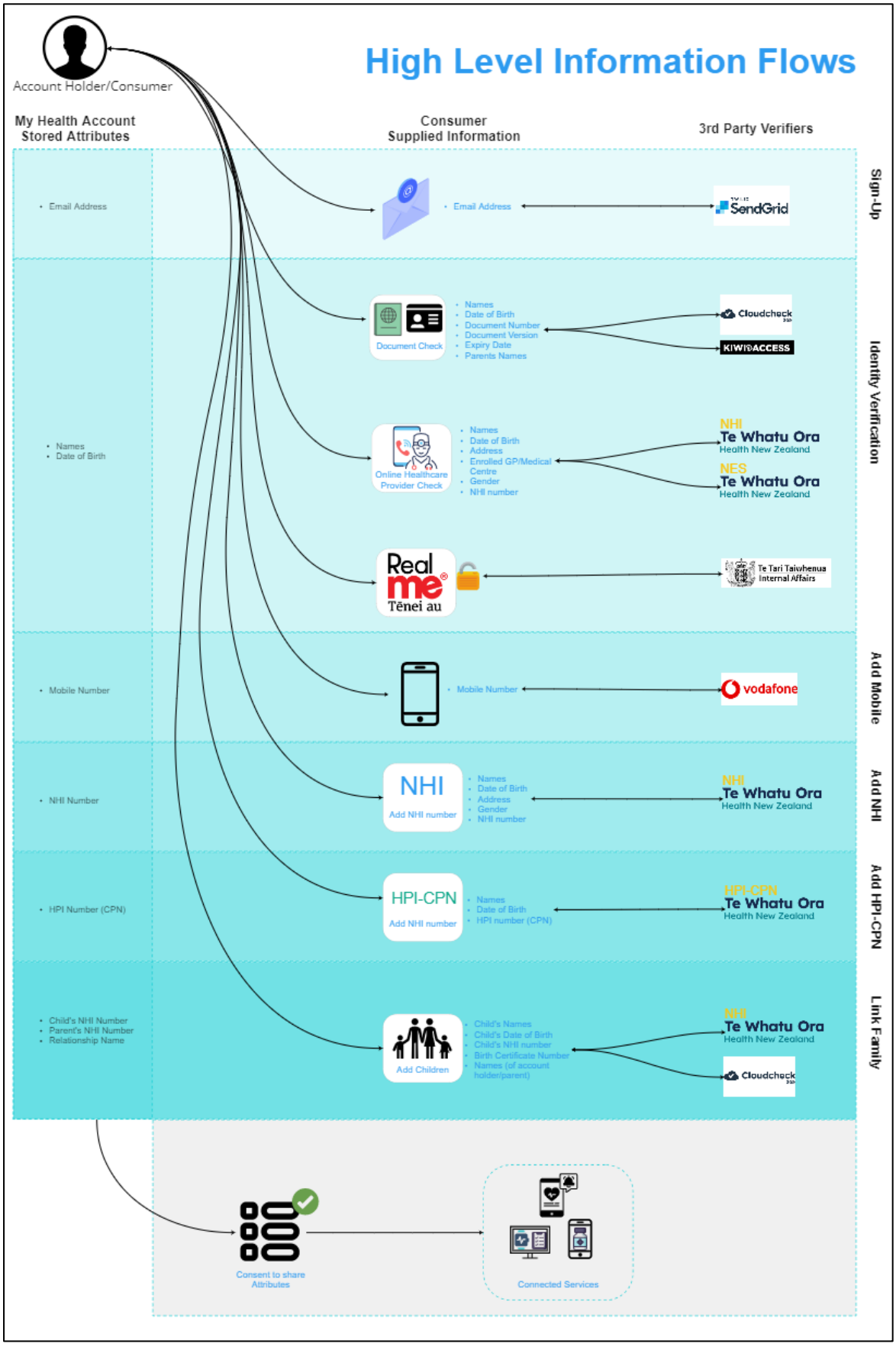
Before users can use My Health Account, their identity must be verified. This verification process involves several steps, and the 'Identification Level' achieved reflects the increasing assurance that can be placed on each step. The Consumer can stop progressing through the identity verification steps when they want to, but they will not be able to access Digital Health Services via My Health Account if they do not meet the Identification Level required for access to the Digital Health Service in question. An identification level summary is set out in Appendix One.

[14] https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/privacy-statement

[15] https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/terms-of-use

[16] Advice on creating your My Health Account: https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/creating-your-account and advice on how to get the most from your account: https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/getting-the-most-from-your-account

Information flows involved in My Health Account Processes:



Information Collected

Sign-up

Users can sign up to My Health Account by either providing an email address and password, or via an existing RealMe® or RealMe® Verified account. All users of My Health Account are required to provide a unique email address as part of their sign-up process. For those users who have signed up using an email address and password, the email address is used both to log in and for communications about the My Health Account service. For those users who have signed up using RealMe or RealMe Verified, the email address is used only for communications about the My Health Account service.

All email addresses are validated via a third-party service (SendGrid) by sending a Time-limited One Time Passcode (TOTP) to the supplied email address. Users have 20 minutes to enter the TOTP into My Health Account to validate that they have access to the email account.

Identity Document Check

Users can claim identity information in My Health Account by verifying an official document, such as a Passport or Driver Licence[17]. Users are required to provide information as recorded on the selected document type, including name, date of birth, document/card number and, depending on the type of document used, other details such as expiry date or document version.

The Consumer-supplied information is checked against the source records (e.g. those held by DIA or Waka Kotahi) via third-party services[18] to ensure that there is a record of an official document that matches the details provided[19]. This check meets the requirements of Information Assurance according to the Identification Management Standards 2020.

My Health Account retains the Consumer-supplied name and date of birth. A 'verification' details record is also kept – i.e. verification method used, verification result (valid or invalid), and the date and time of verification. The verification details are used solely for audit purposes in the event there is an apparent misuse of the verification service (e.g. in the case a person seeks to misrepresent the identity of another Consumer). It will only be accessible to select, authorised individuals from Te Whatu Ora (or their agents) if they are required to investigate a possible breach of the Consumer Terms of use or fraud. This role will be limited, and all access tracked.

Healthcare Provider Check

Users can choose to verify their identity using information already held about them in Te Whatu Ora records. Users are required to provide information about themselves including their name, date of birth, address and the General Practice or Medical Centre with which they are currently enrolled. They also have the option to provide their gender and NHI number.

[17] The identity documents that can be used for verification are listed on the Te Whatu Ora My Health Account website.

[18] Third-party services are Cloudcheck from Verifi and a Kiwi Access Card verification service from CentraPass.

[19] Information about how third-party services retain and manage data in accordance with the Privacy Act can be found here: https://www.verifidentity.com/legal/#privacy and https://kiwiaccess.co.nz/privacy-statement/.

The Consumer-supplied information is used to find and validate the user's NHI number and their patient record in the National Enrolment Service (NES)[20]. If a matching patient record is identified for the Consumer, and if the patient record includes a Mobile phone number, the Consumer can request that My Health Account send a Time-limited One Time Passcode (TOTP) to that Mobile number via SMS. The Consumer is shown the last four digits of the phone number on the My Health Account screen (with the other details obscured) so that they can determine if they still have access to the phone with that number.

The Consumer must correctly input the code into My Health Account within a 20-minute period, before it expires. If the Consumer can successfully complete the TOTP challenge before it expires, it is considered a strong and direct link to the person who owns the NHI and is enrolled with the specified General Practice.

My Health Account retains the Consumer-supplied name and date of birth (where not already stored) along with verification details in line with what is described under the Identity Document Check above.

RealMe® Verified

Users who have signed up via a RealMe[21] account with a 'Verified' status can choose to allow RealMe to share their 'Verified' information with My Health Account.

If a Consumer consents for RealMe to provide their verified attributes, then RealMe shares information including name, date of birth, gender, and address. This information, along with a Consumer-provided unique email address, will be used to create a My Health Account with a strengthened assurance that the person claiming the identity attributes is the owner of the identity. This gives them an account with an Identification Level of 3.

My Health Account retains the name and date of birth along with verification details in line with what is described under the Identity Document Check above.

Adding NHI Number

Users who have completed an identity verification process up to Identification Level 2 or 3, can choose to add their National Health Index (NHI) number to their account. The NHI number is a unique identifier that links an individual to their personal health information recorded in the National Health Index (NHI). This will allow them to share the number as an attribute with connected Digital Health Services, making it easier for them to be linked to their personal health information and records.

My Health Account will use the verified information (names and date of birth) stored against the Consumer's record to search for a matching NHI record. Matching NHI records are scored on uniqueness, based on a matching algorithm. If the record is not deemed to be a unique match, the Consumer is asked to provide more information. The Consumer can choose to provide their NHI number (if known), their gender and/or their address. My Health Account then re-attempts to find a uniquely-matching NHI record.

---

[20] The NES holds the registered details of the GP, or general practice, that each person is enrolled with, and the contact details of each of those enrolled individuals.

[21] RealMe® is a government authentication and identity verification service that can be used to log in to many New Zealand government and public sector sites and services. It is also a secure way to prove who you are when you're online. For more information, see: https://www.realme.govt.nz/.

If a uniquely-matching NHI record is identified, the NHI number for the active NHI record[22] is stored against the Consumer's My Health Account record.

If a uniquely-matching NHI record cannot be identified, or more than one matching NHI record is found, then the record is sent to the Te Whatu Ora NHI-matching team who will review the provided information and other Te Whatu Ora datasets to determine the correct NHI record to link to the My Health Account record. If no existing NHI record is identified, the NHI-matching team may create a new NHI record to be linked to the Consumer's My Health Account record.

If the Consumer has provided a gender and/or address as part of the matching process, this information is deleted from their record as soon as a successful NHI match has been completed.

An NHI number can only be linked to a single My Health Account record.

Adding HPI number (CPN)

In April 2023, Te Whatu Ora released My Health Account Workforce – a digital health identity service for Aotearoa New Zealand's health workforce. The service allows health workforce members to create a trusted digital health identity so that they can interact with the work-related and health information that is necessary for them to perform their work role.

Prior to the release of My Health Account Workforce, registered health practitioners who had completed an identity verification process up to Identification Level 2 or 3, could choose to add their Health Provider Index (HPI) – Common Person Number (CPN) to their My Health Account. The HPI number (CPN) is a unique identifier that is issued to certain health practitioners and links the practitioner to their record in the Health Provider Index (HPI). This allowed them to share the number as an attribute with work-related Digital Health Services, making it easier for them to be linked to their health workforce information.

My Health Account will use the verified information (names and date of birth) stored against the Consumer's record to search for a matching HPI record. Users must provide the HPI number (CPN) but can edit the name information that is used in the search, in case the name on their Annual Practising Certificate is different to the name used on their identity document.

If a uniquely-matching HPI record is identified, the HPI number (CPN) for the HPI record is stored against the Consumer's My Health Account record.

If a uniquely-matching HPI record cannot be identified, the Consumer is provided with advice on how they can try again.

If the Consumer has provided a different name as part of the matching process, this information is not stored against their My Health Account record.

An HPI number (CPN) can only be linked to a single My Health Account record.

Now that Te Whatu Ora has developed My Health Account Workforce, Health Workforce members who are currently using My Health Account for work-related purposes will be supported to transition across to the new Workforce account as Workforce Digital Health Services migrate.

For Health Workforce members still using their My Health Account to access work-related digital health services, My Health Account does not provide their NHI if it is a health workforce-

[22] Under some circumstances, an individual may have multiple NHI records, however only one of these should be 'Active' at any one time, with the duplicate records marked as 'Dormant'.

related application and does not provide their HPI number (CPN) if it is a health consumer service application.

Parent-to-child / children relationships

Some parents can choose to establish a relationship with their child or children so that they can share in their child's or children's health and wellbeing outcomes by accessing their health information online. The current 'Add a child' feature only allows for parent-to-child / children relationships for children up to 12 years of age.

Parents wishing to establish a relationship with their child or children within My Health Account can enter information about their child, including the child's name, date of birth, and NHI number. Additional information, including the birth certificate number, is also required.

The Identification Level of the parent must be Level 3N (i.e. the most secure level, with the parent's NHI number added to the account) before they can establish a relationship with their child within My Health Account.

The Consumer-supplied information about the child is validated against the child's NHI. The Consumer-supplied information and the parent's name (as recorded against their My Health Account record) is checked against the DIA's birth registry (i.e. the child's birth certificate details), via a third-party service (Cloudcheck). If there is no match, a relationship is not established between the child and the 'parent' making the claim.

My Health Account will not store any address information related to the child nor will we make any address information for the child available via the 'Add a child' feature. This will ensure that no confidential information, such as a physical address, is surfaced through the 'Add a child' feature. It is understood that contact details of this type could, in some cases of family violence, risk compromising the privacy, safety, or security of either of the parents or child / children where a parent-to-child relationship is established through this feature. Any Digital Health Services that connect to this feature must also withhold any address or other contact details relating to the child.

If verification is successful, then the parent can choose to provide a nickname for the child or relationship. My Health Account will record the Parent's NHI number, the Child's NHI number, the child's / relationship nickname, the relationship type, and an expiry date (based on when the child will turn 12), along with verification details in line with what is described under the Identity Document Check above.

When a second parent establishes a relationship to the same child via their My Health Account, the original parent is notified by email that the other parent on the birth certificate has claimed a relationship with the same child. Within their My Health Account profile, both parents will see the first name of the other parent flagged to show them that the other parent has established a relationship with their child.

If one parent disputes the right of the other parent to access a child's or children's information, access to the child's or children's information will be immediately suspended for both parties until the matter is resolved. The information is provided on the basis that Rule 11(5) of the Health Information Privacy Code permits a parent to request health information about their child – based on section 22F of the Health Act. If one parent has been legally excluded from accessing such information about their child then evidence could be produced, and the excluded relationship removed from that parent's My Health Account. In the interim, the parties will be able to obtain information about the dependent child using existing channels with any relevant healthcare provider.

If parents have any questions about the ‘Add a child’ feature, they can contact the My Health Account Customer Support team on 0800 222 478 or +64 9 307 6155 during standard office hours, 8 am to 5 pm Monday to Friday or send an email to support@identity.health.nz.

Other Personal Information

Preferred Name

Users can choose to provide a ‘Preferred Name’ for their My Health Account. There is no verification on the preferred name value as it is Consumer-defined and is used to allow a Consumer to inform Digital Health Services they access the name by which they prefer to be known.

Mobile Number

Users can choose to add a Mobile number to their My Health Account. Users can choose for the Mobile number to be used as a second-factor authenticator (i.e. in cases where a higher level of authentication is required, users will receive a Time-limited One Time Passcode (TOTP) challenge via SMS rather than email). In addition, if the number is shared with Digital Health Services, the mobile number may be used for communication purposes (which will need to be addressed within the Digital Health Service’s Privacy statement).

All mobile numbers are validated via a third-party service (Vodafone) by sending a Time-limited One Time Passcode (TOTP) to the supplied mobile phone number. Users have 20 minutes to enter the TOTP into My Health Account to validate that they have access to the mobile phone.

Cookies

My Health Account uses temporary session cookies. The session cookies are limited to the lifetime of the session and provide support for features such as single sign-on (SSO), as well as enhancing the user experience within the My Health Account self-service portal.

My Health Account does not use third-party or ‘tracking’ cookies.

Statistical Information

Te Whatu Ora collects statistical information to help improve the Service and understand how it is being used. This will apply to both user interactions and digital platform performance across all services associated or connected with My Health Account. This includes the event type and session, timestamps, the type of device and browser being used, and the Digital Health Services being accessed. This information is aggregated and doesn't identify the Consumer personally.

Auditing

My Health Account records all activity against all Consumer accounts. System access to audit records is strictly controlled and limited to Te Whatu Ora staff who are responsible for maintaining security standards and resolving customer support queries.

Audit records will be held for a minimum period of five years.

Information Storage

Te Whatu Ora uses Microsoft’s Azure cloud services as the underlying technology platform for My Health Account. As a cloud-based solution, all Consumer information is securely held and managed within Microsoft data centres located in Australia.

The My Health Account system is designed according to strict security principles and practices. The system architecture provides multiple layers of defence, and all Consumer information is encrypted, both at rest and in transit. Moreover, Consumer access to their information within the system is tightly controlled, with all access being both logged and audited.

My Health Account data is held by Te Whatu Ora in two places - namely, the identity and analytical data stores.

The main identity store is where the system uses Consumer data for providing account services, such as enabling users to use their account to log in to verified healthcare applications.

The analytical store (or data warehouse) holds an aggregated view of My Health Account information. Te Whatu Ora uses this store for decision-making. The insights the information provides assist in the planning of new features and functionality.

Data maintained in the analytical store is protected by the same security controls as the main My Health Account system, with full encryption of all information and rigorous access controls.

In addition to secure data storage, the My Health Account system is also designed to be highly available, thereby allowing users to access their My Health Account whenever they need it.

Information Updates / Correction

Users can update or correct some information about themselves directly via the My Health Account self-service pages. The information that a Consumer can update themselves includes:

- Preferred name: (Update or Remove)
- Mobile number: (Update)
- Email address: (Update)
- Linked Child or Children NHI numbers: (Remove the relationship between the parent's and child's NHI numbers)
- Password (Update)

Users can request that other information about them is updated by contacting My Health Account customer services. In addition to the above, the information that a Consumer can request to update is:

- NHI number: (Update or Remove)
- HPI number (CPN): (Remove)
- Linked Child or Children NHI numbers: (Suspend the relationship between the parent's and child's NHI numbers)

Information Use and Sharing

Onboarding Digital Health Services

The purpose of My Health Account is to allow users to create a trusted health identity, which they can use to securely access Digital Health Services that link them with the health information they are authorised to access. Before a Digital Health Service is made available to users via My Health Account, it must pass various testing and compliance requirements. This includes ensuring that the Digital Health Service is:

- restricting access to only those users who meet the agreed criteria (e.g. Identification Level and Consumer's age)

- compliant with the Privacy Act 2020 and Health Information Privacy Code 2020 (which includes only requesting attributes for which it has a valid business need)
- ensuring that no confidential information, such as a physical address, is surfaced through the 'Add a child' feature that may compromise the privacy, safety, or security of either of the parents or child / children when a relationship is established between a parent and child through this feature
- meeting security assurance requirements.

The Te Whatu Ora website lists the connected Digital Health Services currently available to users via My Health Account.

Consent and Sharing Attributes

Once made available, users must choose to interact with a Digital Health Service before any information about the Consumer is shared with it. Users are provided with an attribute list to approve for sharing when logging in to the Digital Health Service and one of the below criteria is met:

- the Consumer is accessing the Digital Health Service for the first time
- the Consumer has previously revoked permission to share attributes with the Digital Health Service
- the Consumer has added a new attribute to their account that the Digital Health Service has requested
- the Digital Health Service has requested an attribute that has not previously been shared
- the Digital Health Service has indicated they intend to use the Consumer's My Health Account information in a different way.

If the Consumer chooses not to share the attributes with the Digital Health Service, then they are not logged in to the Digital Health Service and no information about the Consumer is shared with the Digital Health Service.

