

My Health Account

Privacy Impact Assessment

Date: 3 May 2024

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

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

CONTENTS	3
SECTION ONE – EXECUTIVE SUMMARY	5
SCOPE OF ASSESSMENT	6
ASSESSMENT CONTENT	6
RECOMMENDATION SUMMARY	6
SECTION TWO – MY HEALTH ACCOUNT	9
BACKGROUND	9
MY HEALTH ACCOUNT	9
INFORMATION FLOWS INVOLVED IN MY HEALTH ACCOUNT PROCESSES:	11
INFORMATION COLLECTED	12
SIGN-UP	12
IDENTITY DOCUMENT CHECK	12
HEALTHCARE PROVIDER CHECK	12
ACCOUNT UPLIFT PROCESS	13
REALME® VERIFIED	14
ADDING NHI NUMBER	14
ADDING HPI NUMBER (CPN)	14
PARENT-TO-CHILD / CHILDREN RELATIONSHIPS	15
OTHER PERSONAL INFORMATION	16
COOKIES	17
STATISTICAL INFORMATION	17
AUDITING	17
INFORMATION STORAGE	17
INFORMATION UPDATES / CORRECTION	18
INFORMATION USE AND SHARING	18
ONBOARDING DIGITAL HEALTH SERVICES	18
CONSENT AND SHARING ATTRIBUTES	19
ANALYTICS AND REPORTING	19
INFORMATION DELETED OR MADE INACTIVE.	20
PROCESS FOR MANAGING INFORMATION COMPROMISE	21
GOVERNANCE	22
SECTION THREE – PRIVACY ANALYSIS	23
APPENDIX ONE – IDENTIFICATION LEVELS	30
APPENDIX TWO – RETENTION OF PERSONAL INFORMATION	31
APPENDIX THREE – MY HEALTH ACCOUNT PRIVACY STATEMENT	33
APPENDIX FOUR – CONSUMER TERMS OF USE	40
APPENDIX FIVE – ATTRIBUTES THAT CAN BE REQUESTED BY DIGITAL HEALTH SERVICES VIA MY HEALTH ACCOUNT	43

Section One – Executive Summary

1. My Health Account is the digital health identity service originally developed by the Ministry of Health (the Ministry). Post 1 July 2022 My Health Account was transferred to and is now operated by Health New Zealand | Te Whatu Ora ¹.
2. Health New Zealand aims to enhance Consumers' 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.
3. To allow Consumers to access these digital health services, Health New Zealand first needs to accurately identify Consumers. My Health Account enables health consumers to confirm who they are digitally and engage with online healthcare services.
 - 3.1. The initial use case for My Health Account enabled Consumers to view and confirm their COVID-19 vaccination status and test results. It will shortly expand to include access for Consumers to dispensed medicines, laboratory results and some primary care information (with My Health Record).
 - 3.2. My Health Account now integrates with several approved Digital Health Services to provide the identity component of service access (those current at the date of issue of this PIA are listed on the [My Health Account website](#)).
4. 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.
5. Te Whatu Ora carefully balances these potential privacy risks against the public health benefits of letting Consumers access their health records using My Health Account. Consumer trust is essential to achieve widespread use of My Health Account. Health New Zealand is working hard to earn and retain high levels of public trust.
 - 5.1. Health New Zealand intends to retain Consumer choice, collecting only the essential personal information required to uniquely identify Consumers online, and limit who will have access to that information.
 - 5.2. Information about Consumers who choose to use My Health Account Services is stored by Health New Zealand and will not be shared with any other agencies (Government or otherwise) unless explicit Consumer consent is obtained, or it is authorised by law.
 - 5.3. Consumers are asked for their permission before their information is shared via My Health Account with connected digital health services. Consumers can view a list of all digital health services they have previously given permission to access their information. Consumers can remove these permissions at any time via My Health Account.

¹ Health New Zealand | Te Whatu Ora 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.

