Te Whatu Ora
Health New Zealand

My Health Account

Privacy Impact Assessment

Date: 1 February 2023

Te Whatu Ora
Health New Zealand

Document Approval

	Name/Title	Sign-off date
Approved by Senior Responsible Officer	Gerard Keenan	26/01/23
Approved by Chief Privacy Officer, Te Whatu Ora	Viv Kerr	01/02/23

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

Disclaimer

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

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

Contents

Section One – Executive Summary

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

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

3. To allow Consumers to access to these digital health services, Te Whatu Ora first needs to accurately identify Consumers. Only the right person should be able to access and manage information about themselves. My Health Account confirms that a person is who they say they are, for approved health sector applications and services, then links the right person to the right information.

   3.1. The initial use case for My Health Account meant Consumers were able to view and confirm their COVID-19 vaccination status and test results with My Covid Record.

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

   3.3. Further services will be added over time and recorded on the My Health Account website to keep Consumers informed.

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 has put a lot of effort into minimising any potential privacy risks when developing My Health Account. Te Whatu Ora carefully balances these risks against the public health benefits of letting Consumers access their health records. Consumer trust is essential to achieve widespread use of My Health Account. Te Whatu Ora is working hard to earn and retain high levels of public trust.

   5.1. Te Whatu Ora 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 Te Whatu Ora and will not be shared with any other agencies (Government or otherwise) unless explicit Consumer consent is obtained, or it is authorised by law. Use of information by Service Providers will either be authorised by Consumers or under legal authority (such as in compliance with the rules in the

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

Health Information Privacy Code 2020 and other enactments that require or allow information to be used or disclosed).

5.3. Consumers are asked for their permission before their information is shared via My Health Account with 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.

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

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 anonymous[2] information to be collected from the Consumer to create a My Health Account.

8.2. My Health Account's identity confirmation role for associated digital health applications or services.

9. This Assessment does not address:

9.1. any further digital health applications or services 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.

10. It is instead focused on the collection, storage, use and sharing of personal information for the purposes of providing My Health Account authentication and identity assertion services.

Assessment content

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

[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.

12. Section Three contains the Privacy Analysis.

Recommendation Summary

13. My Health Account is a voluntary identity service, enabling individuals to opt in to having 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.

    13.1. My Health Account is a 'doorway' to approved digital health services and applications. Te Whatu Ora carefully oversees how My Health Account controls are managed within other services (via its onboarding process) and how Consumer control can be retained from within their My Health Account.

    13.2. 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.

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

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

Recommendations:

15. 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 – Second Privacy Assessment (IPA)	Planned Date for completion
IPA-01	Complete any Te Whatu Ora security assessment requirements including Certification and Authorisation, and independent security testing. This has occurred prior to each release to date. If any risks are identified, they will be resolved or mitigated to ensure appropriate security will be applied to all aspects of the service. It is important that security measures are applied across the end-to-end services available via My Health Account to maintain trust in the service, as it is a gateway to those other services. Consumers can reasonably expect that Te Whatu Ora will maintain oversight of all interconnected services (via the onboarding process), and not offer them unless security is assured. These matters, however, will be potentially outside the direct control of My Health Account so communications and oversight must remain strong with other interconnected projects, such as Hira.	Ongoing - Prior to go-live of any new feature release of substance
IPA-02	Clear Privacy Statement Materials to be developed and made available via My Health Account. The current version is attached in Appendix Three. This Statement includes reference to linked digital health services permitted to integrate with My Health Account and includes full service details on a separate My Health Account web page (linked	To be finalised in each case prior to any go-live of a new release (each updated Privacy Statement to change the

	from the Privacy statement to prevent the length of the Privacy statement becoming unwieldy). Te Whatu Ora is planning to modernise providing future updates to Privacy statement materials – whether by banner notification within the My Health Account application or by direct email to all email addresses verified by My Health Account processes.	Effective Date recorded at the top of the Privacy statement on the website)
IPA- 03	The Onboarding process will be reviewed to ensure that the applications will operate at an identification level appropriate with My Health Account settings. Any linked digital health services must also incorporate a relevant Privacy statement for those services as part of the Consumer onboarding processes.	To be finalised prior to go-live in each case of additional services
IPA-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
IPA-05	As Hira develops, and access to more detailed identifiable records potentially become available, then My Health Account and Hira processes will need to be carefully considered in relation to the accounts of the 12 to 15-year-olds who may initially have had parental assistance to set up their accounts. Te Whatu Ora will need to develop a process and safeguards to ensure if / when parents assist a child to create an account (and hold credentials to access the child's account) that there is regular review, and the subsequent opportunity for the children (particularly as they age) to control access to their own information.	Policy work is underway – to be completed prior to expanded access to clinical records is made available
IPA-06	Strong governance is required to ensure that My Health Account and any connecting services remain consistent with the My Health Account expectations set out in this Privacy Impact Assessment. The transition to Te Whatu Ora was monitored to ensure that the governance options available under the Ministry of Health were either transitioned or replaced with appropriate bodies to ensure continuity of governance.	Ongoing governance oversight
IPA-07	A particular feature to be monitored is the parent-to-child relationship 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.	To be finalised prior to go-live in each case of additional services

Section Two – My Health Account

Background

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

Use of My Health Account is voluntary. People must opt in to use it and can determine what Identification Level they wish to achieve based on the Services they want to access.