If the Consumer chooses to share the attributes with the Digital Health Service, then the information is passed to the Digital Health Service each time the Consumer successfully logs in to the Digital Health Service (until they revoke the permission to share the attributes).

Users can review and revoke the existing permissions at any time via the My Health Account self-service profile page under 'Connected Services'.

The actual attributes shared with a Digital Health Service are dependent on what the Digital Health Service has requested and what attributes the Consumer has on their account, however the full list of possible attributes are detailed in Appendix Five.

Analytics and Reporting

Statistical information is used in analytical reporting to understand when and how users are using My Health Account so that we can monitor and improve the performance and capabilities of My Health Account. Any analytical reports use aggregated data and cannot be used to identify users personally.

My Health Account data may be combined with other demographic and health utilisation data linked to the NHI (including age, district, ethnicity, and gender) in order to understand parts of the community where access to digital health information can be improved. Any reports use aggregated data and cannot be used to identify users personally.

Personal information will remain securely contained in Te Whatu Ora systems and only aggregated information (without names, NHI number, or other personal information) will be used in created reports, to preserve individual privacy.

Information Disposal

If a person asks for their My Health Account to be closed, access to the account will be removed and all access inactivated, other than the information required for audit purposes in compliance to the Public Records Act. Information to be retained includes the email used to establish the account, the Identification Level (and related dates it was obtained), and any linked NHI or health identifier number. Information collected into Te Whatu Ora's data warehouse will be retained for analytics' purposes only. The account would not be able to be used to validate further activities in future.

My Health Account administrators may initiate the removal of a HPI number (CPN) from a My Health Account after the transition period to My Health Account Workforce is over and following subsequent attempts to support health practitioners to migrate their account to My Health Account Workforce.

Upon notification of the death of an account holder, their account in inactivated for a period of two years prior to closure. During that time, only authorised representatives may be able to access inactivated accounts, as strictly required for the purposes to settle any affairs of the deceased individual.

Note: Parent-to-child relationships are not automatically deleted when the My Health Account that established them is deleted, since the relationship is between the NHI numbers rather than tied to the My Health Account. Users can remove the relationships themselves within My Health Account before their My Health Account is closed, or by requesting the My Health Account customer services team to remove the relationships either before or after their My Health Account is closed.

The My Health Account operations team may initiate the closing of an account and / or deletion of information, if advice is received that an account may no longer be valid or needed (e.g. on notification that the owner of the account has deceased; or in line with fraud or privacy breach escalation processes, as outlined below).

A Consumer's verified attributes need to be reverified every five years. If a Consumer fails to reverify their attributes, then access to the account may be suspended and verified information deleted after due process.

Process for Managing Information Compromise

To maintain the credibility of the My Health Account service, any suspected compromise, including any unauthorised or accidental access to, disclosure, alteration, loss, or destruction of My Health Account details, NHI details, HPI number (CPN) details, or suspected fraud will be assessed and further investigated, where necessary. As My Health Account continues to be developed, strategies and reporting will continue to be developed to identify when a suspected compromise might have occurred, along with the responsibilities for monitoring this.

- Cases where there is evidence of fraud may be passed to Police for further investigation, and evidence of an offence under the Privacy Act 2020 will be addressed with the Privacy Commissioner[23].
- Notifiable privacy breaches will be reported to the Privacy Commissioner (and affected individuals or the public, where required) as soon as practicable as required by the Privacy Act.
- A warning has been incorporated into Privacy Materials to ensure users are aware of the seriousness of misrepresenting their identity or assuming the identity of another. Users are expected to agree to Terms of use, and this is incorporated into those terms (noting that this may not be appropriate for, or applicable to, young persons).

Governance

Strong governance is in place to manage any potential risk of 'function creep' – the expansion of, use of, or access to information beyond that originally contemplated.

New, and potentially novel, uses of information may evolve over time, and My Health Account will need to be flexible to respond to those innovations. As My Health Account will be part of the wider digital health environment, a governance structure that is empowered to review, and be informed about, other interlinked services will be essential. My Health Account is not a stand-alone service.

The social licence for My Health Account is key in helping manage the features with which My Health Account will interact. Security and audit oversight is also important to enhancing trust in the various services associated with My Health Account.

It is essential that experienced governance oversight and control is retained to make sure users remain fully informed, and their information is used in a way that is acceptable to them.

Governance includes:

- Privacy Impact Assessments of all applications / Services to be associated with or use My Health Account
- Reference of any privacy-related issues to the Te Whatu Ora Privacy Officer
- Governance by the Digital Health Identity Product Governance Board for collection, management, authorised use and disclosure, and deletion of data.

Governance will continue to be reviewed periodically as part of the continued delivery of the My Health Account service to the health sector.

[23] Misleading an agency by impersonating an individual, falsely pretending to be an individual or to be acting under the authority of an individual for the purpose of obtaining access to that individual's personal information or having that individual's personal information used, altered, or destroyed, is an offence under the Privacy Act – see section 212(2)(c).

Section Three – Privacy Analysis

The purpose of this Assessment is to review the process of collection, storage, use and sharing of personal and contact information for the purposes of My Health Account against the 13 Rules in the Health Information Privacy Code (HIPC). My Health Account collects personal and contact information for the purpose of connecting a Consumer with their health-related information or digital health services.

My Health Account has implemented changes incrementally, through a series of Releases. Each change of significance has been subject to Privacy Impact Assessment activity.

It is important to note that this Assessment only addresses the digital health identity component of My Health Account. It does not review any of the interconnected services that are, or may in the future, be used with My Health Account. Applications or services wishing to connect to My Health Account are required to complete an Onboarding process, which includes the completion of a Privacy Impact Assessment. Both privacy and security requirements must be met, prior to connection to My Health Account being offered.

All services authorised to connect with My Health Account must confirm and be verified that their applications or services comply with the agreed Identification Level expectations set by My Health Account or unless approved by Health New Zealand executive leadership.

Health Information Privacy Code Rules		**Background and Key Controls**	**Residual risk**
Rule 1	Purpose of collection of health information - Only collect health information if you really need it	*Purpose* My Health Account's purpose is to enable users to verify their identity information to the level required to access the digital health services with which they wish to engage. *Necessary* My Health Account has analysed the minimum identity information that can reliably be used for identification at different identification levels. A summary of the Identification Levels is contained in Appendix One. My Health Account has endeavoured to balance the amount of information necessary to meet identification requirements with the risk posed by incorrectly assigning an identification level that could enable the wrong person to access sensitive information. There is an initial level of access to generic health information (Identification Level 1), which can be enabled by providing a verified email address only. This does not need to be linked to the Consumer in any identifiable way. To access services that require a higher Identification Level, it is necessary for users of My Health Account to supply additional information that can then be verified against other sources of information. The base information that needs to be verified is: • Name* (including given and family names) • Date of Birth* In addition, depending on the verification method or process selected, users may need to provide additional information, such as: • Document type* • Document number • Expiry Date • Parent's names • Enrolled GP practice • Address • Gender • NHI number* • HPI number (CPN)* • Child's name	**Low**

		• Child's Date of Birth • Child's NHI* Of the above information, only those with an asterisk (*) next to them are retained along with verification method and the result of the verification (i.e. success / failure). Adding an NHI number or HPI number (CPN) to a My Health Account is optional, but necessary if users wish to engage with connected Digital Health Services that do not have the ability to locate those identifiers themselves. Adding a mobile number is an option for users if they prefer to receive second-factor authentication challenges via SMS rather than email, and if they would like to share that contact method with Digital Health Services.	

Rule 2	Source of information
	
	- Get it straight from the people concerned
		My Health Account is an 'opt-in' service with the Consumer (or potentially their representative for a 12- to 15-year-old) supplying most information directly to My Health Account themselves, except for:
		
		• The NHI number, which the Consumer authorises My Health Account to search for and match to their verified information
		• Information related to background processing, such as results of verification processes (i.e. success / failure), including:
		  ○ Document Identity checking
		  ○ Healthcare Provider checking
		  ○ NHI number matching
		  ○ HPI number (CPN) matching
		• The mobile number used in the Healthcare Provider Check, which needs to be sourced from the National Enrolment Service (NES) to complete the verification process
		• The details from RealMe that populate My Health Account (after express authorisation from the Consumer within the RealMe application).
		
		Provided the Privacy Materials that accompany My Health Account remain appropriate and consistent with the expressed intent, Rule 2(2)(a) will apply – the individual authorises collection of the information from someone else.
			Low

Rule 3	Collection of information from individual - Tell them what you're going to do with it	The current Privacy statement is contained in Appendix Three and the current Terms of use in Appendix Four. The documents are stored on the My Health Account website. Both documents are linked from the initial sign-up page on My Health Account and are in the footer of the application. The Privacy Materials provided are of central importance in ensuring users have a clear understanding of what My Health Account involves, and how they may control the amount of information collected, and their interaction with services that can be accessed via My Health Account. The Privacy statement is updated regularly as changes are made in My Health Account. Te Whatu Ora's website contains the most current list of connected digital health services that can be accessed via My Health Account In addition, advice and guidance can be found on the My Health Account website, providing additional context about some My Health Account features.	**Low**
Rule 4	Manner of collection of information - Be considerate when you're getting it	Consideration has been given to the minimum age of potential account holders and those who may not have full legal capacity to act on their own behalf as My Health Account develops over time. RealMe permits individuals aged 14 years and over to create an account. Currently, My Health Account permits those aged over 12 years to create their own account. • The manner of collection of information for a My Health Account is not considered inappropriate for 12- to 15-year-olds, and it remains a voluntary process for users to join My Health Account. For those who are not yet old enough to have a driver licence or other age-related form of identification, the birth certificate is also an option for Cloudcheck or, alternatively, the Healthcare Provider check can be used. • It will be important to remain alert to new applications / Services being added to ensure that any age-appropriate limits are applied if necessary, or alternatives offered.	**Low (but medium if additional services become available that under 12-year-olds may access)**

		The Privacy statement and Terms of use confirm a parent or legal guardian may assist 12- to 15-year-olds to complete the registration process for My Health Account if they wish to obtain assistance, or the young person can complete it themselves. Ongoing focus will be required if additional applications are, in future, able to use My Health Account identity services. While a parent having access to the My Covid Record of their 14-year-old (if they have set up their My Health Account) is unlikely to access particularly sensitive information, this may be quite different if more extensive access were to be available to the medical records of those 14- or 15-year-olds in the future. Careful consideration will need to be given to: • expanded access to additional applications with more sensitive information • how to limit access of a parent who set up an account, as the 12- to 15-year-old ages, and becomes more capable of managing their own information • the potential requirement of a young person to independently see a Trusted Witness to make sure that they are sufficiently competent to access information at that level, and that they have the choice to limit access by others, such as their parents, if they choose. Various solutions are currently under active consideration and, once finalised, will be incorporated into My Health Account. Customer support services are being investigated to address alternative methods of obtaining Identification Levels for those who may not have easily accessible identity documentation or may find Cloudcheck challenging to use. The RealMe identification process is available as an alternative, but it may also be a challenge to achieve for that same group of users. An account at Identification Level 1 is potentially available to any person, irrespective of age or capacity. This enables access to general health information to expand Consumer awareness of their health choices and service availability (and how to obtain those services).	
Rule 5	Storage and security of information - Take care of it once you've got it	Storage and processing of the information on My Health Account is managed by third-party IT vendors, and My Health Account will use its Authority to Operate (ATO) processes to ensure it has done everything reasonably in its power to prevent unauthorised use or disclosure of information. The IT component of My Health Account has been subject to full Ministry of Health and Te Whatu Ora Certification and Accreditation processes, together with independent third-party testing and an Authority to Operate (ATO). Future releases of significance will be subject to this same level of security scrutiny. Section 11 of the Privacy Act 2020 will apply to the hosting of My Health Account, as the information will be held on behalf of Te Whatu Ora for safe custody and processing. All services authorised to connect to My Health Account are required to provide evidence that they meet Te Whatu Ora Privacy and Security requirements. This includes evidence of Security Testing and completion of a Privacy Impact Assessment. For the 'Add a child' feature, access to the child's address and other contact details by either parent must be limited or excluded through design and onboarding controls. It is a recognised risk in a family violence situation that disclosure of address or contact details may enable one parent to locate the other, without the consent of that other parent. All account access and all account updates or changes by users will be tracked, as will all access by system administrators and call centre support. This helps Te Whatu Ora administrators to resolve queries raised by users and maintains a record of who has looked at or changed which details. These audit records will be maintained for a minimum of five years and are to be monitored by system administrators.	**Medium**
Rule 6	Access to personal information - People can see their health information if they want to	It is expected that most of the information held in My Health Account will be easily viewable by the Consumer on their own device. For information not available directly via My Health Account, the My Health Account Privacy statement outlines how to obtain access to it. My Health Account only holds information related to the service it provides and will need to refer requests for information related to other Services on to those services. This will be managed with existing Te Whatu Ora Privacy team processes.	**Low**

Rule 7	Correction of information - They can correct it if it's wrong	Users can correct some information about themselves directly within My Health Account. For other information, Users can request updates to their My Health Account information by contacting Customer services for support and/or can arrange to update information on the NHI service by contacting their general practice or hospital, as per current processes.	**Low**
Rule 8	Accuracy etc. of information to be checked before use - Make sure health information is correct before you use it	Accuracy is very important to the allocation of the unique digital health identity that will be associated with each My Health Account. Third-party processes or checking are involved in management of Identification Levels 2 and 3 (with Cloudcheck, or other approved verification partners including RealMe) or checking against an established NES record used in the provision of healthcare to the Consumer. This should assist with accuracy in assigning a correct identity to the relevant My Health Account. It is noted that the Consumer name provided to other services using My Health Account for verification will be the name that matches the documented identity attributes, not the NHI name, if there is a difference between the two. This is likely to align the legal identity of the user with the results produced via use of My Health Account, as the NHI need not record the user's legal name. This should enhance accuracy of the display produced. Users also have the option of specifying a Preferred name on their profile, which can be shared with Digital Health Services. There is also the ability to seek manual input from the specialist NHI team if an NHI number does not match during the digital processes applied. The accuracy-related issues in other services that interact with or use My Health Account will need to be carefully reviewed in the Privacy Impact Assessments for those other features.	**Low**
Rule 9	Retention of information - Get rid of it when you're done with it	Only information necessary for the effective administration of the account will be retained. A summary of the information retained is recorded in Appendix Two. If a My Health Account is closed by the Consumer (or because of an administration process – e.g. on notification that a Consumer is deceased) a record of the fact that there was an account, the email used to establish the account, the Identification Level (and related dates it was obtained), and any relevant linked NHI or health identifier number is retained. These details will be required as an audit record of authorisation for activity related to their files. A Consumer's verified attributes need to be reverified every five years. If a Consumer fails to reverify their attributes, then access to the account may be suspended and verified information deleted after due process, including when no longer required for business purposes and legal requirements.	**Low**
Rule 10	Limits on use of information - Use it for the purpose you got it	The purpose of My Health Account is to allow users to create a trusted digital health identity, which they can use to securely access Digital Health Services that link them with the health information they are authorised to access. This PIA does not address the use of information by Digital Health Services, however: • Digital Health Services must pass various security testing and compliance requirements before users can interact with them (which includes providing evidence to My Health Account of Privacy and Security due diligence) • Digital Health Services are asked to provide links to their Privacy statement and Terms of use so that these can be displayed to the Consumer in My Health Account • Users are asked for permission to share their attributes with a Digital Health Service • Digital Health Services are required by Terms of Use to advise My Health Account if their intended use of the information changes so that My Health Account can re-prompt users for their permission to share their attributes • Users can revoke their permission to share attributes with a Digital Health Service at any time. Users also need to be made aware that standard uses of their health information (for example, for managing their health) will continue to be managed by service providers in accordance with their usual processes and that My Health Account will not be able to control all access to and use of their information.	**Low**

Rule 11	Limits on disclosure of information - Only disclose it if you have good reason	The disclosure enabled via My Health Account during the verification process is signalled in advance to users, who may then choose to proceed with the disclosures (for example, to Cloudcheck or other authorised third-party identity services). The information disclosed to Digital Health Services about users is determined as part of the onboarding process, following a Privacy Impact Assessment. Only information deemed as necessary for the services offered to the Consumer is approved for disclosure to the Digital Health Service. In addition, users are required to approve the disclosure of information to the Digital Health Service before it is shared. At any time, the Consumer can choose to deny or revoke further disclosure of information. Subsequent controls on disclosure that may be associated with My Health Account will need to be carefully reviewed in future releases, prior to incorporating and enabling those activities. A Framework, within which other services may authorise disclosures, will need to be provided so that other 'enabling' services (such as Hira and My Health Records) fully address disclosure implications to make sure the My Health Account role is fully considered, and any authorisation matches the My Health Account Identification Levels. An area that needs to be specifically addressed in future is how to manage Rule 11(5) obligations in terms of s22F of the HIPC (as an information request may be refused if it would be contrary to the individual's interests or there are reasonable grounds for believing that the individual does not or would not wish the information to be disclosed). This will be a particular challenge with those 12- to 15-year-olds who may have had the assistance of their parent to establish their My Health Account and now wish to exclude their parent from access to sensitive records if services making those available may be authorised by My Health Account in future. Failure to address this risk in future would result in the Residual Risk profile rising to high. The 'Add a child' feature, enabling access by some parents to some information about their young children, will need to be monitored to ensure that address and contact details remain masked so that there is no risk of stalking or locating a former partner via this service. This will include interactions with other Digital Health Services that may inadvertently free up access to this information. There is a business process in place to suspend a parent-to-child relationship if a legitimate concern is raised with the My Health Account Customer Service team. It is also important that the 'Add a child' feature is controlled so that a parent is not able to gain access to a child's full health records via connected Digital Health Services. This is needed to avoid the disclosure of any family violence allegations (which may then inadvertently alert the perpetrator). It is recommended that Onboarding controls are applied to connected Digital Health Services, so this risk is mitigated.	**Low**
Rule 12	Disclosure of personal information outside New Zealand	My Health Account information is hosted in Australia but is held only by Microsoft Azure and Amazon Web Services (AWS) as an agent for Te Whatu Ora and the information may not be used by that contracted provider for its own purposes. Cloudcheck is based in New Zealand but interacts with Australian-based government APIs to check Australian documents, if requested by the Consumer. CentraPass is based in New Zealand but the services that My Health Account interact with are hosted in Australia (AWS). There will be no disclosure of information made outside New Zealand except for users who must support the system under the rules identified in Rule 12 for My Health Account.	**Low**
Rule 13	Unique identifiers - Only assign unique identifiers, where permitted	The National Health Index (NHI) number is the unique identifier for patients who receive healthcare in New Zealand and 'is the cornerstone of clinical and administrative patient-related information'. It is not used as the account identifier. My Health Account's use of the NHI number in the health sector is for the purpose of unique identification of the individual concerned. The applications / Services seeking to use My Health Account NHIs should be restricted to those that comply with the requirements of the HIPC (as per Rule 13(3) (noting that the agencies approved to assign the NHI number have been updated to include the new agencies under the Pae Ora Act). All parties interacting with My Health Account (other than users) will be consistent with Schedule 2 of the HIPC. The Health Provider Index (HPI) – Common Person Number (CPN) is the unique identifier for registered health practitioners in New Zealand and links them to the Health Provider Index. My Health Account initially allowed individuals that have	**Low**

		already been assigned an HPI number (CPN) to add it to their My Health Account, in order to uniquely identify themselves to Digital Health Services as a health practitioner. This complies with the requirements of Rule 13(4) such that any assignment must be by a health agency (in terms of applications / Services authorised to operate with My Health Account). This feature is to be phased out from April 2023, when the new My Health Account Workforce becomes operational. My Health Account uses GUID number (globally Unique 32 hexadecimal characters) for its account identifier. It is used only by consuming systems to uniquely identify the user in such a way that the user can change their email address without affecting access to that consuming system in future. It is not shared with or displayed to the user. It is not shared with any party other than consuming applications in a 'behind the scenes' manner.	