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. The comments were considered initially by the Ministry and subsequently by Health New Zealand, and then included as Health New Zealand saw appropriate.
7. 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

8. The current Assessment covers:
 - 8.1. The personal, demographic, and anonymous² information to be collected from the Consumer to create a My Health Account.
 - 8.2. My Health Account's identity confirmation role for connected digital health services or applications.
9. This Assessment does not address:
 - 9.1. 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.
 - 9.2. the decision-making process, approvals, nor the conclusions reached about the decision to create My Health Account services.

Assessment content

10. Section Two contains the Description of the Service and Information Flows.
11. Section Three contains the Privacy Analysis.

Recommendation Summary

12. 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 Consumers. Individual Consumers can choose the identification level they wish to apply to their account.
 - 12.1. My Health Account is a 'doorway' to approved digital health services and applications. Health New Zealand carefully oversees how My Health Account

² Consumers 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.

12.2. 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.

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

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

Recommendations:

14. 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	<p>Complete any Health New Zealand security assessment requirements including Certification and Authorisation, and independent security testing. This has occurred prior to each release to date.</p> <p>If any risks are identified, they will be resolved or mitigated to ensure appropriate security is applied to all aspects of the service.</p> <p>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. Consumers can reasonably expect that Health New Zealand 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 Record.</p>	Ongoing - Prior to go-live of any new feature release of substance.
PIA-02	<p>Clear Privacy Statement Materials are developed and made available via My Health Account. The current version is attached in Appendix Three.</p> <p>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).</p> <p>Health New Zealand 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.</p>	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 additional services

	Any connected digital health services must also incorporate a relevant Privacy statement for those services as part of the Consumer onboarding processes.	
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 has developed, and access to more detailed identifiable health information will soon become available through My Health Record and other connected services, the My Health Account and Hira processes have been 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.	A technical solution removing the accounts created when a person was aged between 12 and 15 years old is being implemented. It will be in place 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.	Ongoing governance oversight
PIA-07	<p>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, and then view some of their child's health information. In order to protect the autonomy of the child, the parents view access to the child's record will cease once the child turns 12.</p> <p>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.</p>	<p>Removal of parental access to the child's health records once they turn 12 will be implemented prior to the extension of the health information that will be displayed. This will be before the addition of 'dispensed medication' details for linked children in My Health Record.</p> <p>Address redaction action to be finalised prior to go-live in each case of additional services</p>

Section Two – My Health Account

Background

My Health Account is a digital health identity service that enables Consumers of New Zealand health-related services (both health consumers and health workforce members³) 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.

Consumers 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 Consumers 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. Consumers 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 Consumers when creating a My Health Account. My Health Account can be accessed from <https://identity.health.nz>.

³ Noting that the health workforce facility will be removed in the near future when the new My Health Account Workforce is released.

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

Consumers 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 Health Record, refers them to My Health Account to establish their identity and Identification Level.

Before signing up to My Health Account, Consumers are provided links to the Privacy statement⁴ and Consumer Terms of use⁵. 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 guidance⁶.