Appendix One – Identification Levels

Identification Level	What this level means	Information that My Health Account stores	Options to achieve identification level
Level 1	You only need to provide an email address to sign up. You have very limited access to services at Level 1 because you still need to confirm who you are before accessing identifiable information.	Email address Preferred name (if provided) Mobile number (if provided)	Signing up to My Health Account will allow you to set up a Level 1 account
Level 2	You have entered your details from one of the eligible identity documents or you have used information held by your general practice (GP) about you to verify who you are.	As per Level 1 plus: First name Middle name(s) (if you have them) Last name Date of birth HPI number (CPN) (if added)	There are currently two options to achieve Level 2. One of these must be chosen: 1. Identity document check 2. Healthcare provider check
Level 3	This level involves checking that it is really you that has created your account, and the right person has been connected to your Account.	As per Level 2 plus: HPI number (CPN) (if added)	There are currently two options to reach Level 3: 1. Use of your RealMe® Verified account 2. The combination of the Identity document check and the Healthcare provider check
Level 2N or 3N	This level involves you adding your NHI number to your account, which will allow you to access information and digital health services related to it.	As per Level 2 and 3 plus: NHI number Address – temporarily (if provided) Gender – temporarily (if provided)	Your account will be upgraded from Level 2 to 2N or Level 3 to 3N should you decide to add your NHI number to your Account

Appendix Two – Retention of Personal Information

Information attribute	Retention timeframe
Email address	For the duration of the My Health Account (including changes to these details made by the Consumer).
Mobile number	For the duration of the My Health Account (including changes to these details made by the Consumer).
Preferred name	For the duration of the My Health Account (including changes to these details made by the Consumer).
RealMe account token (identifier)	For the duration of the My Health Account.
Name (including first, middle, last name)	For the duration of the My Health Account.
Date of Birth	For the duration of the My Health Account.
Document check information (including document/card number, expiry date, version number, parent's name)	Only captured at the point of attempting to confirm identity. Information is not retained by My Health Account.
Enrolled General Practice or Medical Centre	Only captured at the point of attempting to confirm identity. Information is not retained by My Health Account.
Address	Captured at the point of attempting to confirm identity using the healthcare provider check. Information is not retained by My Health Account. May be requested during an attempt to add an NHI number to an account. Information is retained until the NHI number is successfully added.
Gender	Captured at the point of attempting to confirm identity using the healthcare provider check. Information is not retained by My Health Account. May be requested during an attempt to add an NHI number to an account. Information is retained until the NHI number is successfully added..
NHI number (including both the supplied and verified NHI number where these differ – i.e. in the case of the supplied NHI number being dormant)	For the duration of the My Health Account (or until changed or removed by an Administrator).
HPI number (CPN)	For the duration of the My Health Account (or until removed by an Administrator).
Relationship information (including Parent NHI, Child NHI, child/relationship nickname, expiry date)	For the duration of the relationship (or until changed or removed by the Consumer or Administrator). **Note:** Deleting the My Health Account that established the relationship does not delete the relationship information as

	required for audit and when no longer required for business purposes and legal requirements.
Audit records	For a minimum of five years from creation of each record and when no longer required for business purposes and legal requirements. **Note:** Access to audit records is strictly controlled and limited to Te Whatu Ora staff who are responsible for maintaining security standards and resolving customer support queries.

Appendix Three – My Health Account Privacy statement

Privacy statement

Effective 6 November 2023

My Health Account is a digital health identity service operated by Te Whatu Ora – Health New Zealand. Find out what personal information is collected if you use My Health Account, where it's kept, and who can access it.

About My Health Account

At My Health Account, we know how important privacy is to all people in Aotearoa New Zealand. This Privacy statement explains how we collect and use your personal information for a My Health Account ('Account').

- It's voluntary for you to sign up for an Account.
- My Health Account is designed to make it easy for you to access your health information, and to connect with New Zealand digital health services.
- If you are 12 years or older, you can create your own My Health Account.
- Your parent or legal guardian can also create it on your behalf, with your permission, if you are aged 12 to 15 years old.
- Some parents may also access some information about their child or children aged under 12 years if they use the 'Add a child' feature to establish a relationship between their NHI number and the NHI number of their child or children.
- If one parent disputes the right of the other parent to access a child or children's information, access to the child's or children's information will be immediately suspended for both parties until the matter is resolved.
- The information and services you can access and share via your Account are limited by the level at which you have verified your identity.

You can read more about this in our Privacy Impact Assessment (PIA).

What information is collected

We collect information you provide to us as part of confirming who you are. The information you provide and how you verify your identity sets up an 'Identification Level' for your account. This enables you to connect with digital health services that match your Identification Level. The higher your Account Identification Level, the surer we can be about who you are, and the more services you can access.

Identification Level 1

At Level 1, you only need to provide an email address to sign up. You have very limited access to digital health services at this level because you still need to confirm who you are. At Level 1, My Health Account stores the following information about you:

- Your email address
- Your preferred name (if provided)
- Your mobile phone number (if provided).

Identification Level 2

At Level 2, you have entered your details from one of the eligible identity documents or you have used information held by your general practice (GP) to verify who you are. At Level 2, My Health Account stores the same information as Level 1, plus:

- Your first name, middle name/s (if you have them), and last name
- Your date of birth
- Your HPI number (CPN) if you have added it.

You must use either the identity document check or the healthcare provider check to reach Level 2.

Identification Level 3

At Level 3, we check that it is really you that has created the account and that the right person has been connected to the account. At Level 3, My Health Account stores the same information as for Levels 1 and 2, plus:

- Your HPI number (CPN) if you have added it.

To reach Level 3, you must use:

- your RealMe® Verified account, or
- the combination of the identity document check and the healthcare provider check.

Identification Level 2N or 3N

Your account will be upgraded from Level 2 to 2N or Level 3 to 3N if you decide to add your NHI number to your account. This allows you to access your health information and digital health services related to your NHI information. At Levels 2N and 3N, My Health Account stores the same information as for Levels 1, 2, and 3 plus:

- Your NHI number
- Your address, temporarily (if provided)
- Your gender, temporarily (if provided).

Identity document check

When you use the identity document check, we verify your identity document details provided such as name, date of birth, document number, and other details (depending on the document – for example, your NZ driver licence).

We send the information you give us to our document-checking partners, Cloudcheck from Verifi or Kiwi Access Card Verification via CentraPass, for verification that the document matches the details you provide.

Verifi is a New Zealand company that provides Cloudcheck, a service to check records such as passports, driver licences, birth certificates, and other records with the Department of Internal Affairs, Waka Kotahi NZTA, and Australian authorities, on our behalf. We do record when and how you verified your identity, and the type of document you used, but do not retain the unique identifiers associated with those forms of ID.

CentraPass is a New Zealand company that provides a service to verify Kiwi Access Card details with Hospitality New Zealand. As with Cloudcheck, we do record when and how you verified your identity, and that you used your Kiwi Access Card, but do not retain the unique identifiers associated with your card.

Healthcare provider check

When you use the healthcare provider check, we verify your identity using details held by the general practice with which you are enrolled.

If you have not already added your NHI number to your account, we will check the details you give us against the NHI database to link those details to a unique NHI number.

We then check the contact details held about you by your general practice with which you are currently enrolled (if you authorise us to do so). We send you a one-time code challenge to the mobile phone number that your general practice has on their records.

If you have that mobile phone, you will be able to get and input the one-time code into My Health Account. If you do this successfully, the Identification Level of your account will be updated.

Health workforce

Health workforce members can set up a health workforce identity account using My Health Account. This allows them to connect with digital health services in a health workforce role when they have a current registration. This includes health practitioners with a Common Person Number (CPN), otherwise known as HPI Number, or other industry-recognised identifier, if approved by My Health Account for this purpose.

We use your CPN or other approved identifier, together with the name and contact details you have given to us to give you access to health workforce-related digital health services, and to record what health workforce-related digital health services you access.

Te Whatu Ora has developed a new digital health identity service for health workforce members called My Health Account Workforce. Health Workforce members who are currently using My Health Account for work-related purposes will be supported to transition across to the new Workforce account as Workforce Digital Health Services migrate.

As a health workforce member, if you are still using your My Health Account to access work-related digital health services, we will not provide your NHI if it is a health workforce-related application, and we will not provide your CPN if it is a health consumer service application.

How we use your information

Your My Health Account information is used to:

- respond to your requests and enquiries made through or about your Account
- protect against and identify fraud and other criminal activity. It is important to note that it is an offence under section 212(2)(c) of the Privacy Act 2020 to falsely pretend to be an individual or falsely claim to be acting under their authority to obtain access to that individual's personal information
- comply with and enforce applicable legal requirements, relevant standards, and our policies, including this Privacy statement
- enable us to prepare reports of statistical information about use of the services (you will not be identified in the reports produced) so that we can monitor and improve the performance of My Health Account and monitor interactions with participating third-party applications and services using My Health Account.

The Account allows you to interact with and use participating third-party apps and services:

- You need to review relevant information from those other services before you sign up to them, and grant permissions to sharing your information with those other services at the time you first access the services.
- We disclose to those participating apps and services your documented identity attributes, such as your first name, middle name, preferred name (if one is provided), last name, date of birth, email address, mobile phone number, NHI number, HPI number (CPN), related family member NHI numbers (if applicable), and identification level associated with your account.
- Attributes will only be shared with digital health services as necessary for that service. If the details are not necessary for operation of the application, they will not be supplied.
- The list of which attributes digital health services can receive is agreed upon and configured during the application onboarding process. My Health Account will ask you to grant permissions when first accessing the service and those permissions will be displayed to you as part of the Account services.
- You can also choose to stop sharing your information within your My Health Account to an application if you have previously given permission. They may retain any information supplied about you while the permission was granted but will not be able to access your Account information in future.
- Some services that require My Health Account verification apply age restrictions. If your date of birth is outside the permitted age range, you will be refused access to those services.

Visit our Connected digital health services page on our website for details of how these services use Consumer information.

Your email address: To help keep your Account secure, we may email you a verification code to use when you log in. This can also be used to help maintain your Account, for example, when you change your password. The email address must be one that is unique to you, and that you have control over, not one that is already linked to another Account. We will use this email address to contact you and may email you with updates to the My Health Account Privacy statement, and services and applications that you can access via My Health Account.

Your mobile number: We can communicate with you via SMS (text message) for 'One Time Passwords' (OTPs) rather than email. We will verify your mobile number with you before we send a text message. The mobile phone number details held within My Health Account may be shared with digital health services that are authorised and linked to the My Health Account service. These digital health services may display the stored mobile phone number from My Health Account to allow you to give permission for that digital health service to communicate with you via text message.

How we protect your privacy

We take your privacy seriously.

We have discussed the My Health Account service with the Office of the Privacy Commissioner and the Government Chief Privacy Officer. We continue to take their advice as we develop the service.

A Privacy Impact Assessment (PIA) has been completed. The PIA is updated to reflect new My Health Account features and functionality as they become available.

How we secure your information

Your personal information is held and managed in accordance with the Privacy Act and Health Information Privacy Code.

Any information you share with Te Whatu Ora – Health New Zealand will not be shared with other Government agencies without your permission. It will not be used for enforcement purposes unless there is evidence of fraudulent use of the account.

Information you choose to share with us will be held securely in compliance with Te Whatu Ora – Health New Zealand standards. Security measures are in place to protect your information from unauthorised access.

We use Microsoft Azure Services in Australia to deliver the Service. Use of other third-party services is detailed in the current Privacy Impact Assessment.

We use Google reCAPTCHA v3 as a security measure to defend My Health Account against bots. reCAPTCHA will collect information such as IP address, hardware and software information, and device and application data. This information is only used to provide, maintain, and improve reCAPTCHA and for general security purposes.

How long we keep your information

Once a My Health Account is created, the following information is retained: Applicant name, date of birth, preferred name, email, mobile phone number, and supplied and verified NHI number or HPI number (CPN). Related child NHI numbers are also retained until the relationship is removed (not when the My Health Account that established the relationship is deleted). These details are supplied to authorised services connecting to the My Health Account service as identified in the PIA for each of those services (and as approved by the My Health Account service).

You can ask for your account to be closed by calling the Contact Centre on 0800 222 478 or +64 9 307 6155. Once closed, your account is not able to be used for any further activities and all details, other than those required for audit activity, will be deleted. The email associated with the account, the Identification Level obtained (and the related dates) and the NHI number and / or CPN (if added) will be retained.

Tips to keep your My Health Account secure

- Do not share your account details with other people.
- Keep your password safe.
- We recommend using a screen lock on your device.

If you believe your password may have been compromised, please change it. If you believe your account has been compromised, please call the Contact Centre on 0800 222 478 or +64 9 307 6155 as soon as you can.

Viewing or changing your information

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

The Privacy Officer
Te Whatu Ora - Health New Zealand
PO Box 793
Wellington 6140
Email: hnzprivacy@health.govt.nz

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

When you contact us for help, your communications, including any information you provide regarding your identity and the matter you're contacting us about, will be collected.

Giving feedback

- Phone: 0800 222 478 or +64 9 307 6155 during standard office hours, 8 am to 5 pm Monday to Friday
- Email: support@identity.health.nz

Feedback is important and is used to evaluate and improve My Health Account. If you provide feedback by email, that feedback is sent to the appropriate Te Whatu Ora – Health New Zealand staff. This could include your email address and other identifying information that you have provided.

Statistical information

We may collect statistical information to help us improve the Service and understand how it is being used. In summary, this includes the event type and session, timestamps, and the type of device being used. This information is aggregated and doesn't identify you personally. Full details about the statistical information collected is addressed in our Privacy Impact Assessment.

Your My Health Account details (including NHI number, and related attributes of age, address (suburb, town, and postcode and relevant Te Whatu Ora district), ethnicity, gender, New Zealand citizenship / residency status) may be used for statistical reporting on the performance of My Health Account to enable performance monitoring and service improvement. It may also include interactions with integrating applications, such as My Covid Record, to identify usage statistics. Your personal information will remain securely contained in our systems and only aggregated information (without your name details, NHI number, or contact details) will be used in reports created, to preserve individual privacy for reporting purposes.

My Health Account uses temporary session cookies. The session cookies are limited to the lifetime of the session and provide support for features such as single sign-on (SSO), as well as enhancing the user experience within the My Health Account self-service portal. My Health Account does not use third-party or "tracking" cookies.

If you have a privacy concern

Please contact us by email: hnzprivacy@health.govt.nz.

If you are not satisfied with the response to any privacy concern, you can contact the Office of the Privacy Commissioner.

Updates to this Privacy statement

This Privacy statement may be updated to let you know about changes in how we collect and process your information in the Services or changes in related laws. The date when the document was last updated is shown at the top of this Privacy statement.

Privacy Impact Assessment

My Health Account Privacy Impact Assessment (PDF file)

Download My Health Account Privacy Impact Assessment

My Health Account Privacy Impact Assessment (Word document)

Download My Health Account Privacy Impact Assessment

Appendix Four – Consumer Terms of use

Terms of use

My Health Account is the digital health identity service operated by Te Whatu Ora – Health New Zealand. With a My Health Account, you can gain secure access to your health information online. You can also link your National Health Index (NHI) number to your account. If you are a registered health practitioner, you can link your HPI number (CPN) to your account and securely access health information and applications for professional purposes.

If you choose to create and use a My Health Account, these Terms of use will apply to you. These terms form an agreement between you and Te Whatu Ora – Health New Zealand.

What you are agreeing to

By accepting these terms, you understand and agree:

- you are aged 12 years or over (if you are aged 12 to 15 years, your parent or legal guardian may complete the registration process for you if you agree).
- some parents will be able to use the 'Add a child' feature to establish a relationship between their NHI number and the NHI number of their child or children under 12 years. This will enable the parent to connect to a digital health service and access some health information about their child or children.
- if one parent disputes the right of the other parent to access a child or children's information, access to the child's or children's information will be suspended for both parties until the matter is resolved.
- we will act on your instructions without further enquiry provided you have successfully logged in.
- you consent to us sharing your validated My Health Account identity, your HPI number (CPN) if you are a registered health practitioner, or any other NHI attribute, with participating service providers so that you can access the digital health services you choose, and they can provide services to you. **Note:** If you are a health practitioner and have both an NHI and HPI number (CPN), My Health Account will only share one of these attributes with each application, and never both.
- the information you submit and verify will be true and accurate and is about you or your dependent child.
- to any terms and conditions that apply to any digital health services that you choose to use via your My Health Account.
- that My Health Account is intended for use by people who are ordinarily resident in New Zealand and services may not be available outside New Zealand.

Your login is valuable and confidential. It authenticates your online identity with participating service providers. You must take good care of the login details you create (email address and password) and keep them secure. You agree to:

- notify the My Health Account Contact Centre on 0800 222 478 or +64 9 307 6155 immediately if you know or have reason to believe that there has been or is about to be fraudulent or other unlawful use of your login or code.
- immediately change your password and notify the My Health Account Contact Centre on 0800 222 478 or +64 9 307 6155 if you believe the security of your password has been compromised or if you are aware of any unauthorised use of your username or password.

My Health Account will never contact you and request your password, NHI number, HPI number (CPN), or access to your personal computer or other devices either by phone or email.

Anyone who knowingly accesses or uses, or attempts to access or use, any My Health Account or related Te Whatu Ora – Health New Zealand, Ministry of Health, or third-party provider service for an unlawful purpose (including, but not limited to, fraud or attempted fraud or hacking or attempted hacking) may be liable to prosecution under New Zealand Law.

It is an offence to falsely claim to be a health practitioner under section 7 of the Health Practitioners Competence Assurance Act 2003 and could result in a conviction and fine not exceeding $10,000.

If you would like help with the My Health Account service, please email us at: support@identity.health.nz. If your support request relates to a digital health service from a third-party provider, please address your queries directly to them.

Privacy and how we use your information

You can choose how much information you provide to My Health Account, and the identity verification level you want. Some digital health services are restricted to higher verification levels. We will guide you through your options.

We will securely hold and manage the information you provide to us through My Health Account. Your account allows you to decide how your information may be managed.

My Health Account Privacy statement
Read our Privacy statement at My Health Account Privacy statement.

Disclaimer

Except where we have an explicit legal obligation under New Zealand legislation, we disclaim and exclude all liability for any claim, loss, demand, or damages of any kind whatsoever (including for our negligence) arising out of or in connection with the use of either this service or the information, content or materials included in this service or on any website we link to.

It is your responsibility to provide accurate information to us, and we are entitled to rely, without making further inquiry, on information provided by you or any third party you choose to interact with via this service.

Continuity of service

We will make reasonable efforts to always keep My Health Account operational, but we make no warranty or representation, express or implied, as to continuity of service. We reserve the right to suspend, terminate or otherwise alter access to some or all the services at any time and without notice if we consider that:

- this is necessary to maintain the integrity or security of related services; or
- your login is being misused or has otherwise been compromised; or
- you breach these terms; or
- we decide to remove or reduce the services available.

Changes to these Terms of use

We may revise these Terms at any time. Changes take effect when published to our website.

Security

You must not modify, distribute, alter, tamper with, repair, or otherwise create derivative works of My Health Account unless expressly permitted.

You must not reverse engineer, disassemble, or decompile the services or apply any other process or procedure to derive the source code of any software included in the services (except to the extent applicable law doesn't allow this restriction).

My Health Account has been, and will continue to be, subjected to independent security audits. If you discover a potential security vulnerability or suspect a security incident related to this service, please email itsecurity@identity.health.nz, or report it by following the disclosure process on the CERT NZ website.

Last updated: 29 March 2023

Appendix Five – Attributes that can be requested by Digital Health Services via My Health Account

Attribute	Description	Note
Unique ID	The unique identifier for the My Health Account holder.	Must be provided.
Email	The verified email address for the My Health Account holder.	Must be provided.
Identification Level	The Identification Level that the My Health Account holder has achieved by completing verification processes.	Must be provided if any attributes other than Unique ID and Email are requested.
Mobile number	The verified mobile number as supplied by the My Health Account holder.	
Given name	The account holder's optional given name, as recorded on the official document they supplied as evidence of identity on sign-up.	Available on accounts at Identification Level 2 and higher.
Middle name	The account holder's optional middle name, as recorded on the official document they supplied as evidence of identity on sign-up.	Available on accounts at Identification Level 2 and higher.
Family name	The account holder's family name, as recorded on the official document they supplied as evidence of identity on sign-up.	Available on accounts at Identification Level 2 and higher.
Nickname / Preferred name	The account holder's preferred name as set on the self-service profile page of My Health Account.	
Date of birth	The date of birth as recorded on the account holder's official document used as evidence of identity.	Available on accounts at Identification Level 2 and higher.
NHI number	The NHI number of the My Health Account holder.	Available on accounts at Identification Level 2 and higher.
HPI number (CPN)	The HPI number (CPN) of the My Health Account holder.	Available on accounts at Identification Level 2 and higher.
Related NHI numbers	The list of NHIs that the My Health Account holder has linked to their own NHI number.	Available on accounts at Identification Level 3N.

Te Whatu Ora
Health New Zealand

Glossary

The following are definitions used in this Assessment:

Terms	Description, relationship, and business rules
Authorised Private Entity	An entity authorised to participate as a Service Provider in the health information sector after completing authorisation processes established by Te Whatu Ora / the Ministry of Health. This includes both providers of health services and health IT services.
Cloudcheck	This is the electronic identity verification service used to verify an identity document as part of My Health Account processes. More information can be found here: https://www.verifidentity.com/cloudcheck/.
Consumer	Each user who registers to use My Health Account services as their unique Digital Health Identity.
Consumer Terms of use	The terms that the Consumer will accept as part of signing up to use the My Health Account service.
Digital Health Identity	The entity information that is bound to the My Health Account used by the Consumer. Informally – an individual's My Health Account. Non-identity accounts are also available as an information channel.
Digital Health Service	A service or application offered by a Service Provider that has been onboarded to use My Health Account as a Digital Health Identity provider.
Health Practitioner	A person who is, or is deemed to be, registered with an authority as a health practitioner of a particular health profession. An authority is a body corporate responsible for the registration and oversight of health practitioners of a particular profession under the Health Practitioners Competence Assurance Act 2003.
Health Provider Index (HPI)	The central national database for use by the New Zealand health and disability sector which uniquely identifies Health Practitioners, health provider organisations and facilities.
Health Workforce	The Health Workforce includes both Health Practitioners and Non-registered Workforce members who are working in Aotearoa New Zealand's health workforce, and who are aged 16 years or over.
Health Workforce member	Each user who registers to use My Health Account Workforce services as their unique work-related Health Workforce Digital Identity.
Hira	This is a Health NZ - Te Whatu Ora initiative. It will be the national health information platform programme and will be designed to enable accessibility of health information from many sources and provide a range of digital services that make health information easier to access, use and share (with appropriate controls around privacy and security). Hira Website.
HPI number (CPN)	Also known as the Common Person Number (CPN). A unique identifier given to some Health Practitioners as part of Te Whatu Ora health identity processes. The CPN is a separate identifier given to the Health Practitioner and is recorded in the format NNXXXX where N is numeric, and X is alphabetic. It is different to the NHI number assigned to that person as a health Consumer.
Identification Level	The level of identification confirmed by My Health Account for the Consumer, as further described in Appendix 1.
Ministry	Manatū Hauora – the Ministry of Health.

Terms	Description, relationship, and business rules
My Health Account	The Te Whatu Ora application that enables users to obtain, and assert, a digital health identity.
My Health Record	The Te Whatu Ora consumer channel and interface for users using My Health Account to access Te Whatu Ora-held digital health information and available services for themselves or their authorised whānau.
My Health Account Workforce	The Te Whatu Ora application that enables members of Aotearoa New Zealand's health workforce to obtain, and assert, a Health Workforce Digital Identity.
Onboarding	The formal process (including the security and privacy aspects of the service or application) a potential connected Digital Health Service must complete prior to being permitted to use My Health Account services.
Privacy Statement Materials	Material prepared to inform users in compliance with relevant rules in the Health Information Privacy Code 2020, including rule 3 in particular.
RealMe® / RealMe® Verified	A Consumer-facing digital identity service for government agency use provided by the Department of Internal Affairs. More information at https://realme.govt.nz.
Service Provider	A government agency (including Te Whatu Ora) or Authorised Private Entity that successfully completes the Onboarding process and is authorised to use My Health Account to authenticate users in order to provide healthcare services and / or support health information management by users.
Service Provider Terms of use	The terms that will apply to each Service Provider when allocated rights to connect to My Health Account services.
Te Whatu Ora – Health New Zealand	A Crown agent established under section 11 of the Pae Ora (Healthy Futures) Act 2022.

Appendix 4

Previous version MHA-W

My Health Account Workforce

Privacy Impact Assessment

Date: 31 March2025

Te Whatu Ora
Health New Zealand

Document Approval

	Name/Title	Sign-off date
Approved by Senior Responsible Officer	Joel Brown	xx/xx/xxxx
Approved by Chief Privacy Officer, Te Whatu Ora	Karin Anderson	xx/xx/xxxx

The author of this document is the Data & Digital Directorate, Te Whatu Ora – Health New Zealand.

Disclaimer

Every effort has been made to ensure that the information contained in this report is reliable and up-to-date. This Privacy Impact Assessment (PIA) represents the current expectations of the way My Health Account Workforce services will operate.

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

Contents

SECTION ONE – EXECUTIVE SUMMARY 117

SCOPE OF ASSESSMENT 119
ASSESSMENT CONTENT 119
RECOMMENDATION SUMMARY 119

SECTION TWO – MY HEALTH ACCOUNT WORKFORCE 122

BACKGROUND 122
MY HEALTH ACCOUNT WORKFORCE 123
IDENTIFICATION LEVELS 123
INFORMATION FLOWS INVOLVED IN MY HEALTH ACCOUNT WORKFORCE IDENTIFICATION LEVEL PROCESSES: 124
INFORMATION COLLECTED DURING SIGN-UP PROCESSES 125
SIGN-UP 125
MY HEALTH ACCOUNT (HEALTH CONSUMER) CHECK 125
IDENTITY DOCUMENT CHECK 125
HEALTHCARE PROVIDER CHECK 126
REALME® VERIFIED 127
ADDING HPI NUMBER (CPN) 128
OTHER PERSONAL INFORMATION 129
COOKIES 129
STATISTICAL INFORMATION 130
AUDITING 130
INFORMATION STORAGE 130
INFORMATION UPDATES / CORRECTION 131
INFORMATION USE AND SHARING 131
ONBOARDING DIGITAL HEALTH SERVICES 131
CONSENT AND SHARING ATTRIBUTES 132
ANALYTICS AND REPORTING 132
INFORMATION DISPOSAL 133
REVERIFICATION OF DETAILS 133
PROCESS FOR MANAGING INFORMATION COMPROMISE 133
GOVERNANCE 134

SECTION THREE – PRIVACY ANALYSIS 135

APPENDIX ONE – IDENTIFICATION LEVELS 141

APPENDIX TWO – RETENTION OF IDENTIFIABLE INFORMATION 144

APPENDIX THREE – MY HEALTH ACCOUNT WORKFORCE PRIVACY STATEMENT 146

APPENDIX FOUR – MY HEALTH ACCOUNT WORKFORCE TERMS OF USE 153

APPENDIX FIVE – ATTRIBUTES THAT CAN BE REQUESTED BY DIGITAL HEALTH SERVICES VIA MY HEALTH ACCOUNT WORKFORCE 156

GLOSSARY 157

Section One – Executive Summary

22. My Health Account Workforce is the Health Workforce Digital Identity service for Aotearoa New Zealand's Health Workforce members. It is developed by Health New Zealand - Te Whatu Ora –[24].

23. Health New Zealand aims to enable the Health Workforce to establish a trusted digital identity. This will enable Health Workforce members to interact with digital channels that involve work-related information. In some cases, it may also support secure access, via digital channels, to the health information of the users that the Health Workforce support.

24. Only the right person should be able to access and manage work-related information about themselves and health information about users they support. My Health Account Workforce can confirm that a person is who they say they are, for approved health sector applications and services (Digital Health Services) and link the right person to the right information.

25. Depending on the Identification Level achieved, My Health Account Workforce will be able to confirm a digital identity has been established for the following Health Workforce members:

    25.1. for registered Health Practitioners, including their Common Person Number (CPN); and

    25.2. for non-Registered Workforce members that provides care, products or support delivery services

26. My Health Account Workforce does not confirm the person's role (other than as identified with the CPN) .and will only support self-assertions of their work-related associations.

27. My Health Account Workforce integrates with approved Digital Health Services to enable them to establish the identity of the Health Workforce Member. Those Digital Health Services with current approval at the date of issue of this PIA are listed on the My Health Account Workforce website.

    27.1. As further Digital Health Services are added over time, they will be recorded on the My Health Account Workforce website to keep Health Workforce members informed.

    27.2. Each digital health service must complete a PIA and meet the requirements of My Health Account Workforce's Identification Level framework before being allowed to use the My Health Account Workforce service.

28. Health New Zealand has recognised that there are potential privacy risks, not just to Health Workforce members contributing their information to obtain a My Health Account Workforce, but also in relation to some of the Digital Health Services that seek to connect to My Health Account Workforce if they involve Consumer information. Health

[24] Te Whatu Ora - Health New Zealand is a Crown agent within the meaning of section 10(1) of the Crown Entities Act 2004 and is established under the Pae Ora (Healthy Futures) Act 2021.

New Zealand is aware that it needs to carefully balance these risks against the benefits of enabling Health Workforce members to securely assert a digital identity to Digital Health Services.

29. Gaining the trust of Health Workforce members, the Service Providers offering the Digital Health Services, and users (if any of their identifiable information will be involved in the Digital Health Services) is essential to achieve trusted and widespread use of My Health Account Workforce. Health New Zealand a is working hard to earn and retain high levels of wider health and disability sector trust.

    29.1. Health New Zealand intends to retain Health Workforce member choice, collecting only the essential work-related information required to uniquely identify health workforce members online, and limit who will have access to that information.

    29.2. Information about Health Workforce members who use My Health Account Workforce Services is stored by Health New Zealand. That information may be shared with other Government agencies with your permission or as authorised by law. This may happen:

    - if you have authorised this sharing
    - if we think it is necessary for your care and treatment
    - If there is an incident we need to investigate, or a technology issue
    - for your safety or the safety of others, or
    - if authorised by law.

    We may provide information to other government agencies where the account is used by both agencies, such as ACC ProviderHub. In these instances, we would share information to authenticate your account, identify you, help you access your account or to troubleshoot any account issues identified by us or the agency using the account. We may also provide your information to the Ministry of Health and other government agencies that require us to provide information for administrative, legal, contractual, statistical, research or public health purposes.

    29.3. Health Workforce members are asked for their permission before their information is shared via My Health Account Workforce with connected Digital Health Services. Health Workforce members can view a list of all Digital Health Services they have previously given permission to access their information. Health Workforce members can remove these permissions at any time via My Health Account Workforce.

    29.4. Prior to being permitted to connect to My Health Account Workforce, each Digital Health Service must meet Onboarding requirements set by Health New Zealand, as well as complete a PIA. Each Digital Health Service will need to be able to enforce a minimum age requirement of 16 years on Users and ensure that they have additional processes to establish role-based access requirements if Consumer-identifiable information is accessible via the Digital Health Service.

    29.5. Any exceptions to stated above is managed on a case-by-case individual basis with assessment of merit and strong Health New Zealand governance approval only.

30. Health New Zealand consulted with the Office of the Privacy Commissioner and the Government Chief Privacy Officer prior to finalising this Privacy Impact Assessment.

31. This Privacy Impact Assessment (PIA) is a 'living' document that will be reviewed as My Health Account Workforce continues to develop. Health New Zealand will release new functionality in My Health Account Workforce Services in phases. As new features are developed and released, the privacy impacts will be reviewed and reassessed.

Scope of Assessment

32. The current Assessment covers:

    32.1. The work-related associations, demographic, and anonymous[25] information to be collected from the Health Workforce member to create a My Health Account Workforce.

    32.2. My Health Account Workforce's identity confirmation role for connected Digital Health Services.

33. This Assessment does not address:

    33.1. The Digital Health Services themselves, nor the information access available, or activities involved in those Services.

    33.2. the decision-making process, approvals, nor the conclusions reached about the decision to create My Health Account Workforce.

34. This Assessment is instead focused on the collection, storage, use and sharing of information for the purposes of providing My Health Account Workforce authentication and identity assertion services.

Assessment content

35. Section Two contains the Description of the Service and Information Flows.

36. Section Three contains the Privacy Analysis.

Recommendation Summary

37. My Health Account Workforce is a voluntary Health Workforce Digital Identity service, enabling Aotearoa New Zealand's Health Workforce members to opt in and identify themselves in order to access work-related Digital Health Services that enable them to perform their work role.

[25] Health workforce members can choose their level of engagement with My Health Account Workforce. At the lowest Identification Level (Level 1), users can provide pseudonymous information such as phone number, email address and preferred "names" without this information being verified with official sources. Health Workforce members who choose a low Identification Level will not be able to access features on the Digital Health Services, such as have access to sensitive information (e.g. medical records), until they successfully provide further evidence of identity and can meet role-based access control (RBAC) requirements within the relevant Digital Health Service.

38. Individual Health Workforce members can choose the Identification Level they wish to apply to their account. Some Digital Health Services are restricted to higher Identification Levels or may only be available to Health Practitioners or credentialed health providers. Health Workforce members will need to meet all Identification Level requirements before they can access these Digital Health Services.

    38.1. My Health Account Workforce is a 'doorway' to approved Digital Health Services, particularly for delivery of publicly funded health services. .

    38.2. Health New Zealand oversees how My Health Account Workforce controls are managed within Digital Health Services, via its Onboarding process, and retains control for Health Workforce members within their My Health Account Workforce, by enabling choice about which Digital Health Services the Health Workforce member uses and how applications are able to respond.

    38.3. There is a danger of function creep if:

        38.3.1. other services, access, or authorities are enabled that are not directly subject to easily-manageable Health Workforce member control within My Health Account Workforce; or

        38.3.2. Digital Health Services enable access to Consumer information without adequate checking of roles and facility permissions independent of the My Health Account Workforce identity processes.

    38.4. Privacy risks associated with My Health Account Workforce are successfully managed by Health Workforce member-applied controls, security measures, and strong governance oversight. Digital Health Services controls are expected to be applied via Onboarding processes and only authorised users will have access to applications..

39. Health New Zealand will work to ensure it obtains, and then maintains, Health Workforce trust in its operation of My Health Account Workforce and related services.

Recommendations:

40. The following recommendations apply to any future changes to My Health Account (or any significant changes arising from associated digital health services):

	My Health Account Workforce – Privacy Impact Assessment (PIA)	Planned Date for completion
PIA-01	Complete any Health New Zealandsecurity assessment requirements including Certification and Authorisation, and independent security testing. If any risks are identified, they will be resolved or mitigated to ensure appropriate security is applied to all aspects of the service. It is important that security measures are applied across the end-to-end services available via My Health Account Workforce to maintain trust in the service, as it is a gateway to approved Digital Health Services. Health Workforce members can reasonably expect that Health New Zealand will maintain oversight of all connected Digital	Ongoing - Prior to go-live of any new feature release of substance

	Health Services (via the Onboarding process), and not approve access to those Digital Health Services unless security is assured. These matters, however, will be potentially outside the direct control of My Health Account Workforce so communications and oversight must remain strong with other interconnected projects, such as Hira.	
PIA-02	Clear Privacy Statement Materials are to be developed and made available via My Health Account Workforce. The current version is attached in Appendix Three. This Statement includes reference to Digital Health Services permitted to integrate with My Health Account Workforce and includes full service details on a separate My Health Account Workforce web page (linked from the Privacy statement to prevent the length of the Privacy statement becoming unwieldy). Health New Zealand is planning to modernise providing future updates to Privacy statement materials – whether by banner notification within the My Health Account Workforce application or by direct email to all email addresses verified by My Health Account Workforce processes. Health New Zealand reserves the right to assess the validity of Workforce accounts in accordance to maintaining Identification Management Standards principles, such as inactivating accounts determined to belong to deceased or those deemed no longer under access to the named individuals when an organisation or account profile has ceased operations.	To be finalised in each case prior to any go-live of a new release (each updated Privacy Statement to change the Effective Date recorded at the top of the Privacy statement on the website)
PIA-03	The Onboarding process will be reviewed to ensure that Digital Health Services: • have completed a PIA and incorporate a relevant privacy statement as part of the Health Workforce Onboarding processes • will operate at an Identification Level appropriate with My Health Account Workforce settings • can apply the under 16-year-old exclusion process • can independently confirm role and employer if that is required for the Digital Health Service's operation, or be able to accept additional attributes on context of the workforce user • can independently confirm the status of any Health Practitioner registration required to allow the Health Practitioner to access that Digital Health Service • understand the limitations applicable to the Health Workforce Digital Identity established (in terms of exactly what is, and is not, verified by the My Health Account Workforce, particularly in relation to the Non-registered Workforce).	To be finalised prior to go-live in each case of additional services
PIA-04	Service Providers (who are Onboarded for their Digital Health Services) must be bound to appropriate Terms of Use that confirm the permitted purposes for use of any information accessed, to ensure Service Providers are clear about expectations for use, and limitations on use of this work-related information.	Prior to service providers being permitted to interact with My Health Account Workforce
PIA-05	Strong governance is required to ensure that My Health Account Workforce and any connecting Digital Health Services remain consistent with the My Health Account Workforce expectations set out in this Privacy Impact Assessment.	Ongoing governance oversight

Section Two – My Health Account Workforce

Background

My Health Account Workforce is a digital identity service that enables Aotearoa New Zealand's Health Workforce members to create a trusted Health Workforce Digital Identity. This is so that they can establish their identity to interact with the work-related Digital Health Services that is necessary for them to perform their work role.