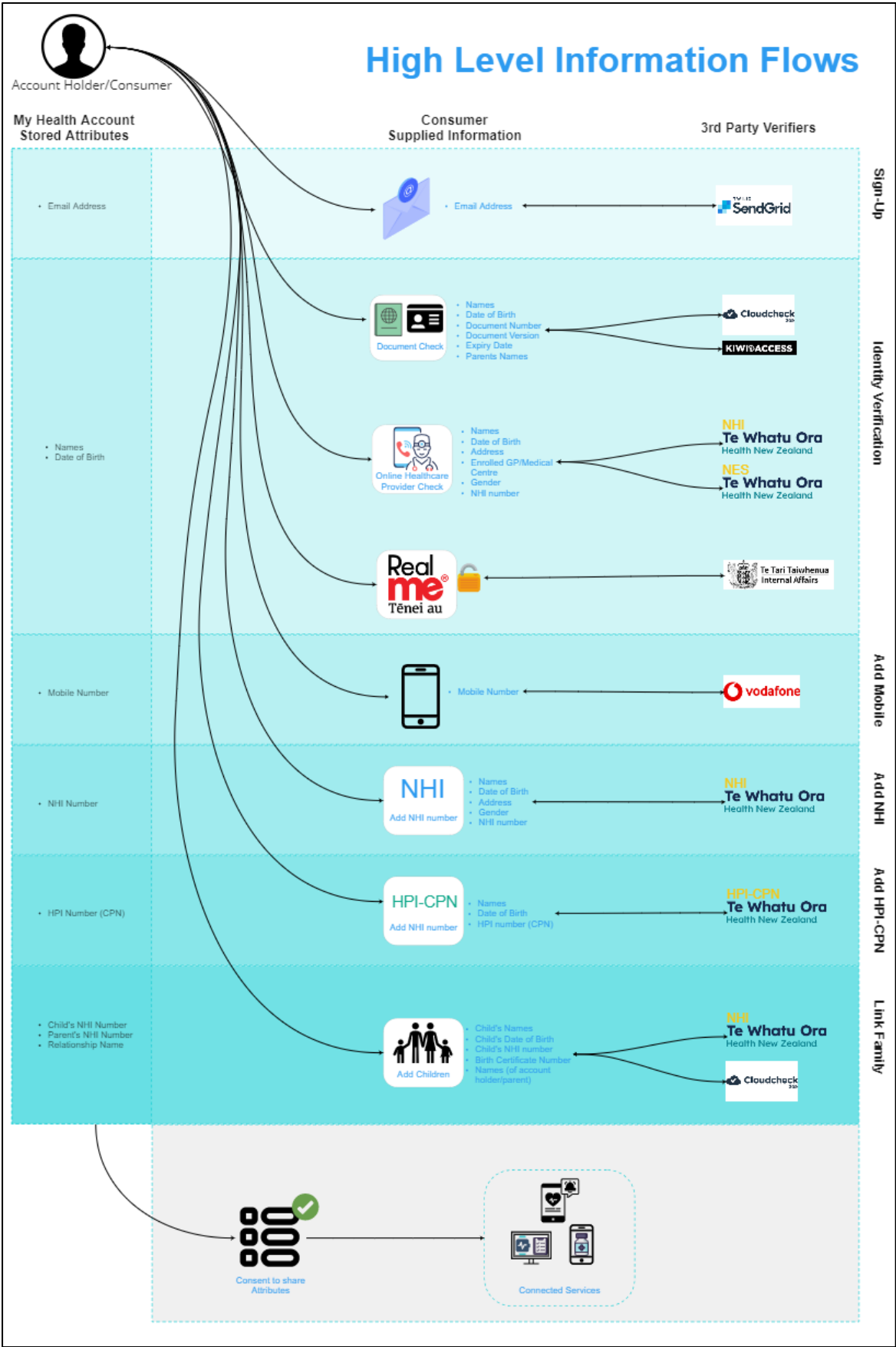
Before Consumers can use My Health Account, their identity must be verified. This verification process involves several steps, and the 'Identification Level' achieved reflects the increasing assurance that can be placed on each step. The Consumer can stop progressing through the identity verification 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](#).

⁴ <https://www.tewhatauora.govt.nz/our-health-system/digital-health/my-health-account/privacy-statement>

⁵ <https://www.tewhatauora.govt.nz/our-health-system/digital-health/my-health-account/terms-of-use>

⁶ Advice on creating your My Health Account: <https://www.tewhatauora.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.tewhatauora.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

Consumers 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 Consumers of My Health Account are required to provide a unique email address as part of their sign-up process. For those Consumers 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 Consumers 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. Consumers have 20 minutes to enter the TOTP into My Health Account to validate that they have access to the email account.

Consumers will shortly only be able to set up their own account once they attain 16 years of age (and Privacy Statement materials and Terms of Use will be updated to reflect this change).

Identity Document Check

Consumers can claim identity information in My Health Account by [verifying an official document](#), such as a Passport or Driver Licence⁷. Consumers 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 services⁸ to ensure that there is a record of an official document that matches the details provided⁹. 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 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

Consumers can choose to verify their identity using information already held about them in Health New Zealand records. Consumers are required to provide information about themselves including their name, date of birth, address and the General Practice or Medical

⁷ The [identity documents](#) that can be used for verification are listed on the Te Whatu Ora My Health Account website.