- Health Workforce members must opt in to use My Health Account Workforce and can determine what Identification Level they wish to achieve.

- Depending on the level and type of identity proof that the Health Workforce member provides, My Health Account Workforce sets an Identification Level (guided by the Identification Management Standards 2020 revision 1.1 (October 2024)).

Some Digital Health Services are restricted to higher Identification Levels. Health Workforce members will need to meet all Identification Level requirements before they can access these Digital Health Services.

- Health Workforce members can then assert the necessary Identification Level to Digital Health Services that require an Identification Level to use them.

- Service Providers can use the Identification Level to ensure that private information is only released to Health Workforce members who meet their identity requirements.

My Health Account Workforce has developed a consenting process so that Health Workforce members can understand how their information is to be shared with the Digital Health Services they need to access to perform their work role and can give their consent within the My Health Account Workforce application for that information to be shared. At any time, Health Workforce members can also revoke consent for future access to their information by those same Digital Health Services.

My Health Account Workforce will be transparent with the use of the data, to maintain and grow social licence. My Health Account Workforce always follows these principles:

- The information collected will be provided (or authorised) by the Health Workforce member.
- Information collected is always secured and only shared with those who need to know.
- Only the minimum information that is needed is collected to perform a purpose. Information used temporarily (e.g. only for identity verification) is deleted once the purpose has been completed.
- The Health Workforce member can grant or deny permission to share their My Health Account Workforce information with participating Digital Health Services.

- My Health Account Workforce service may review the purpose and use of the account, and revoke access if deemed necessary for legal, security or privacy considerations.

My Health Account Workforce

The screen flows for My Health Account Workforce have been designed to be relatively self-explanatory for Health Workforce members when creating a My Health Account Workforce. My Health Account Workforce can be accessed from https://workforce.identity.health.nz.

The approach Health New Zealand has taken is to balance the need to make My Health Account Workforce as easy as possible for Health Workforce members to sign up and provide their information, against the need for appropriate security and assurance levels.

- Health Workforce members can sign up directly from the My Health Account Workforce website, but initially, most accounts will be created when a Digital Health Service the Health Workforce member wishes to use, such as a reporting tool or patient management system[26], refers them to My Health Account Workforce to establish their identity and Identification Level.

- Before signing up to My Health Account Workforce, Health Workforce members are provided links to the Privacy statement[27] and Terms of use[28] (as per current drafts in Appendix Three and Four). The website will also provide access to advice and guidance[29].

Identification Levels

Before Health Workforce members can use My Health Account Workforce, their identity must be verified. This verification process involves several steps, and the 'Identification Level' achieved reflects the increasing assurance that can be placed on each step.

The Health Workforce member can stop progressing through the identity verification steps when they want to, but they will not be able to access some Digital Health Services via My Health Account Workforce if they do not meet the Identification Level required for access to the Service in question. An Identification Level summary is set out in Appendix One.

The lowest level, Level 1 will establish only a verified email account for that User, while Level 3 will verify documented identity attributes for a person, and that the person has access to an established authentication source.

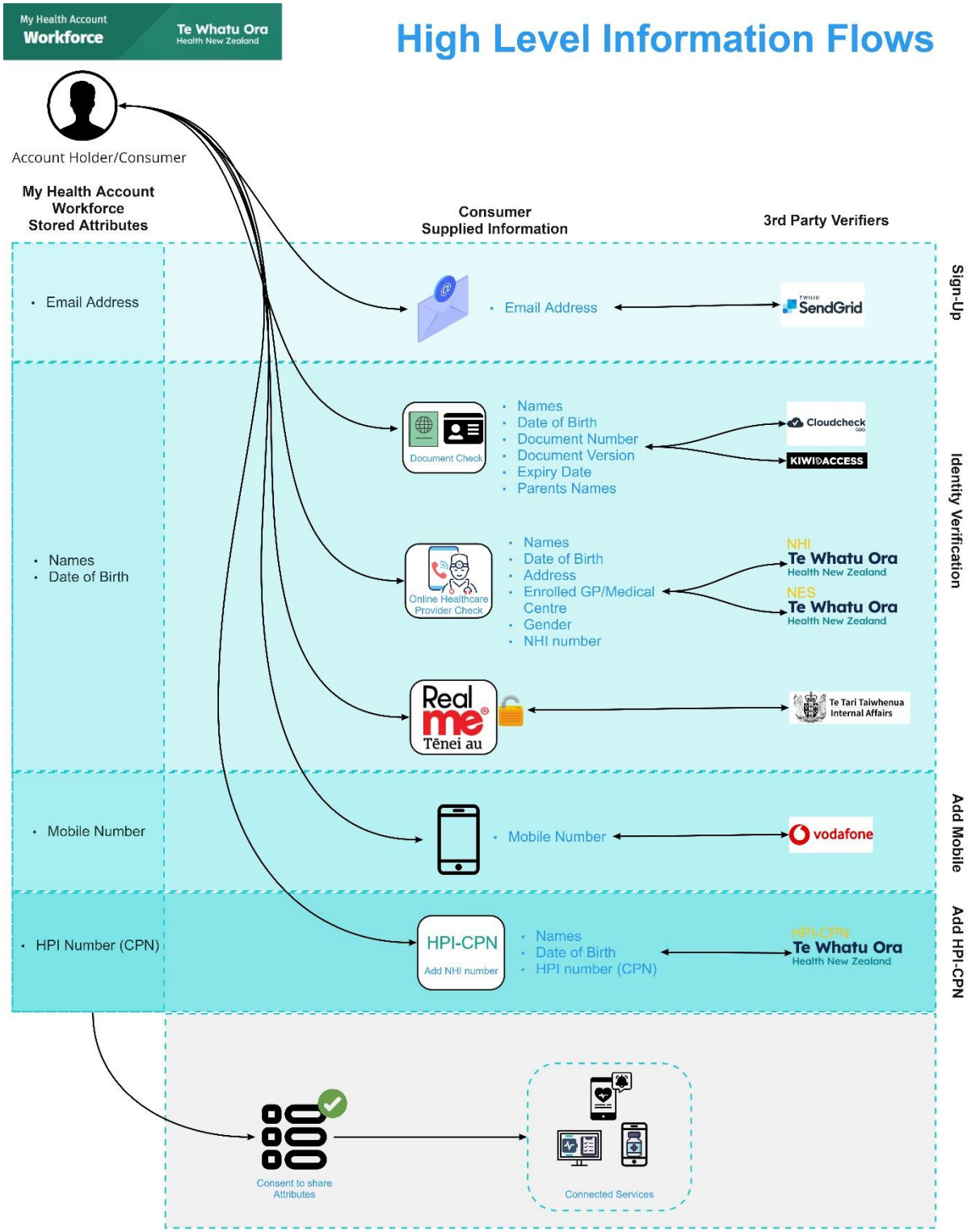
[26] Noting that My Health Account Workforce will be providing only the identification verification at the relevant Identification Level, and the existence of a corresponding CPN, if provided. The Digital Health Service would need to manage any applicable role-based access or current employment matters.

[27] https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/privacy-statement

[28] https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/terms-of-use

[29] Advice on creating your My Health Account Workforce: https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/creating-your-account and advice on how to get the most from your account: https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/getting-the-most-from-your-account

Information flows involved in My Health Account Workforce Identification Level processes:



Information Collected during sign-up processes

Sign-up

Health Workforce members can sign up to My Health Account Workforce by either providing a unique email address and password, or via an existing RealMe® or RealMe® Verified account. All Health Workforce members of My Health Account Workforce are required to provide a unique email address as part of their sign-up process. For those Health Workforce members who have signed up using an email address and password, the email address is used both to log in and for communications about the My Health Account Workforce service. For those Health Workforce members who have signed up using RealMe® or RealMe® Verified, the email address is used only for communications about the My Health Account Workforce service.

All email addresses are validated via a third-party service (SendGrid) by sending a Time-limited One Time Passcode (TOTP) to the supplied email address. Health Workforce members have 20 minutes to enter the TOTP into My Health Account Workforce to validate that they have access to the email account.

Identification Level 1 is only a verified email account.

My Health Account (health consumer) check

Health Workforce members who already have a My Health Account and have verified their identity to either Level 2 or 3 for this health consumer account, can enter the details of their My Health Account into My Health Account Workforce and the corresponding Identification Level of their consumer My Health Account will be applied to their My Health Account Workforce.

My Health Account Workforce will only retain the Health Workforce member's first name, middle name / s (if any), last name, date of birth, and the method they used to verify their identity for their My Health Account, as well as their HPI number (CPN) if it has been added to their My Health Account.

Additional attributes may be entered in, such as other 'known as' names, or associations they may have with a credentialling organisation or employer. While these are optional, they may support context for providing user access to linked digital health services that require them, particularly if the Health Workforce member is representing multiple organisations or roles signing into the same application.

No other details from their My Health Account will be stored in their My Health Account Workforce.

Identity Document Check

Health Workforce members can claim identity information in My Health Account Workforce by verifying an official document, such as a Passport or Driver Licence[30]. Health Workforce members are required to provide information as recorded on the selected document type, including name, date of birth, document/card number and, depending on the type of document used, other details such as expiry date or document version.

[30] The list of documents that can be used for verification are listed on the Te Whatu Ora My Health Account Workforce website.

The Health Workforce member-supplied information is checked against the source records (e.g. those held by DIA or Waka Kotahi) via third-party services[31] to ensure that there is a record of an official document that matches the details provided[32]. This check meets the requirements of Information Assurance according to the Identification Management Standards 2020.

My Health Account Workforce retains the Health Workforce member-supplied name and date of birth. A 'verification' details record is also kept – i.e. verification method used, verification result (valid or invalid), and the date and time of verification. The verification details are used solely for audit purposes in the event there is an apparent misuse of the verification service (e.g. in the case a person seeks to misrepresent the identity of another Consumer). It will only be accessible to select, authorised individuals from Health New Zealand (or their agents) if they are required to investigate a possible breach of the Health Workforce Terms of Use or fraud. This role will be limited, and all access tracked.

Healthcare Provider Check

Health Workforce members can choose to verify their identity using information already held about them in Health New Zealand records. Health Workforce members are required to provide information about themselves including their name, date of birth, address and the General Practice or Medical Centre with which they are currently enrolled. They also have the option to provide their gender and NHI number as part of this check process. However, the gender and NHI number details are not retained by My Health Account Workforce[33].

The Health Workforce member-supplied information is used to find and validate the user's NHI number and their patient record in the National Enrolment Service (NES)[34]. If a matching patient record is identified for the Health Workforce member, and if the patient record includes a Mobile phone number, the Health Workforce member can request that My Health Account Workforce send a Time-limited One Time Passcode (TOTP) to that Mobile number via SMS. The Health Workforce member is shown the last four digits of the phone number on the My Health Account Workforce screen (with the other details obscured) so that they can determine if they still have access to the phone with that number.

The Health Workforce member must correctly input the code into My Health Account Workforce within a 20-minute period, before it expires. If the Health Workforce member can successfully complete the TOTP challenge before it expires, it is considered a strong and direct link to the person who owns the NHI and is enrolled with the specified General Practice.

My Health Account Workforce retains the Health Workforce member-supplied name and date of birth (where not already stored) along with verification details in line with what is described under the Identity Document Check above. No information related to the Health Workforce

---

[31] Third-party services are Cloudcheck from Verifi and a Kiwi Access Card verification service from CentraPass.

[32] Information about how third-party services retain and manage data in accordance with the Privacy Act can be found here: https://www.verifidentity.com/legal/#privacy and https://kiwiaccess.co.nz/privacy-statement/.

[33] Health Workforce members are unable to add their National Health Index (NHI) number to their My Health Account Workforce. This creates a clear line of separation between their personal health information and work-related information.

[34] The NES holds the registered details of the GP, or general practice, that each person is enrolled with, and the contact details of each of those enrolled individuals.

member's NHI number or their enrolment with a general practice or healthcare provider is retained or stored.

RealMe® Verified

Health Workforce members who have signed up via a RealMe[35] account with a 'Verified' status can choose to allow RealMe to share their 'Verified' information with My Health Account Workforce.

If a Health Workforce member consents for RealMe to provide their verified attributes, then RealMe shares information including name, date of birth, gender, and address. This information, along with a Health Workforce member-provided unique email address, will be used to create a My Health Account Workforce with a strengthened assurance that the person claiming the identity attributes is the owner of the identity. This gives them an account with an Identification Level of 3.

My Health Account retains the name and date of birth along with verification details in line with what is described under the Identity Document Check above.

Uplift by relationship

Under certain circumstances, Health Workforce members are unable to access their account because they don't hold the identity documents required for document verification service. This may be due to holding documents that don't meet the current API standards, or is a Non-New Zealand or Australian government issued foreign identity document that is not a digitally verifiable.

The Health workforce member may also be based overseas where their identity is not verifiable by an Immigration New Zealand request. The expectations is that anyone using this service is under contract to a health providing service domiciled in New Zealand and that the contract is active and has provisions for security in New Zealand.

Under these circumstances, the following details are collected to ensure identity validation under this uplift by relationship process':

4. The Digital services provider's key responsible person, providing us the name of the employee is asserted that the person is real and details on the document is correct (and dated)
5. The details of the individual against an official document details (Name on file, DOB, document type, doc reference number, issue + expiry date, version number if applicable)
6. A health provider contracted in NZ (HIPC Schedule 2 provider) has confirmed that they employer of the developer is providing services to NZ health sector users.

[35] RealMe® is a government authentication and identity verification service that can be used to log in to many New Zealand government and public sector sites and services. It is also a secure way to prove who you are when you're online. For more information, see: https://www.realme.govt.nz/.

Adding HPI number (CPN)

Health Workforce members who are Health Practitioners and completed an identity verification process up to Identification Level 2 or 3, can add their Health Provider Index (HPI) – Common Person Number (CPN) to their Workforce account. The HPI number (CPN) is a unique identifier that is issued to certain Health Practitioners and links the Practitioner to their record in the Health Provider Index (HPI). This will allow them to share the number as an attribute with work-related Digital Health Services, making it easier for them to be linked to their health workforce information.

My Health Account Workforce will use the verified information (names and date of birth) stored against the Health Workforce member's record to search for a matching HPI record. Health Workforce members must provide the HPI number (CPN) but can edit the name information that is used in the search, in case the name on their Annual Practising Certificate is different to the name used on their identity document.

If a uniquely-matching HPI record is identified, the HPI number (CPN) for the HPI record is stored against the Health Workforce member's My Health Account Workforce record.

If a uniquely-matching HPI record cannot be identified, the Health Workforce member is provided with advice on how they can try again.

If the Health Workforce member has provided a different name as part of the matching process, this information is not stored against their My Health Account Workforce record.

An HPI number (CPN) can only be linked to a single My Health Account Workforce record.

My Health Account Workforce can confirm the link between a Health Practitioner's Health Workforce Digital Identity and the HPI number (CPN) assigned to them by their Responsible Authority. My Health Account Workforce does not, however, assert the annual registration status of the Health Practitioner, nor whether any conditions apply to the Health Practitioner, such as suspension. If relevant, the Digital Health Service must be required, during Onboarding, to check that the Health Practitioner's registration is current, and ensure that the Health Practitioner is not subject to suspension or any other limitation.

The HPI website specifies that in Checking credentials for access, it is expected that when *'a practitioner who has been de-registered but continues to practice tries to use their HPI identifier to log on to the system to find out information about a patient... the de-registered practitioner's credentials are automatically checked through the HPI when they try to log on and they are denied access to the information, thus protecting patient safety and privacy.*' This will need to be part of the Digital Health Service Onboarding process.

HPI number (CPN) and My Health Account

Prior to the development and launch of My Health Account Workforce, health workforce members could set up a health workforce identity account using My Health Account. This allowed them to connect with Digital Health Services in their health workforce role when they had a current registration. This included Health Practitioners with an HPI number (CPN), or other industry-recognised identifier, if approved by My Health Account for this purpose.

Health practitioners with an HPI number (CPN) were able to add their CPN to their My Health Account, if they wished to do so.

Now that Health New Zealand has developed My Health Account Workforce, Health Workforce members who are currently using My Health Account for work-related purposes will be supported to transition across to the new Workforce account as Workforce Digital Health Services is provided an option to support single sign on approaches.

Other Personal Information

Preferred Name

Health Workforce members can choose to provide a 'Preferred Name' for their My Health Account Workforce. There is no verification on the preferred name value as it is Health Workforce member-defined. The preferred name feature is used to allow a Health Workforce member to inform the Digital Health Services accessed the name by which they prefer to be known.

Mobile Number

Health Workforce members can choose to add a Mobile number to their My Health Account Workforce. Health Workforce members can choose for the Mobile number to be used as a second-factor authenticator (i.e. in cases where a higher level of authentication is required, Health Workforce members will receive a Time-limited One Time Passcode (TOTP) challenge via SMS rather than email). In addition, if the number is shared with Digital Health Services, the mobile number may be used for communication purposes (which will need to be addressed within the Digital Health Service's Privacy statement).

All mobile numbers are validated via a third-party service (One.nz) by sending a Time-limited One Time Passcode (TOTP) to the supplied mobile phone number. Health Workforce members have 20 minutes to enter the TOTP into My Health Account Workforce to validate that they have access to the mobile phone.

Additional names

Health Workforce members who may be known as other names, such as maiden, assumed or professional names may be able to add those names as part of their identity attribute profile. This is to help support binding of the user that may have been provisioned differently by each organisation or event-based issurance of a document. Consent is obtained to store, and share with third parties for purposes of determining whether the identity matches with Digital Health Service provisioning profiles or if claimed to represent the organisation.

Employer Organisations

A Health workforce member may be provided an option to associate their employer organisations who they claim to represent for access to an application using My Health Account Workforce as authenticator. This may be required by end-user applications, particularly national cloud-based services to differentiate who the user may be working 'on behalf of' prior to determining a suitable role profile for application access. My Health Account Workforce will support multiple associations by employer (identified by NZ Business Number) and will aim to assert verification of the employment relationship on a frequency (e.g. monthly, quarterly) suitable for the organisation, who will hold a contract for delivering health and disability services in New Zealand. This will help support those on hybrid accounts whom the employer may not provision a unique individual email to the employee, the Health workforce member may be health provider contracted across multiple organisations, or a

person who runs multiple health organisations, facilities or locations. Start and end date (by start or end date of month) will be recorded against the employer organisations, and this may be presented as an attribute token to the receiving Digital Health Services to help determine access rights.

Membership Organisations

A Health workforce member may be able to provide additional information around their membership by association to determine credentialling requirements, such as their association with a responsible authority, educational institutions or training evidence. Depending on the type of association and membership, these may be validated on a frequency that is suitable for the organisation. The completion and validation of such information may unlock additional functionality for those users, such as demonstration of course completion by a specialised code supports additional privileges in their profile. The purpose of collection is to support validation of user credentials beyond the HPI-CPN for wider health, social and disability workforces.