⁸ Third-party services are [Cloudcheck](#) from Verifi and a Kiwi Access Card verification service from CentraPass.

⁹ 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/>.

Centre with which they are currently enrolled. They also have the option to provide their gender and NHI number.

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)¹⁰. 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.

Account Uplift Process

There are a number of individuals currently at My Health Account Identity Level 2N who may have challenges meeting the current verification processes to achieve Level 3N.

A total of 3.5 million accounts are now linked to unique individuals. Currently only 6%, or 320,000 of the population have reached Level 3N confidence level, while 3.11 million remain on Level 2N. Of those accounts over 87,000 individuals attempted to match to Level 3N but failed.

If an account meets the following criteria – the user has established their My Health Account, successfully matched their NHI, and have a unique email that matches the email held by NES for the relevant NHI account - an alternative verification method will be offered as part of a one-off 'Data Driven Uplift Programme'.

The current requirement is to respond to a code sent to your National Enrolment Service (NES) registered mobile. This will be replaced with a code sent to the person's NES registered email – where it has been established that NES email matches the unique email used to establish the My Health Account. The next time the Level 2N user meeting the criteria logs in to their My Health Account they will be invited to perform a time-limited One Time Passcode (TOTP) process – via the NES recorded email address – if they wish to be uplifted to Level 3N.

This process will apply to approximately 1 million My Health Accounts, who may then choose to 'uplift' to Level 3N¹¹.

¹⁰ 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.

¹¹ The My Health Account team will continue engagement with the HISO team to update HISO 100046:2023 Consumer Health Identity Standard to reflect this change.

RealMe® Verified

Consumers who have signed up via a RealMe¹² 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

Consumers 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 record¹³ 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

¹² 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/>.

¹³ 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'.

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.

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

When creating the legacy account entries with CPN, My Health Account used the verified information (names and date of birth) stored against the Consumer's record to search for a matching HPI record. Consumers provided the HPI number (CPN) but could edit the name information 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 was identified, the HPI number (CPN) for the HPI record was stored against the Consumer's My Health Account record.
- If a uniquely-matching HPI record could not be identified, the Consumer was provided with advice on how they could try again.
- If the Consumer provided a different name as part of the matching process, this information was not stored against their My Health Account record.
- An HPI number (CPN) could only be linked to a single My Health Account record.

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. Once the child attains the age of 12 years My Health Account will 'de-link' the parent authority over the account in terms of information to be shared. There will still be a record of the parent child relationship held with the NHI record, but health information will no longer display to the parent for that child.

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](tel:0800222478) or [+64 9 307 6155](tel:+6493076155) 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

Consumers 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

Consumers can choose to add a Mobile number to their My Health Account. Consumers 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, Consumers 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. Consumers 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

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 Consumer personally.

Auditing

My Health Account records all activity against all Consumer 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.

Audit records will be held for a minimum period of seven 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 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 Health New Zealand 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 Consumers 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. Health New Zealand 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 Consumers to access their My Health Account whenever they need it.

Information Updates / Correction

Consumers 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)

Consumers 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 Consumers 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 Consumers 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 Consumers 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

- correctly applying the Identification Level applicable to the information to be made available (Level 3 for access to identifiable health information)
- meeting security assurance requirements.

The Te Whatu Ora website lists the [connected Digital Health Services currently available](#) to Consumers via My Health Account.

Consent and Sharing Attributes

Once a connected service is made available for consumers to access using their My Health Account, Consumers must choose to interact with a Digital Health Service before any information about the Consumer is shared with it. Consumers 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).

Consumers 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 Consumers 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 Consumers 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) to understand where in the community access to digital health information can be improved. Any reports use aggregated data and cannot be used to identify Consumers personally.

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

Information Deleted or made Inactive.

Consumer request - Inactivate Account:

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 limited administrative access. The information required for audit purposes, in compliance with the Public Records Act, will be retained for a seven-year period. Other information will be deleted.

- 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.

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. Consumers 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.

Death of account holder:

My Health Account may identify the death of an individual from NHI records. Upon notification of the death of an account holder, their account is inactivated for a period of two years prior to closure, and subsequent deletion of the record in accordance with the Public Records Act requirements. After the consumer's death there will be no further access via that consumer's account (including by any delegate if they had access prior to the consumer's death). Executors for the deceased person can request access to information about the deceased person via an assisted channel or directly from the information source if necessary.

Administrative account activity:

The My Health Account operations team may initiate the closing of an account and / or deletion of information¹⁴, 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).

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.

¹⁴ Subject to audit requirements or the requirements of the Public Records Act

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.

Youth Accounts

During the peak COVID period My Health Account permitted youth accounts to be set up for young people aged between 12 and 15 years old. Their parents were able to set up these accounts on behalf of those young people, potentially without the knowledge of those young people¹⁵. As services using My Health Account as the digital identity component will soon offer more detailed medical information, these youth accounts are to be deactivated by My Health Account. If the accounts were not deactivated, parents could potentially review the young person's information without their consent (such as the contraceptive medication dispensed to a 15 year old).

Health New Zealand consulted with the Office of the Privacy Commissioner, and has determined that the following steps will be taken to balance the privacy risk of incorrectly disclosing health information about a young person to a parent, with the inconvenience of being required to create a new account for the young person.

- All accounts created when the person was under 16 years of age at the time of creation will be deactivated.
- The NHI and email address (and other related audit information) will be removed to a secure storage location within the My Health Account environment.
- The NHI and email address (or an alternative email address) will be able to be used to create a new My Health Account for the young people (or they may use a new unique email address of their choosing).
- Only young people of at least 16 years of age will be able to establish a My Health Account for themselves.
- Appropriate messaging and assistance will be provided to explain the change and assist the young people to create their own accounts.
- Previous Privacy Statement and Terms of Use messaging will be updated to capture the new requirements.

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

¹⁵ Approximately 180,000 accounts were created for 12 to 15 year olds, with approximately 900 at Level 3N.

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 Commissioner¹⁶.
- 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 Consumers are aware of the seriousness of misrepresenting their identity or assuming the identity of another. Consumers 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 Consumers 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 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.

¹⁶ 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 verify that their applications or services comply with the agreed Identification Level expectations set by My Health Account.

Health Information Privacy Code Rules		Background and Key Controls	Residual risk
Rule 1	<p>Purpose of collection of health information</p> <ul style="list-style-type: none">- Only collect health information if you really need it	<p><i>Purpose</i></p> <p>My Health Account's purpose is to enable Consumers to verify their identity information to the level required to access the digital health services with which they wish to engage.</p> <p><i>Necessary</i></p> <p>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.</p> <p>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.</p> <p>To access services that require a higher Identification Level, it is necessary for Consumers 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:</p> <ul style="list-style-type: none">• Name* (including given and family names)• Date of Birth* <p>In addition, depending on the verification method or process selected, Consumers may need to provide additional information, such as:</p> <ul style="list-style-type: none">• Document type*• Document number	Low

		<ul style="list-style-type: none"> • 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* <p>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).</p> <p>Adding an NHI number or HPI number (CPN) to a My Health Account is optional, but necessary if Consumers wish to engage with connected Digital Health Services that do not have the ability to locate those identifiers themselves.</p> <p>Adding a mobile number is an option for Consumers 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.</p>	
Rule 2	<p>Source of information</p> <ul style="list-style-type: none"> - Get it straight from the people concerned 	<p>My Health Account is an 'opt-in' service with the Consumer supplying most information directly to My Health Account themselves, except for:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ 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). <p>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.</p>	Low
Rule 3	<p>Collection of information from individual</p> <ul style="list-style-type: none"> - Tell them what you're going to do with it 	<p>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.</p> <p>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 Consumers 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.</p> <p>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</p> <p>In addition, advice and guidance can be found on the My Health Account website, providing additional context about some My Health Account features.</p> <p>Updates are included in the current draft of the Privacy Statement and Terms of Use in relation to the removal of the youth accounts.</p>	Low