Cookies

My Health Account Workforce uses temporary session cookies. The session cookies are limited to the lifetime of the session and provide support for features such as single sign-on (SSO), as well as enhancing the user experience within the My Health Account Workforce self-service portal.

My Health Account Workforce does not use third-party or 'tracking' cookies.

Statistical Information

Health New Zealand collects statistical information to help improve the Service and understand how it is being used. This includes the event type and session, timestamps, the type of device and browser being used, and the Digital Health Service being accessed. This information is aggregated and doesn't identify the Health Workforce member personally.

Auditing

My Health Account Workforce records all activity against all Workforce accounts. System access to audit records is strictly controlled and limited to Te Whatu Ora staff who are responsible for maintaining security standards and resolving customer support queries.

Audit records will be held for a minimum period of five years.

Information Storage

Health New Zealand uses Microsoft's Azure cloud services as the underlying technology platform for My Health Account. As a cloud-based solution, all Health Workforce member information is securely held and managed within Microsoft data centres located in Australia.

The My Health Account system is designed according to strict security principles and practices. The system architecture provides multiple layers of defence, and all Health Workforce member information is encrypted, both at rest and in transit. Moreover, Health Workforce member access to their information within the system is tightly controlled, with all access being both logged and audited.

My Health Account Workforce data is held by Health New Zealand in two places – namely, the identity and analytical data stores.

The main identity store is where the system uses Health Workforce member data for providing account services, such as enabling Health Workforce members to use their account to log in to Digital Health Services.

The analytical store (or data warehouse) holds an aggregated view of My Health Account Workforce information. Health New Zealand uses this store for decision-making and audits. The insights the information provides assist in the planning of new features and functionality, as well as user profile management on deceased or inactive users.

Data maintained in the analytical store is protected by the same security controls as the main My Health Account Workforce system, with full encryption of all information and rigorous access controls.

In addition to secure data storage, the My Health Account Workforce system is also designed to be highly available, thereby allowing Health Workforce members to access their My Health Account Workforce whenever they need it.

Information Updates / Correction

Health Workforce members can update or correct some information about themselves directly via the My Health Account Workforce self-service pages. The information that a Health Workforce member can update themselves includes:

- Preferred name: (Update or Remove)
- Mobile number: (Update)
- Email address: (Update)
- Password (Update)

Health Workforce members can request that other information about them is updated by contacting My Health Account Workforce customer services. In addition to the above, the information that a Health Workforce member can request to update is:

- HPI number (CPN): (Remove)

Information Use and Sharing

Onboarding Digital Health Services

The purpose of My Health Account Workforce is to allow Health Workforce members to create a trusted Health Workforce Digital Identity, which they can use to securely access Digital Health Services that link them with the work-related health information they are authorised to access. Before a Digital Health Service is made available to the Health Workforce via My Health Account Workforce, it must pass various testing and compliance requirements. This includes ensuring that the Digital Health Service is:

- restricting access to only those Health Workforce members who meet the agreed criteria (e.g. Identification Level and Health Workforce member's age is 16 years old or over[36])
- compliant with the Privacy Act 2020 and Health Information Privacy Code 2020 (which includes only requesting attributes for which it has a valid business need)
- meeting security assurance requirements.

[36] It is noted that service (or employment) contracts can have effect as if the minor is of full age – s92 of the Contract and Commercial Law Act 2017.

Part of the Onboarding service will be to ensure the Digital Health Service only uses the My Health Account Workforce Identification Level that is appropriate to the type of health information Health Workforce members will be accessing via that Digital Health Service. It must be made clear to each Digital Health Service wishing to onboard to My Health Workforce, the scope of My Health Account Workforce as a Health Workforce Digital Identity service, noting some onboarding services may have expectations that My Health Account Workforce performs other functions such as role-based access control.

The Health New Zealand website lists the Digital Health Services currently available to the Health Workforce via My Health Account Workforce.

Consent and Sharing Attributes

Once made available, Health Workforce members must choose to interact with a Digital Health Service before any information about the Health Workforce member is shared with it. Health Workforce members are provided with an attribute list to approve for sharing when logging in to the Digital Health Service and one of the below criteria is met:

- the Health Workforce member is accessing the Digital Health Service for the first time
- the Health Workforce member has previously revoked permission to share attributes with the Digital Health Service
- the Health Workforce member has added a new attribute to their account that the Digital Health Service has requested
- the Digital Health Service has requested an attribute that has not previously been shared
- the Digital Health Service has indicated they intend to use the Health Workforce member's My Health Account Workforce information in a different way.

If the Health Workforce member chooses not to share the attributes with the Digital Health Service, then they are not logged in to the Digital Health Service and no information about the Health Workforce member is shared with the Digital Health Service.

If the Health Workforce member chooses to share the attributes with the Digital Health Service, then the information is passed to the Digital Health Service each time the Health Workforce member successfully logs in to the Digital Health Service (until they revoke the permission to share the attributes).

Health Workforce members can review and revoke the existing permissions at any time via the My Health Account Workforce self-service profile page under 'Connected Services'.

The actual attributes shared with a Digital Health Service are dependent on what the Digital Health Service has requested and what attributes the Health Workforce member has on their account, however the full list of possible attributes are detailed in Appendix Five.

Analytics and Reporting

Statistical information is used in analytical reporting to understand when and how Health Workforce members are using My Health Account Workforce so that we can monitor and improve the performance and capabilities of My Health Account Workforce. Any analytical reports use aggregated data and cannot be used to identify Health Workforce members personally.

My Health Account Workforce User information will remain securely contained in Te Whatu Ora systems and only aggregated information (without names, HPI number (CPN), or other individually-identifiable information) will be used in created reports, to preserve individual health workforce member privacy.

Information Disposal

If a Health Workforce member asks for their My Health Account Workforce to be closed, access to the account will be removed and all information deleted, other than the information required for audit purposes. Information to be retained includes the email used to establish the account, the Identification Level (and related dates it was obtained), and any linked HPI number (CPN) or health identifier number. Information collected into Te Whatu Ora's data warehouse will be retained for analytics' purposes only. The account would not be able to be used to validate further activities in future.

The My Health Account Workforce operations team may initiate the closing of an account and / or deletion of information, if advice is received that an account may no longer be valid or needed (e.g. on notification that the owner of the account is deceased; or in line with fraud or privacy breach escalation processes, as outlined below).

Reverification of Details

A Health Workforce member's full verified attributes need to be reverified every five years. If a Health Workforce member fails to reverify their attributes, then access to the User's My Health Account Workforce may be suspended and verified information deleted after due process.

Process for Managing Information Compromise

To maintain the credibility of the My Health Account Workforce service, any suspected compromise of the User's My Health Account Workforce, including any unauthorised or accidental access to, disclosure, alteration, loss, or destruction of My Health Account Workforce details, HPI number (CPN) details, or suspected fraud will be assessed and further investigated, where necessary. As My Health Account Workforce continues to be developed, strategies and reporting will continue to be developed to identify when a suspected compromise might have occurred, along with the responsibilities for monitoring this.

- Cases where there is evidence of fraud may be passed to Police for further investigation, and evidence of an offence under the Privacy Act 2020 will be addressed with the Privacy Commissioner[37].
- Notifiable privacy breaches will be reported to the Privacy Commissioner (and affected individuals or the public, where required) as soon as practicable as required by the Privacy Act.
- A warning has been incorporated into Privacy Materials to ensure Health Workforce members are aware of the seriousness of misrepresenting their identity or assuming

[37] Misleading an agency by impersonating an individual, falsely pretending to be an individual or to be acting under the authority of an individual for the purpose of obtaining access to that individual's personal information or having that individual's personal information used, altered, or destroyed, is an offence under the Privacy Act – see section 212(2)(c). It is also an offence to falsely claim to be a health practitioner under section 7 of the Health Practitioners Competence Assurance Act 2003 and could result in a conviction and fine not exceeding $10,000.

the identity of another. Health Workforce members are expected to agree to Terms of use, and this is incorporated into those terms.

Digital Health Services will be responsible for monitoring their own systems against potential wrongful activity.

Governance

Strong governance is in place to manage any potential risk of 'function creep' – the expansion of, use of, or access to information beyond that originally contemplated.

New, and potentially novel, uses of information may evolve over time, and My Health Account Workforce will need to be flexible to respond to those innovations. As My Health Account Workforce will be part of the wider digital health environment, a governance structure that is empowered to review, and be informed about, other interlinked services will be essential. My Health Account Workforce is not a stand-alone service.

The social licence for My Health Account Workforce is key in helping manage the features with which My Health Account Workforce will interact. Security and audit oversight is also important to enhancing trust in the various services associated with My Health Account Workforce.

It is essential that experienced governance oversight and control is retained to make sure Health Workforce members remain fully informed, and their information is used in a way that is acceptable to them.

Governance includes:

- Privacy Impact Assessments of all Digital Health Services to be associated with or use My Health Account Workforce
- Reference of any privacy-related issues to the Te Whatu Ora Privacy Officer
- Governance by the Digital Health Identity Product Governance Board for collection, management, authorised use and disclosure, and deletion of data.

Governance will continue to be reviewed periodically as part of the continued delivery of the My Health Account Workforce service to the health sector.

Section Three – Privacy Analysis

The purpose of this Assessment is to review the process of collection, storage, use and sharing of personal and contact information for the purposes of My Health Account Workforce against the 13 Rules in the Health Information Privacy Code (HIPC).

The pattern established for My Health Account, has been followed in My Health Account Workforce, minimising the amount of information retained to establish the Health Workforce Digital Identity. My Health Account Workforce has several privacy-enhancing features. Users are informed about what information will be shared with each Digital Health Service and are asked to give consent to that information being shared with that service. They have the option to decline to share information, in which case they will not be given access to that Digital Health Service. They can also log in to their My Health Account Workforce, at any time, and revoke access for their information to be shared with a Digital Health Service from that time forward. Security of the My Health Account Workforce environment effectively replicates that of My Health Account (and will be subject to similar Certification and Accreditation review by the Te Whatu Ora security team, and appropriate third-party testing).

A key difference will, however, be that the My Health Account Workforce will operate in the health workforce environment through Digital Health Services and may, therefore, involve access to information about health Consumers, rather than just enable access to information about the Health Workforce member themselves. This is a significant difference.

It is important to note that this Assessment only addresses the Health Workforce Digital Identity component of My Health Account Workforce. It does not review any of the connected Digital Health Services that are, or may in the future, be used with My Health Account Workforce.

- Digital Health Services wishing to connect to My Health Account Workforce are required to complete an Onboarding process, which includes the completion of a Privacy Impact Assessment. Both privacy and security requirements must be met, prior to connection to My Health Account Workforce being offered.
- Although it will be the responsibility of the Digital Health Service to manage any access it provides to information about other health Consumers (if that is its purpose), it is crucial that My Health Account Workforce is very clear about the scope of the Health Workforce Digital Identity, and the implications of what is able to be confirmed via the Identification Levels.
- It is also noted that in terms of Non-registered Workforce members only the identity of the person is established at any of the Identification Levels. If a person who was not in the Health Workforce chose to create a My Health Account Workforce account, My Health Account Workforce would not be able to identify that fact.
- It is strongly recommended that the Onboarding processes are stringent in terms of refusing access to Digital Health Services that cannot demonstrate the full solution for appropriate management of Consumer health information, such that the Service complies with the Health Information Governance Guidelines. My Health Account Workforce is likely to be only a single component of that full solution.
- All Digital Health Services authorised to connect with My Health Account Workforce must confirm that their applications or services will comply with the agreed Identification Level expectations set by My Health Account Workforce.

My Health Account Workforce will implement changes incrementally, through a series of Releases. Each change of significance will be subject to Privacy Impact Assessment activity.

Health Information Privacy Code Rules		Background and Key Controls	Residual risk
Rule 1	Purpose of collection of health information - Only collect health information if you really need it	*Purpose* My Health Account Workforce's purpose is to enable Aotearoa New Zealand's Health Workforce to verify their identity information to the level required to access the work-related Digital Health Services with which they wish to engage. *Necessary* My Health Account Workforce has analysed the minimum identity information that can reliably be used for identification at different Identification Levels. A summary of the Identification Levels is contained in Appendix One. My Health Account Workforce has endeavoured to balance the amount of information necessary to meet identification requirements with the risk posed by incorrectly assigning an Identification Level that could enable the wrong person to access sensitive information. There is an initial level of access to generic health information (Identification Level 1), which can be enabled by providing a verified email address only. This does not need to be linked to the Health Workforce member in any identifiable way. To access services that require a higher Identification Level, it is necessary for Health Workforce members using My Health Account Workforce to supply additional information that can then be verified against other sources of information. The base information that needs to be verified is: • Name* (including given and family names) • Date of Birth* In addition, depending on the verification method or process selected, Health Workforce members may need to provide additional information, such as: • Document type* • Document number • Expiry Date • Parent's names • Enrolled GP practice • Address • Gender • HPI number (CPN)* Of the above information, only those with an asterisk (*) next to them are retained along with verification method and the result of the verification (i.e. success / failure). Adding an HPI number (CPN) to a My Health Account Workforce is optional, but necessary if Health Practitioners wish to engage with Digital Health Services that do not have the ability to locate those identifiers themselves. Adding a mobile number is an option for Health Workforce members if they prefer to receive second-factor authentication challenges via SMS rather than email, and if they would like to share that contact method with Digital Health Services.	**Low**
Rule 2	Source of information - Get it straight from the people concerned	My Health Account Workforce processes involve the Health Workforce member supplying most information directly to My Health Account Workforce themselves, except for those activities it authorises My Health Account Workforce to undertake, as follows: • The HPI number (CPN), which the Health Workforce member authorises My Health Account Workforce to search for and match to their verified information • Information related to background processing, such as results of verification processes (i.e. success / failure), including:	**Low**

		○ Document Identity checking ○ Healthcare Provider checking ○ My Health Account (consumer) checking ○ HPI number (CPN) matching • The mobile number used in the Healthcare Provider Check, which needs to be sourced from the National Enrolment Service (NES) to complete the verification process • The details from RealMe that populate My Health Account Workforce (after express authorisation from the Health Workforce member within the RealMe application). Provided the Privacy Materials that accompany My Health Account Workforce remain appropriate and consistent with the expressed intent, Rule 2(2)(a) will apply – the individual authorises collection of the information from someone else.	
Rule 3	Collection of information from individual - Tell them what you're going to do with it	The current Privacy statement is contained in Appendix Three and the current Terms of use in Appendix Four. The documents are stored on the My Health Account Workforce website. Both documents are linked from the initial sign-up page on My Health Account Workforce and are in the footer of the application. The Privacy Materials provided are of central importance in ensuring have a clear understanding of what My Health Account involves, and how they may control the amount of information collected, and their interaction with services that can be accessed via My Health Account. The Privacy statement is updated regularly as changes are made in My Health Account Workforce. Te Whatu Ora's website contains the most current list of services that can be accessed via My Health Account Workforce. In addition, advice and guidance can be found on the My Health Account Workforce website, providing additional context about some My Health Account Workforce features. If a third-party Consumer's information is accessible to a Health Workforce member through a Digital Health Service, My Health Account Workforce's Onboarding process will require a Privacy Impact Assessment and Privacy Statement to be completed by that Digital Health Service.	**Low, subject to appropriate Onboarding Controls being applied to connected Digital Health Services**
Rule 4	Manner of collection of information - Be considerate when you're getting it	Consideration has been given to the minimum age of potential account holders as My Health Account Workforce develops over time. • RealMe permits individuals aged 14 years and over to create a RealMe account. Currently, My Health Account Workforce permits those aged over 16 years to create their own Workforce account. Sixteen years is considered the youngest age when it is most likely that Non-registered Health Workforce members would hold an employment role and could be expected to comply with the Terms of Use. If it is identified that there is an equity issue for younger Health Workforce members, the relevant age settings will be reconsidered. It is noted, however, that there are no technical controls on My Health Account Workforce to prevent a younger person between 12 and 16 years creating an account – it is governed by a requirement in the Terms of Use. It will, therefore, be made an Onboarding requirement for any relevant Digital Health Service that it can restrict Users to the appropriate age groups. • The manner of collection of information for a My Health Account Workforce is considered appropriate for those over 16 years old, and it remains a voluntary process for Health Workforce members to join My Health Account Workforce. • It will be important to remain alert to new Digital Health Services being added to ensure that any age-appropriate limits are applied, if necessary, or alternatives offered. Ongoing focus will be required if additional applications are, in future, able to use My Health Account Workforce Digital Health Identity services. Careful consideration will need to be given to: • Expanded access to additional Digital Health Services with more sensitive information.	**Low**

		• It might be a requirement of a young person under 18 years of age to independently see a Trusted Witness to make sure that they are sufficiently competent to access information at that level. Various solutions are currently under active consideration and once finalised will be incorporated into My Health Account. Customer support services are being investigated to address alternative methods of obtaining Identification Levels for those who may not have easily accessible identity documentation or may find Cloudcheck challenging to use. The RealMe identification process is available as an alternative, but it may also be a challenge to achieve for that same group of users.	
Rule 5	Storage and security of information - Take care of it once you've got it	Storage and processing of the information on My Health Account Workforce is managed by third-party IT vendors, and My Health Account Workforce will use its Authority to Operate (ATO) processes to ensure it has done everything reasonably in its power to prevent unauthorised use or disclosure of information. The IT component of My Health Account Workforce has been subject to full Te Whatu Ora Certification and Accreditation processes, together with independent third-party testing and an Authority to Operate (ATO). Future releases of significance will be subject to this same level of security scrutiny. Section 11 of the Privacy Act 2020 will apply to the hosting of My Health Account Workforce, as the information will be held on behalf of Te Whatu Ora for safe custody and processing. All Digital Health Services authorised to connect to My Health Account Workforce are required to provide evidence that they meet Te Whatu Ora Privacy and Security requirements. This includes evidence of Security Testing and completion of a Privacy Impact Assessment. All account access and all account updates or changes by Health Workforce member Users will be tracked, as will all access by system administrators and call centre support. This helps Te Whatu Ora administrators to resolve queries raised by Health Workforce members and maintains a record of who has looked at or changed which details. These audit records will be maintained for a minimum of five years and are to be monitored by system administrators.	**Low**
Rule 6	Access to personal information - People can see their health information if they want to	It is expected that most of the information held in My Health Account Workforce will be easily viewable by the Health Workforce member on their own device. For information not available directly via My Health Account Workforce, the My Health Account Workforce Privacy statement outlines how to obtain access to it. My Health Account Workforce only holds information related to the Digital Health Identity service it provides and will need to refer requests for information related to other Services on to those services. This will be managed with existing Te Whatu Ora privacy team processes.	**Low**
Rule 7	Correction of information - They can correct it if it's wrong	Health Workforce members can correct some information about themselves directly within My Health Account Workforce. For other information, Health Workforce member can request updates to their My Health Account Workforce information by contacting Te Whatu Ora customer services for support and/or can arrange to update information on the HPI service by contacting their Responsible Authority, as per current processes.	**Low**
Rule 8	Accuracy etc. of information to be checked before use - Make sure health information is correct before you use it	Accuracy is very important to the allocation of the unique Health Workforce Digital Identity that will be associated with each My Health Account Workforce. Third-party processes or checking are involved in management of Identification Levels 2 and 3 (with Cloudcheck, or other approved verification partners including RealMe) or checking against an established NES record used in the provision of healthcare to the Consumer or checking against the Health Workforce member's My Health Account (health consumer). This should assist with accuracy in assigning a correct Digital Health Identity to the relevant Identification Level in the User's My Health Account Workforce. It is important that the Digital Health Services clearly understand the implications of 'accuracy' in terms of the information available in the Digital Health Identity provided by the My Health Account Workforce. For a Non-registered Workforce member, only the person's identity can be established – the fact that they are an account holder does not actually establish that they are a Health Workforce member, nor the role they might hold if they are a Health Workforce member, nor their employer.	**Low**