Rule 4	<p>Manner of collection of information</p> <ul style="list-style-type: none"> - Be considerate when you're getting it 	<p>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. At this time My Health Account will move to requiring an individual to be 16 years old before they can open their own account.</p> <p>Historically, for reasons associated with the Covid-19 pandemic, My Health Account permitted those aged over 12 years to create their own account (or their parent to create an account on their behalf). These accounts will now be deactivated, and the young person required to establish their own account after they turn 16.</p> <p>The legacy impact of My Health Account Covid settings is that the accounts of the 12- to 15-year-olds may be in the control of the parents. The parents could have, legitimately, reached Level 3N for their children's accounts. The impact of this would be that when My Health Record starts to display medicines dispensed (due in late May) or summary GP data or laboratory test results (due by the end of June), those parents would be able to see those results in relation to their children.</p> <p>Exposure of these details of the young person's medical encounters may be against the young person's interests or wishes. Obvious examples may include sexual health matters or contraceptive advice and medication. Many of these young people may have no awareness that their parents have access to My Health Account in the young person's name.</p> <p>Section 22F(1) of the Health Act provides that <i>'Every person who holds health information of any kind shall, at the request of the individual about whom the information is held, or a representative of that individual, or any other person that is providing, or is to provide, services to that individual, disclose that information to that individual or, as the case requires, to that representative or to that other person.'</i></p> <p>The interpretation provisions of the Health Information Privacy Code (HIPC) provide that a 'representative' means <i>'where the individual is under the age of 16 years, that individual's parent or guardian'</i>.</p> <p>Rule 11(5) of the HIPC provides that any such request must be treated as if it were a privacy request made under Rule 6. But it has an important caveat (also reflected in clause 22F(2) of the Health Act). The health agency requested to provide the information <i>'may refuse to disclose the information to the representative if (i) the disclosure of the information would be contrary to the individual's interests, or (ii) the agency has reasonable grounds for believing that the individual does not or would not wish the information to be disclosed, or (iii) there would be good grounds for withholding the information under Part 4 of the Act if the request had been made by the individual concerned.'</i></p> <p>Some younger individuals are capable of making their own decisions about receiving or not receiving clinical treatment (for example Gillick competency – a factual decision in relation to the individual child). There are similar expectations about what medical information they might or might not choose to share. Current practices would involve the parent requesting access from the clinician, who could then make a choice whether it was appropriate to release the information, or not.</p> <p>In order to achieve a balance between autonomy of children, and their ability to manage their own healthcare in the digital environment enabled by My Health Account, the following age restrictions will apply:</p> <ul style="list-style-type: none"> • Account establishment for a person's own account will start at age 16. The Human Rights Act 1993 provides that the prohibited grounds of discrimination include age (but commencing with 16 years of age – s21(ii)). • Linked children's accounts will permit ongoing for parents access until the child turns 12, and the link will then be deactivated. • Accounts established for 12- to 15-year-olds will be deactivated, and those young people will then be able to follow standard account development processes once those individuals reach 16 years of age. • Alternative processes will be considered in the future for the individuals who are aged between 12 and 15 - noting that existing channels for 	Low
--------	--	---	-----

		<p>obtaining information and services will continue to exist outside the My Health Account digital environment.</p> <p>The Privacy statement and Terms of use previously confirmed 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. These documents will be updated to remove this option, as there will now be sensitive health information available via My Health Record as it was necessary to remove full access for a parent to accounts to prevent information being displayed to a parent where the child may not be aware that the parent had that access.:</p> <p>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 Consumers.</p> <p>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).</p>	
Rule 5	<p>Storage and security of information</p> <ul style="list-style-type: none"> - Take care of it once you've got it 	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>All account access and all account updates or changes by Consumers 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 Consumers 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.</p>	Medium
Rule 6	<p>Access to personal information</p> <ul style="list-style-type: none"> - People can see their health information if they want to 	<p>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.</p> <p>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.</p>	Low

Rule 7	<p>Correction of information</p> <ul style="list-style-type: none"> - They can correct it if it's wrong 	<p>Consumers can correct some information about themselves directly within My Health Account. For other information, Consumers 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.</p>	Low
Rule 8	<p>Accuracy etc. of information to be checked before use</p> <ul style="list-style-type: none"> - Make sure health information is correct before you use it 	<p>Accuracy is very important to the allocation of the unique digital health identity that will be associated with each My Health Account.</p> <p>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, to obtain the mobile number to send a one-time-code to (or in the case of the Data Driven Uplift Programme – confirmation of the email on the NES is the same as that used to set up My Health Account). This should assist with accuracy in assigning a correct identity to the relevant My Health Account.</p> <p>The Data Driven Uplift Programme used a series of analytical measures to determine the appropriate accounts that could be expected to follow a similar process to the Healthcare Provider Check – exchanging the mobile phone register with NES for the email – to confirm the One Time Passcode. The equity need of increasing the opportunity for individuals to have access to an account was balanced to a level Health NZ considered reasonable in terms of the accuracy of the identification of the individuals.</p> <p>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 Consumer 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. Consumers also have the option of specifying a Preferred name on their profile, which can be shared with Digital Health Services.</p> <p>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.</p> <p>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.</p>	Low
Rule 9	<p>Retention of information</p> <ul style="list-style-type: none"> - Get rid of it when you're done with it 	<p>Only information necessary for the effective administration of the account will be retained. A summary of the information retained is recorded in Appendix Two.</p> <p>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 as an audit record of activity related to their files.</p> <p>Consideration will be given to the method of notifying the cessation of a delegate account after the death of the individual (to avoid the account closure bluntly informing the delegate of the death).</p> <p>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.</p>	Low
Rule 10	<p>Limits on use of information</p> <ul style="list-style-type: none"> - Use it for the purpose you got it 	<p>The purpose of My Health Account is to allow Consumers 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:</p>	Low

		<ul style="list-style-type: none"> Digital Health Services must pass various security testing and compliance requirements before Consumers 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 Consumers 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 Consumers for their permission to share their attributes Consumers can revoke their permission to share attributes with a Digital Health Service at any time. <p>Consumers 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.</p>	
Rule 11	<p>Limits on disclosure of information</p> <ul style="list-style-type: none"> Only disclose it if you have good reason 	<p>The disclosure enabled via My Health Account during the verification process is signalled in advance to Consumers, who may then choose to proceed with the disclosures (for example, to Cloudcheck or other authorised third-party identity services).</p> <p>The information disclosed to Digital Health Services about Consumers 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.</p> <p>In addition, Consumers 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.</p> <p>Other 'enabling' services (such as Hira Digital Services Hub and My Health Record) must be required to fully address disclosure implications for information to be made available via the apps, to make sure any authorisation matches the My Health Account Identification Levels.</p> <p>The Rule 11(5) obligations in terms of s22F of the HIPC have been addressed for young people (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). Accounts for 12- to 15-year-olds who may have had the assistance of their parent to establish their My Health Account will now need to create their own accounts when they turn 16 (and previous accounts will be deactivated). This gives the young people the opportunity to decide to share information with their parent if they wish to.</p> <p>The 'Add a child' feature will allow information to be displayed until the child turns 12 years old and will then stop automatically displaying the details to the parent who has linked to that child's information. Parents will still be able to follow existing processes of requesting information from care providers if required, and appropriate, outside the MHA processes.</p> <p>It is also noted that there may be some instances of children younger than 12 accessing health services without a parent, where it may be in their best interests that the information is not shared automatically with the parent. This may require training for health professionals to enable them to mark records as confidential to limit exposure of sensitive information for those under 12 years of age.</p> <p>As this 'add a child' feature enables access by some parents to some information about their young children, it 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</p>	Low