		It is noted that the Health Practitioner name provided to other Digital Health Services using My Health Account Workforce for verification will be the name that matches the documented identity attributes. The Health Practitioner's name stated on their Annual Practising Certificate (APC) – i.e. the one attached to the HPI number (CPN) – may be different. Health Practitioners can use the 'Change' feature in the My Health Account Workforce profile page to update their Preferred name so that it matches the name stated on their APC. This additional 'nickname' attribute can then be shared with Digital Health Services. If a connected Digital Health Service needs the Health Practitioner's name to match the Health Practitioner's name attached to the HPI number (CPN), then they can query the Health Provider Index directly. There is also the ability to seek manual input from the HPI team if an HPI number (CPN) does not match during the digital processes applied. The accuracy-related issues in other services that interact with or use My Health Account Workforce will need to be carefully reviewed in the Privacy Impact Assessments for those other features.	
Rule 9	Retention of information - Get rid of it when you're done with it	Only information necessary for the effective administration of the account will be retained. A summary of the information retained is recorded in Appendix Two. If a My Health Account Workforce is closed by the Health Workforce member (or because of an administration process – e.g. on notification that a Health Workforce member is deceased) a record will be retained of the fact that there was an account, the email used to establish the account, the Identification Level (and related dates it was obtained), and any linked CPN or health identifier number. These details will be required as an audit record of authorisation for activity related to their files. A Health Workforce member's verified Digital Health Workforce Identity attributes need to be reverified every five years. If a Health Workforce member fails to reverify their attributes, then access to the account may be suspended and verified information deleted after due process.	**Low**
Rule 10	Limits on use of information - Use it for the purpose you got it	The purpose of My Health Account Workforce is to allow Health Workforce members to create a trusted Health Workforce Digital Identity, which they can use to securely access Digital Health Services that link them with the work-related health information they are authorised to access. • This PIA does not address the subsequent use of the Health Workforce Digital Identity information by Digital Health Services but notes that it is important for the integrity of this identity system that the Digital Health Services ensure they use the correct Identification Levels and that any use of My Health Account Workforce to access identifiable health Consumer information is appropriately supported by other Digital Health Service processes. • It is however noted that Digital Health Services must pass various Onboarding, security testing and compliance requirements before they are permitted to access any My Health Account Workforce information (which includes providing evidence to My Health Account Workforce of Privacy and Security due diligence) The Digital Health Services are required to meet the 'use' requirements described in the Privacy Statement for My Health Account Workforce as part of the Onboarding process: • Digital Health Services are asked to provide links to their Privacy statement and Terms of use so that these can be displayed to the Health Workforce member in My Health Account Workforce • My Health Account Workforce Users are asked for permission to share their attributes with each Digital Health Service prior to the initial connection with the Service • Digital Health Services are required by Terms of Use to advise My Health Account Workforce if their intended use of the information changes so that My Health Account Workforce can re-prompt Health Workforce members for their permission to share their attributes for the changed use • Health Workforce members can revoke their permission to share attributes with a Digital Health Service at any time.	**Low**

		Health Workforce members also need to be made aware that standard uses of their work-related information (for example, for managing their access to Digital Health Services that they need to do their job) will continue to be managed by service providers in accordance with their usual processes and that My Health Account Workforce will not be able to control all access to and use of their work-related information.	
Rule 11	Limits on disclosure of information - Only disclose it if you have good reason	The disclosure enabled via My Health Account Workforce during the verification process is signalled in advance to Health Workforce members, who may then choose to proceed with the disclosures (for example, to Cloudcheck or other authorised third-party identity services). The information disclosed to Digital Health Services about Health Workforce members is first determined as part of the Onboarding process, following a Privacy Impact Assessment. Only information deemed necessary for the Digital Health Services about the Health Workforce member are approved for disclosure to the Digital Health Service. In addition, Health Workforce members are required to approve the disclosure of information to the Digital Health Service before it is shared on the first occasion on which they use the Digital Health Service. At any time, the Health Workforce member can choose to deny or revoke further disclosure of information in relation to that particular Digital Health Service.	**Low**
Rule 12	Disclosure of personal information outside New Zealand	My Health Account Workforce information is hosted in Australia but is held only by Microsoft Azure and Amazon Web Services (AWS) as an agent for Te Whatu Ora and the information may not be used by that contracted provider for its own purposes. Cloudcheck is based in New Zealand but interacts with Australian-based government APIs to check Australian documents, if requested by the Health Workforce member. CentraPass is based in New Zealand but the services that My Health Account Workforce interact with are hosted in Australia (AWS). There will be no disclosure of information made outside New Zealand under the rules identified in Rule 12 for My Health Account Workforce.	**Low**
Rule 13	Unique identifiers - Only assign unique identifiers, where permitted	All Digital Health Services connecting to My Health Account Workforce will be required to be consistent with Schedule 2 of the HIPC as part of the Onboarding process. The Health Provider Index (HPI) – Common Person Number (CPN) is the unique identifier for Health Practitioners in New Zealand and links them to the Health Provider Index. My Health Account Workforce allows individuals that have already been assigned an HPI number (CPN) to add it to their My Health Account Workforce, in order to uniquely identify themselves to Digital Health Services as a Health Practitioner. This complies with the requirements of Rule 13(4) such that any assignment must be by a health agency (in terms of applications / Services authorised to operate with My Health Account Workforce). My Health Account Workforce uses GUID number (globally Unique 32 hexadecimal characters) for its account identifier. It is used only by consuming systems to uniquely identify the User in such a way that the User can change their email address without affecting access to that consuming system in future. It is not shared with or displayed to the User. It is not shared with any party other than consuming applications in a 'behind the scenes' manner.	**Low**

Appendix Five– Identification Levels

For My Health Account Workforce User

Identification Level	What this level means to a My Health Account Workforce member	Information that My Health Account Workforce stores	Options to achieve identification level
Level 1	You only need to provide an email address to sign up. You have very limited access to services at Level 1 because you still need to confirm who you are before accessing identifiable information.	Email address Preferred name (if provided) Mobile number (if provided)	Signing up to My Health Account Workforce will allow you to set up a Level 1 account.
Level 2	You have used your My Health Account (consumer) already verified to Level 2, or you have entered your details from one of the eligible identity documents or you have used information held by your general practice (GP) about you to verify who you are.	As per Level 1, plus: First name Middle name(s) (if you have them) Last name Date of birth HPI number (CPN) (if added)	There are currently three options to achieve Level 2. One of these must be chosen: 3. My Health Account (health consumer) check if the account is verified to Level 2 4. Identity document check 5. Healthcare provider check
Level 3	This level involves checking that it is really you that has created your Workforce account, and the right person has been connected to your Account.	As per Level 2, plus: HPI number (CPN) (if added)	There are currently three options to reach Level 3: 3. Use of your RealMe® Verified account 4. Use of the My Health Account (health consumer) check if your account is verified to Level 3 5. The combination of the Identity document check and the Healthcare provider check

For Digital Health Services authorised to Onboard with My Health Account Workforce

Identification Level established by My Health Account Workforce User	What this Identification Level represents to a Digital Health Service about a My Health Account Workforce User	Information that My Health Account Workforce can share at that Identification Level (as approved during the Onboarding process)	My Health Account Workforce authentication of identity scope associated with this Identification Level
Level 1	This confirms only that the My Health Account Workforce User has a verified email address that has not been used by any other User.	Email address Preferred name (if provided) Mobile number (if provided)	Level 1 identification does not confirm the identity of the User.
Level 2	This confirms the My Health Account Workforce User has a verified email address, and that the User has established a Health Workforce Digital Identity in only one of the following ways: • Attributes: The User has presented an identity document that is verified as matching the User Account name and Date of Birth; OR • Authenticate: The User has been able to verify they have access to a device recorded in Te Whatu Ora records as belonging to a person with the User name. If an HPI number (CPN) is recorded this will have been verified against the Health Provider Index records held by Te Whatu Ora as correct for the person with that User name.	As per Level 1, plus: First name Middle name(s) Last name Date of birth HPI number (CPN) (if added)	Level 2 confirms EITHER that a User's name and date of birth has been confirmed with a document verification process OR that the User has access to a device known to belong to the named person. If a Health Practitioner adds their HPI number (CPN) to their account, Level 2 confirms that there is a match between the Health Practitioner and the HPI number (CPN) provided. Level 2 is not sufficient to authorise any Health Workforce member User to access a Digital Health Service that contains identifiable health information about a Consumer. The Digital Health Service is responsible for: 1. ensuring any onboarded Health Workforce member has an appropriate Identification Level 2. meeting all role-based access control requirements

			3. confirming that a Health Practitioner's annual registration is current. My Health Account Workforce does not show details of any employment role related to a Health Workforce member and, in the case of Non-registered Health Workforce members, does not confirm the person has a Health Workforce role.
Level 3	This level confirms that the My Health Account Workforce User has: • both Verified their name and date of birth attributes via a recognised identity document and authenticated their identity with a device known to be possessed by the User of that name; OR • confirmed their identity with RealMe Verified Services. If an HPI number (CPN) is recorded this will have been verified against the Health Provider Index records held by Te Whatu Ora as correct for the person with that User name.	As per Level 2, plus: HPI number (CPN) (if added)	Level 3 confirms the person has established their Health Workforce Digital Identity, and an HPI number (CPN) connected to that Health Practitioner (if one is provided). The Digital Health Service is responsible for: 1. ensuring any onboarded Health Workforce member has an appropriate Identification Level 2. meeting all role-based access control requirements 3. confirming that a Health Practitioner's annual registration is current. My Health Account Workforce does not show details of any employment role related to a Health Workforce member and, in the case of Non-registered Health Workforce members, does not confirm the person has a Health Workforce role.

Appendix Two – Retention of Identifiable Information

Information attribute	Retention timeframe
Email address	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
Mobile number	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
Preferred name	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
RealMe account token (identifier)	For the duration of the My Health Account Workforce.
Name (including first, middle, last name)	For the duration of the My Health Account Workforce.
Date of Birth	For the duration of the My Health Account Workforce.
Document check information (including document/card number, expiry date, version number, parent's name)	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
Enrolled General Practice or Medical Centre	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
Address	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
Gender	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
HPI number (CPN)	For the duration of the My Health Account Workforce (or until removed by an Administrator).
Audit records	For a minimum of five years from creation of each record. **Note:** Access to audit records is strictly controlled and limited to Te Whatu Ora staff who are responsible for maintaining security standards and resolving customer support queries
Alternative names	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
Employer association	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
Association by membership	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).

Appendix Three – My Health Account Workforce Privacy statement

Privacy statement

Effective 20 April 2023

My Health Account Workforce is a health workforce digital identity service operated by Te Whatu Ora – Health New Zealand, for members of Aotearoa's health workforce. Find out what work-related information is collected about you if you use My Health Account Workforce, where it's kept, and who can access it.

About My Health Account Workforce

All of Aotearoa New Zealand's health workforce members can set up a health workforce digital identity using My Health Account Workforce. This allows them to connect with relevant digital health services in their health workforce role. This includes health practitioners with a current registration and Common Person Number (CPN), otherwise known as a Health Provider Index (HPI) Number, or other industry-recognised identifier, if approved by My Health Account for this purpose.

At My Health Account Workforce, we know how important privacy is to people in the health sector – both health workforce member information and information about the people to whom they provide healthcare services. This Privacy statement explains how we collect and use your work-related information for a My Health Account Workforce ('Account').

- It's voluntary for you to sign up for an Account.
- My Health Account Workforce is designed to make it easy for you to confirm who you are online and to connect with New Zealand work-related digital health services.
- If you are 16 years or older and a member of Aotearoa New Zealand's health workforce, you can create your My Health Account Workforce.
- The information and services you can access and share via your Account are limited by the level at which you have verified your identity and the Terms of use of any workforce-related digital health service with which you connect.

You can read more about this in our Privacy Impact Assessment (PIA).

Health workforce members can set up a separate health consumer My Health Account (for when they are receiving health services) and a My Health Account Workforce (for when they are operating in their health workforce role to deliver services).

If you have previously added your CPN to your My Health Account and use it for both personal and work purposes, or if you currently have a separate My Health Account with your CPN added that you use for work purposes only, you will be given support to transition to My Health Account Workforce.

What information is collected

We collect information you provide to us as part of confirming who you are. The information you provide and how you verify your identity sets up a Workforce Account 'Identification Level' for your account. This enables you to connect with work-related digital health services that match your Identification Level. The higher your Account Identification Level, the surer we can be about who you are, and the more services you can access.

If you are a health practitioner, you can add your HPI number (CPN) to your account if you wish.

Identification Level 1

At Level 1, you only need to provide an email address to sign up and we will send you a verification code to confirm it is an email account to which you have access. You have very limited access to work-related digital health services at this level because you still need to confirm who you are. At Level 1, My Health Account stores the following information about you:

- Your email address
- Your preferred name (if provided)
- Your mobile phone number (if provided).

Identification Level 2

At Level 2, you have entered your details from one of the eligible identity documents or you have used information held by your general practice (GP) to verify who you are, or you have used your Level 2 My Health Account (consumer) to verify your identity. At Level 2, My Health Account Workforce stores the same information as Level 1, plus:

- Your first name, middle name/s (if you have them), and last name
- Your date of birth
- Your HPI number (CPN) if you have added it.

You must use either the identity document check, the healthcare provider check, or the My Health Account (consumer) check to reach Level 2. If you provide your HPI number (CPN), we will verify it against our records.

Identification Level 3

At Level 3, we check that it is really you that has created the account and that the right person has been connected to the account. At Level 3, My Health Account stores the same information as for Levels 1 and 2, plus:

- Your HPI number (CPN) if you have added it.

To reach Level 3, you must use:

- your RealMe® Verified account, or
- the combination of the identity document check and the healthcare provider check
- The My Health Account (consumer) check if your consumer account is at Level 3.

Identity document check

When you use the identity document check, we verify your identity document details provided such as your name, date of birth, document number, and other details (depending on the document – for example, your NZ driver licence).

We send the information you give us to our document-checking partners, Cloudcheck from Verifi or Kiwi Access Card Verification via CentraPass, for verification that the document matches the details you provide.

Verifi is a New Zealand company that provides Cloudcheck, a service to check records such as passports, driver licences, birth certificates, and other records with the Department of Internal Affairs, Waka Kotahi NZTA, and Australian authorities, on our behalf. We do record when and how you verified your identity, and the type of document you used, but do not retain the unique identifiers associated with those forms of ID.

CentraPass is a New Zealand company that provides a service to verify Kiwi Access Card details with Hospitality New Zealand. As with Cloudcheck, we do record when and how you verified your identity, and that you used your Kiwi Access Card, but do not retain the unique identifiers associated with your card.

Healthcare provider check

When you use the healthcare provider check, we verify your identity using details held by the general practice with which you are enrolled.

We check the details you give us against the NHI database to link those details to a unique NHI number. We do not retain this NHI detail on your My Health Account Workforce.

We then check the contact details held about you by your general practice with which you are currently enrolled (if you authorise us to do so). We send you a one-time code challenge to the mobile phone number that your general practice has on their records.

If you have that mobile phone, you will be able to get and input the one-time code into My Health Account Workforce. If you do this successfully, the Identification Level of your account will be updated.

My Health Account (consumer) check

If you have a My Health Account and you have verified your identity to either Level 2 or 3 for your consumer account, you can enter the details of your My Health Account into My Health Account Workforce and the corresponding Identification Level of your consumer account will be applied to your My Health Account Workforce. We will only retain your first name, middle name / s (if you have any), last name, date of birth, and the method you used to verify your identity for your My Health Account, as well as your HPI number (CPN) if it has been added to your My Health Account. No other details from your My Health Account will be stored in your My Health Account Workforce.

Your HPI number (CPN)

If you are a registered health practitioner, you can add your HPI number (CPN) or other approved identifier to your account. Together with the name and contact details you have given us, this enables us to give you access to health workforce-related digital health services, and to record what health workforce-related digital health services you access.

How we use your information

Your My Health Account Workforce information is used to:

- respond to your requests and inquiries made through or about your Account
- protect against and identify fraud and other criminal activity. **Note:** it is an offence to falsely claim to be a health practitioner under section 7 of the Health Practitioners Competence Assurance Act 2003 and could result in a conviction and fine not exceeding $10,000. It is also an offence under section 212(2)(c) of the Privacy Act 2020 to falsely pretend to be an

individual or falsely claim to be acting under their authority to obtain access to that individual's personal information.
- comply with and enforce applicable legal requirements, relevant standards, and our policies, including this Privacy statement.
- enable us to prepare reports of statistical information about how services are used (you will not be identified in the reports produced) so that we can monitor and improve the performance of My Health Account Workforce and monitor interactions with participating third-party applications and services using My Health Account Workforce.

The Account allows you to connect with and use participating Te Whatu Ora – Health New Zealand or third-party work-related apps and services:

- You need to review relevant information from those other services before you sign up to them, and grant permissions to sharing your information with those other services at the time you first access the services.
- We disclose to those participating apps and services your documented identity attributes, such as your first name, middle name, preferred name (if one is provided), last name, date of birth, email address, mobile phone number, HPI number (CPN), and identification level associated with your account.
- Attributes will only be shared with digital health services as necessary for that service. If the details are not necessary for operation of the application, they will not be supplied.
- The list of which attributes digital health services can receive is agreed upon and configured during the application onboarding process.
- My Health Account Workforce will ask you to grant permissions when first accessing the service and those permissions will be displayed to you as part of the Account services.
- You can also choose to stop sharing your information within your My Health Account Workforce to an application if you have previously given permission. They may retain any information supplied about you while the permission was granted but will not be able to access your Account information in future.
- Some services that require My Health Account Workforce verification apply age restrictions. If your date of birth is outside the permitted age range, you will be refused access to those services.

Visit our connected digital health services page on our website for details of how these services use Health Workforce information.

Your email address: To help keep your Account secure, we may email you a verification code to use when you log in. This can also be used to help maintain your Account, for example, when you change your password. The email address must be one that is unique to you, and that you have control over, and cannot be already linked to another Account. We will use this email address to contact you and may email you with updates to the My Health Account Workforce Privacy statement and services, and applications that you can access via My Health Account Workforce.