		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 confidential 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.	
Rule 12	Disclosure of personal information outside New Zealand	<p>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).</p> <p>There will be no disclosure of information made outside New Zealand under the rules identified in Rule 12 for My Health Account.</p>	Low
Rule 13	<p>Unique identifiers</p> <ul style="list-style-type: none"> - Only assign unique identifiers, where permitted 	<p>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.</p> <p>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).</p> <p>All parties interacting with My Health Account (other than Consumers) will be consistent with Schedule 2 of the HIPC.</p> <p>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.</p> <p>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.</p>	Low

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	<p>Captured at the point of attempting to confirm identity using the healthcare provider check. Information is not retained by My Health Account.</p> <p>May be requested during an attempt to add an NHI number to an account. Information is retained until the NHI number is successfully added.</p>
Gender	<p>Captured at the point of attempting to confirm identity using the healthcare provider check. Information is not retained by My Health Account.</p> <p>May be requested during an attempt to add an NHI number to an account. Information is retained until the NHI number is successfully added..</p>
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	For the duration of the relationship (or until changed or removed by the Consumer or Administrator).

NHI, child/relationship nickname, expiry date)	Note: Deleting the My Health Account that established the relationship does not delete the relationship information which is held against the NHI of each party.
Audit records	<p>For a minimum of five years from creation of each record and when no longer required for business purposes and legal requirements.</p> <p>Note: 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.</p>

Appendix Three – My Health Account Privacy statement

Privacy statement

Effective 1 May 2024

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.

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. Our rules have recently changed, and we have removed accounts historically created for 12- to 15-year-olds. These young people can create their own new accounts once they reach 16.
- 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](#).
- We will also provide a one-off opportunity to some individuals with a Level 2N account if have created their account with an email that matches the email held by the general practice they are enrolled with (if the account holder chooses to respond with the one-time password sent to them).

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 (or, in limited circumstances, to the email) that your general practice has on their records.

If you have that mobile phone, (or email) 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 New Zealand 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
- 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
- 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.

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, 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 Health New Zealand | Te Whatu Ora 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 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 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
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, will be collected.

Giving feedback

- Phone: [0800 222 478](tel:0800222478) or [+64 9 307 6155](tel:+6493076155) 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 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 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](#).

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 Health New Zealand | Te Whatu Ora. 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 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 Health New Zealand.

What you are agreeing to

By accepting these terms, you understand and agree:

- you are aged 16 years or over.
- 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, 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 Health New Zealand | Te Whatu Ora, 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 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.

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: 1 May 2024

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.

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 Health New Zealand 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 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.
<u>Consumer Terms of use</u>	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 <u>uniquely identifies</u> 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 New Zealand 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). <u>Hira Website</u> .
<u>HPI number (CPN)</u>	Also known as the Common Person Number (CPN). A unique identifier given to some Health Practitioners as part of Health New Zealand 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.

Terms	Description, relationship, and business rules
Ministry	Manatū Hauora – the Ministry of Health.
My Health Account	The Health New Zealand application that enables Consumers to obtain, and assert, a digital health identity.
My Health Record	The Health New Zealand consumer channel and interface for consumers using My Health Account to access Health New Zealand-held digital health information and available services for themselves or their authorised whānau.
My Health Account Workforce	The Health New Zealand 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 Consumers 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 Health New Zealand) or Authorised Private Entity that successfully completes the Onboarding process and is authorised to use My Health Account to authenticate Consumers in order to provide healthcare services and / or support health information management by Consumers.
Service Provider Terms of use	The terms that will apply to each Service Provider when allocated rights to connect to My Health Account services.
Health New Zealand Te Whatu Ora	A Crown agent established under section 11 of the Pae Ora (Healthy Futures) Act 2022.

National Privacy Office

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

Name: Viv Kerr – Health NZ Head of Privacy

Signature: _____

Date: 09 / 05 / 2024

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: Michael Dreyer – Health NZ Director Sector Digital Channels

Signature: _____

Date: 9 / 5 / 2024

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: Joel Brown – Health NZ Group Manager, Health Identity and Eligibility

Signature: _____

Date: 9 / 5 / 2024