Your mobile number: We can communicate with you via SMS (text message), rather than email, for 'One-Time Passwords' (OTPs). We will verify your mobile number with you before we send a text message. Your mobile phone number details held within My Health Account Workforce may be shared with digital health services that are authorised and linked to the My Health Account Workforce service. These digital health services may display your stored mobile phone number from My Health Account Workforce to allow you to give permission for that digital health service to communicate with you via text message.

How we protect your privacy

We take your privacy seriously.

We have discussed the My Health Account Workforce service with the Office of the Privacy Commissioner and the Government Chief Privacy Officer. We continue to take their advice as we develop the service further.

A Privacy Impact Assessment (PIA) has been completed. The PIA is updated to reflect new My Health Account Workforce features and functionality as they become available.

How we secure your information

Your workforce-related information is held and managed in accordance with the Privacy Act and Health Information Privacy Code.

Any information you share with Te Whatu Ora – Health New Zealand will not be shared with other Government agencies without your permission or as authorised by law. It will not be used for enforcement purposes unless there is evidence of fraudulent use of the account, or it is required to establish which individual's Account was used to access digital health services in the event of a potential breach of privacy or for other inappropriate activities.

Information you choose to share with us will be held securely in compliance with Te Whatu Ora – Health New Zealand standards. Security measures are in place to protect your information from unauthorised access.

We use Microsoft Azure Services in Australia to deliver the Service. Use of other third-party services is detailed in the current Privacy Impact Assessment.

We use Google reCAPTCHA v3 during the account sign-up stage as a security measure to defend My Health Account Workforce against bots. reCAPTCHA collects information such as IP address, hardware and software information, and device and application data. This information is only used to provide, maintain, and improve reCAPTCHA and for general security purposes.

How long we keep your information

Once a My Health Account Workforce account is created, the following information is retained: Applicant name, date of birth, preferred name, email, mobile phone number, and supplied and verified HPI number (CPN). These details are supplied to authorised services connecting to the My Health Account Workforce service as identified in each of the respective service's PIA (and as approved by the My Health Account Workforce service).

You can ask for your account to be closed by calling the Contact Centre on 0800 222 478 or +64 9 307 6155. Once closed, your account is not able to be used for any further activities and all details, other than those required for audit activity, will be deleted. The email associated with the account, the Identification Level obtained, and the related dates and CPN (if added) are retained.

Tips to keep your My Health Account Workforce secure

- Do not share your account details with other people.
- Keep your password safe.
- If you use a shared device in your workplace, ensure you log out of your account before anyone else uses the device.

- We recommend using a screen lock on your device.

If you believe your password may have been compromised, please change it. If you believe your account has been compromised, please call the Contact Centre on 0800 222 478 or +64 9 307 6155 as soon as you can.

Viewing or changing your information

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

The Privacy Officer
Te Whatu Ora – Health New Zealand
PO Box 793
Wellington 6140
Email: hnzprivacy@health.govt.nz

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

When you contact us for help, your communications, including any information you provide regarding your identity and the matter you're contacting us about, are collected.

Giving feedback

- Phone: 0800 222 478 or +64 9 307 6155 during standard office hours, 8 am to 5 pm Monday to Friday
- Email: support@identity.health.nz

Feedback is important and is used to evaluate and improve My Health Account Workforce. If you provide feedback by email, that feedback is sent to the appropriate Te Whatu Ora – Health New Zealand staff. This could include your email address and other identifying information that you have provided.

Statistical information

We may collect statistical information to help us improve the Service and understand how it is being used. In summary, this includes the event type and session, timestamps, and the type of device being used. This information is aggregated and doesn't identify you personally. Full details about the statistical information collected is addressed in our Privacy Impact Assessment.

Your My Health Account Workforce details may be used for statistical reporting on the performance of My Health Account Workforce to enable performance monitoring and service improvement. It may also include interactions with integrating work-related applications to identify usage statistics. Your personal information will remain securely contained in our systems and only aggregated information (without your name details, HPI number (CPN), or contact details) will be used in reports created, to preserve individual privacy for reporting purposes.

My Health Account uses temporary session cookies. The session cookies are limited to the lifetime of the session and provide support for features such as single sign-on (SSO), as well as enhancing the user experience within the My Health Account self-service portal. My Health Account does not use third-party or "tracking" cookies.

If you have a privacy concern

Please contact us by email: hnzprivacy@health.govt.nz.

If you are not satisfied with the response to any privacy concern, you can contact the Office of the Privacy Commissioner.

Updates to this Privacy statement

This Privacy statement may be updated to let you know about changes in how we collect and process your information in the Services or changes in related laws. The date when the document was last updated is shown at the top of this Privacy statement.

Privacy Impact Assessment

My Health Account Workforce Privacy Impact Assessment (PDF file)

Download My Health Account Workforce Privacy Impact Assessment (PDF)

My Health Account Workforce Privacy Impact Assessment (Word document)

Download My Health Account Workforce Privacy Impact Assessment (Word)

Appendix Four – My Health Account Workforce Terms of use

Terms of use

My Health Account Workforce is the health workforce digital identity service operated by Te Whatu Ora – Health New Zealand for members of Aotearoa's health workforce. With a My Health Account Workforce, you can gain secure access to work-related digital health services for professional purposes and may be able to securely access health information (subject to the requirements of those digital health services). If you are a registered health practitioner, you can link your HPI number (CPN) to your account.

If you choose to create and use a My Health Account Workforce, these Terms of use will apply to you. These terms form an agreement between you and Te Whatu Ora – Health New Zealand.

What you are agreeing to

By accepting these terms, you understand and agree:

- you are aged 16 years and over.
- we will act on your instructions without further enquiry provided you have successfully logged in.
- you consent to us sharing your validated My Health Account Workforce identity, and your HPI number (CPN) if you are a registered health practitioner, with the digital health services permitted to connect to My Health Account Workforce.
- the information you submit and verify will be true and accurate and is about you, in your professional capacity as a member of Aotearoa New Zealand's health workforce.
- to any terms and conditions that apply to any digital health services that you choose to use via your My Health Account Workforce.
- that My Health Account Workforce is intended for use by people who are ordinarily resident in New Zealand and are members of Aotearoa's health workforce and services may not be available outside New Zealand.

Note: As a member of the health workforce, you are not able to add your NHI number to your workforce account, nor are you able to access your personal health information or consumer-related digital health services from this account. If you wish to set up a digital identity so that you can access digital health services as a health consumer, you need to set up a separate My Health Account.

Your workforce login is valuable and extremely confidential. It authenticates your health workforce digital identity with participating digital health service providers to the identity level you have established. You must take good care of the login details you create (email address and password) and keep them secure. You agree to:

- notify the My Health Account Workforce Contact Centre on 0800 222 478 or +64 9 307 6155 immediately if you know or have reason to believe that there has been or is about to be fraudulent or other unlawful use of your login or code.
- immediately change your password and notify the My Health Account Workforce Contact Centre on 0800 222 478 or +64 9 307 6155 if you believe the security of your password has been compromised or if you are aware of any unauthorised use of your username or password.

My Health Account Workforce will never contact you and request your password, HPI number (CPN), or access to your personal computer or other devices either by phone or email.

It is an offence to falsely claim to be a health practitioner under section 7 of the Health Practitioners Competence Assurance Act 2003 and could result in a conviction and fine not exceeding $10,000.

It is an offence to mislead an agency by impersonating an individual or falsely pretending to be an individual or acting under their authority for the purpose of obtaining access to that individual's personal information and could result in a conviction and fine not exceeding $10,000.

Anyone who knowingly accesses or uses, or attempts to access or use, any My Health Account Workforce or related Te Whatu Ora – Health New Zealand, Ministry of Health, or third-party provider service for an unlawful purpose (including, but not limited to, misrepresentation of your role in the New Zealand health workforce, fraud or attempted fraud or hacking or attempted hacking) may be liable to prosecution under New Zealand Law.

If you would like help with the My Health Account Workforce service, please email us at: support@identity.health.nz. If your support request relates to a digital health service from a third-party provider, please address your queries directly to them.

Privacy and how we use your information

You can choose how much information you provide to My Health Account Workforce, and the identity verification level you want. Some digital health services are restricted to higher verification levels, due to the nature of information they hold. We will guide you through your options.

We will securely hold and manage the information you provide to us through My Health Account Workforce. Your account allows you to decide how your My Health Account Workforce information may be managed.

My Health Account Workforce Privacy statement

Read our Privacy statement at My Health Account Workforce Privacy statement.

Disclaimer

Except where we have an explicit legal obligation under New Zealand legislation, we disclaim and exclude all liability for any claim, loss, demand, or damages of any kind whatsoever (including for our negligence) arising out of or in connection with the use of either this service or the information, content or materials included in this service or on any website we link to.

It is your responsibility to provide accurate information to us, and we are entitled to rely, without making further inquiry, on information provided by you or any third party you choose to interact with via this service.

Continuity of service

We will make reasonable efforts to always keep My Health Account Workforce operational, but we make no warranty or representation, express or implied, as to continuity of service. We reserve the right to suspend, terminate or otherwise alter access to some or all the services at any time and without notice if we consider that:

- this is necessary to maintain the integrity or security of related services; or
- your login is being misused or has otherwise been compromised; or
- you breach these terms; or
- we decide to remove or reduce the services available.

Changes to these Terms of use

We may revise these Terms at any time. Changes take effect when published to our website.

Security

You must not modify, distribute, alter, tamper with, repair, or otherwise create derivative works of My Health Account Workforce unless expressly permitted.

You must not reverse engineer, disassemble, or decompile the services or apply any other process or procedure to derive the source code of any software included in the services (except to the extent applicable law doesn't allow this restriction).

My Health Account Workforce has been, and will continue to be, subjected to independent security audits. If you discover a potential security vulnerability or suspect a security incident related to this service, please email itsecurity@identity.health.nz, or report it by following the disclosure process on the CERT NZ website.

Last updated: 30 March 2023

Appendix Five – Attributes that can be requested by Digital Health Services via My Health Account Workforce

Attribute	Description	Note
Unique ID	The unique identifier for the My Health Account Workforce holder.	Must be provided.
Email	The verified email address for the My Health Account Workforce holder.	Must be provided.
Identification Level	The Identification Level that the My Health Account Workforce holder has achieved by completing verification processes.	Must be provided if any attributes other than Unique ID and Email are requested.
Mobile number	The verified mobile number as supplied by the My Health Account Workforce holder.	
Given name	The account holder's optional given name, as recorded on the official document they supplied as evidence of identity on sign-up.	Available on accounts at Identification Level 2 and higher.
Middle name	The account holder's optional middle name, as recorded on the official document they supplied as evidence of identity on sign-up.	Available on accounts at Identification Level 2 and higher.
Family name	The account holder's family name, as recorded on the official document they supplied as evidence of identity on sign-up.	Available on accounts at Identification Level 2 and higher.
Nickname / Preferred name	The account holder's preferred name as set on the self-service profile page of My Health Account Workforce.	
Date of birth	The date of birth as recorded on the account holder's official document used as evidence of identity.	Available on accounts at Identification Level 2 and higher.
HPI number (CPN)	The HPI number (CPN) of the My Health Account Workforce holder.	Available on accounts at Identification Level 2 and higher.

Glossary

The following are definitions used in this Assessment:

Terms	Description, relationship, and business rules
Authorised Private Entity	An entity authorised to participate as a Service Provider in the health information sector after completing Onboarding processes established by Te Whatu Ora. This includes both providers of health services and health IT services.
Cloudcheck	This is the electronic identity verification service used to verify an identity document as part of My Health Account Workforce processes. More information can be found here: https://www.verifidentity.com/cloudcheck/
Consumer	An individual consumer of health services in Aotearoa.
Digital Health Service	A service or application offered by a Service Provider that has been Onboarded to use My Health Account Workforce as a Digital Health Identity provider.
Health Practitioner	A person who is, or is deemed to be, registered with an authority as a health practitioner of a particular health profession. An authority is a body corporate responsible for the registration and oversight of health practitioners of a particular profession under the Health Practitioners Competence Assurance Act 2003.
Health Provider Index (HPI)	The central national database for use by the New Zealand health and disability sector which uniquely identifies Health Practitioners, health provider organisations and facilities.
Health Workforce	The Health Workforce includes both Health Practitioners and Non-registered Workforce members who are working in Aotearoa New Zealand's health workforce, and who are aged 16 years or over.
Health Workforce Digital Identity	The identity information that is bound to a Health Workforce member's My Health Account Workforce.
Health Workforce member	Each User who registers to use My Health Account Workforce services as their unique work-related Health Workforce Digital Identity.
Health Workforce Terms of use	The terms that Health Workforce members must accept as part of signing up to use the My Health Account Workforce service.
Hira	This is a Te Whatu Ora initiative. It will be the national health information platform programme and will be designed to enable accessibility of health information from many sources and provide a range of digital services that make health information easier to access, use and share (with appropriate controls around privacy and security). Hira Website.
HPI number (CPN)	Also known as the Common Person Number (CPN). A unique identifier given to some Health Practitioners as part of Te Whatu Ora health identity processes. The HPI number (CPN) is a separate identifier given to the Health Practitioner and is recorded in the format NNXXXX where N is numeric, and X is alphabetic. It is different to the NHI number assigned to that person as a health Consumer.
Identification Level	The level of identification confirmed by My Health Account Workforce for the Health Workforce member, as further described in Appendix 1.
My Health Account	The Te Whatu Ora application that enables users to obtain, and assert, a digital health identity.
My Health Account Workforce	The Te Whatu Ora application that enables Health Workforce members to obtain, and assert, a Health Workforce Digital Identity.
Non-registered Health Workforce	Those individuals who are working in roles in Aotearoa New Zealand's health sector but who are not Health Practitioners.
Onboarding	The formal process (including the security and privacy aspects of the service or application) a potential connected Digital Health Service must complete prior to

Terms	Description, relationship, and business rules
	being permitted to use My Health Account Workforce services, which will include entering terms of use.
Privacy Statement Materials	Material to be prepared to inform Health Workforce members in compliance with relevant rules in the Health Information Privacy Code 2020, including rule 3 in particular.
RealMe® / RealMe® Verified	A Consumer-facing digital identity service for government agency use provided by the Department of Internal Affairs. More information at https://realme.govt.nz
Service Provider	A government agency (including Te Whatu Ora) or Authorised Private Entity that successfully completes the Onboarding process and is authorised for their Digital Health Services to connect with My Health Account Workforce to authenticate the identity of Health Workforce members.
Service Provider Terms of use	The terms that will apply to each Service Provider when allocated rights to connect to My Health Account Workforce services.
Te Whatu Ora – Health New Zealand	A Crown agent established under section 11 of the Pae Ora (Healthy Futures) Act 2022
Terms of use	See above **Health Workforce Terms of use**.
User	The individual Health Practitioner or Non-registered Health Workforce member who has obtained a My Health Account Workforce and uses it to interact with Digital Health Services.

Appendix 5 – Identification Levels of Confidence

For My Health Account User

Identification Level	What this level means to a My Health Account (Unified) member	Information that My Health Account stores	Options to achieve identification level
Level 1	You only need to provide an email address to sign up. You have very limited access to services at Level 1 because you still need to confirm who you are before accessing identifiable information.	Email address Preferred name (if provided) Mobile number (if provided)	Signing up to My Health Account will allow you to set up a Level 1 account.
Level 2	You have used your My Health Account verification with Cloudcheck to reach Level 2, or you have entered your details from one of the eligible identity documents or you have used information held by your general practice (GP) about you to verify who you are.	As per Level 1, plus: First name Middle name(s) (if you have them) Last name Date of birth HPI number (CPN) (if added) NHI added if matched	There are currently three options to achieve Level 2. One of these must be chosen: 1. My Health Account (health consumer) check if the account is verified to Level 2 2. Identity document check 3. Healthcare provider check
Level 3	This level involves checking that it is really you that has created your account, and the right person has been connected to your Account.	As per Level 2, plus: HPI number (CPN) (if added)	There are currently three options to reach Level 3: 1. Use of your RealMe® Verified account 2. Use of the My Health Account (health consumer) check if your account is verified to Level 3 3. The combination of the Identity document check and the Healthcare provider check

For Digital Health Services authorised to Onboard with My Health Account Workforce

Identification Level established by My Health Account Workforce User	What this Identification Level represents to a Digital Health Service about a My Health Account (Unified) User	Information that My Health Account can share at that Identification Level (as approved during the Onboarding process)	My Health Account authentication of identity scope associated with this Identification Level
Level 1	This confirms only that the My Health Account User has a verified email address that has not been used by any other User.	Email address Preferred name (if provided) Mobile number (if provided)	Level 1 identification does not confirm the identity of the User.
Level 2	This confirms the My Health Account User has a verified email address, and that the User has established a Health Workforce Digital Identity in only one of the following ways: • Attributes: The User has presented an identity document that is verified as matching the User Account name and Date of Birth; OR • Authenticate: The User has been able to verify they have access to a device recorded in Te Whatu Ora records as belonging to a person with the User name. If an HPI number (CPN) is recorded this will have been verified against the Health Provider Index records held by Health New Zealand as correct for the person with that User name.	As per Level 1, plus: First name Middle name(s) Last name Date of birth HPI number (CPN) (if added) NHI if matched	Level 2 confirms EITHER that a User's name and date of birth has been confirmed with a document verification process OR that the User has access to a device known to belong to the named person. If a Health Practitioner adds their HPI number (CPN) to their account, Level 2 confirms that there is a match between the Health Practitioner and the HPI number (CPN) provided. Level 2 is not sufficient to authorise any Health Workforce member User to access a Digital Health Service that contains identifiable health information about a Consumer. The Digital Health Service is responsible for: 1. ensuring any onboarded Health Workforce member has an appropriate Identification Level 2. meeting all role-based access control requirements 3. confirming that a Health Practitioner's annual registration is current.
Level 3	This level confirms that the My Health Account Workforce User has: • both Verified their name and date of birth attributes via a recognised identity	As per Level 2, plus: HPI number (CPN) (if added)	Level 3 confirms the person has established their Health Workforce Digital Identity, and an HPI number (CPN) connected to that Health

	document and authenticated their identity with a device known to be possessed by the User of that name; OR • confirmed their identity with RealMe Verified Services. If an HPI number (CPN) is recorded this will have been verified against the Health Provider Index records held by Health New Zealand as correct for the person with that User name.		Practitioner (if one is provided). The Digital Health Service is responsible for: 1. ensuring any onboarded Health Workforce member has an appropriate Identification Level 2. meeting all role-based access control requirements 3. confirming that a Health Practitioner's annual registration is current. .

Appendix 6 – Approved Connected Live Applications

Website: https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/my-health-account/integrated-digital-health-services

Digital health services integrated with My Health Account for consumer access

- My Health Record
- Manage My Health
- Pacific Health Scholarships
- Piki Te Ora
- Tātai Iwi Affiliation Collection
- Te Pitomata grants
- MedicAlert

Digital health services integrated with My Health Account Workforce for health workforce, healthcare professionals and businesses

- Tuhi
- Provider View
- Vountary Bonding Scheme
- Health Advisory and Regulatory Platform (HARP)
- Workforce Requests
- Aotearoa Immunisation Register (AIR)
- NZ Health Terminology Services (NZHTS)
- ACC Provider Hub
- Assisted Dying Service
- Student Placement Service