Consumers will be able to 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 as to which Digital Health Services they wish to connect to. Consumers can also revoke that consent when they wish to 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.

The approach Te Whatu Ora 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.

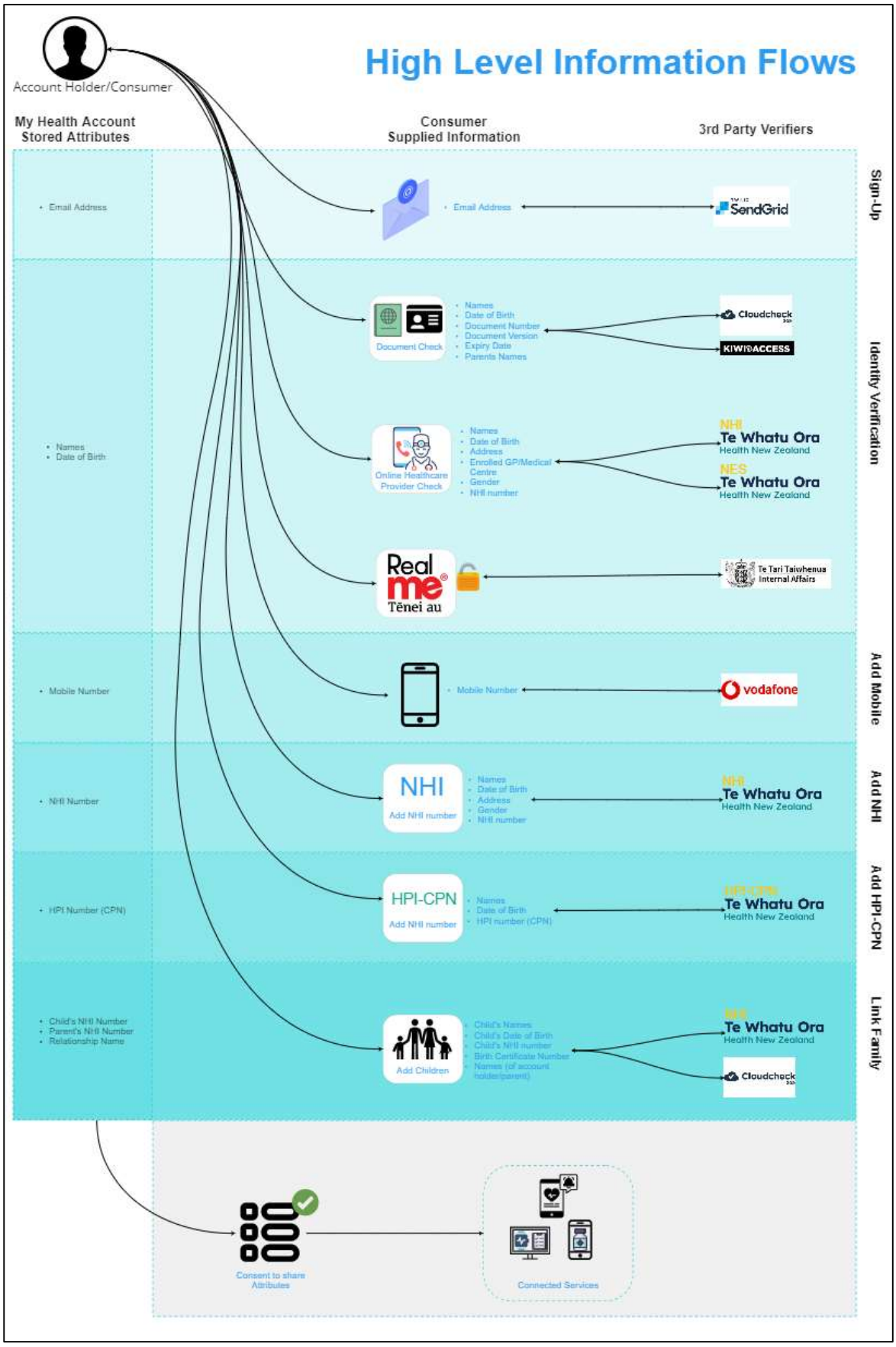
Consumers can sign up directly from the My Health Account website, but most accounts are created when an application or Service the Consumer wishes to use, such as My Covid Record, refers them to My Health Account to establish their identity and Identification Level.

Before signing up to My Health Account, Consumers are provided links to the Privacy statement[3] and Consumer Terms of use[4]. Te Whatu Ora has produced standardised Privacy Statement Materials that are compliant with Rule 3 of the Health Information Privacy Code. The current version of the Privacy statement is in Appendix Three. The website also provides access to advice and guidance[5].

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 Services via My Health Account if they do not meet the Identification Level required for access to the Service in question. An identification level summary is set out in Appendix One.

[3] https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/privacy-statement
[4] https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/terms-of-use
[5] Advice on creating your My Health Account: https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/creating-your-account and advice on how to get the most from your account: https://www.tewhatuora.govt.nz/our-health-system/digital-health/my-health-account/getting-the-most-from-your-account

Information flows involved in My Health Account Processes:



Information Collected

Sign-up

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.

Identity Document Check

Consumers can claim identity information in My Health Account by verifying an official document, such as a Passport or Driver Licence[6]. 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 services[7] to ensure that there is a record of an official document that matches the details provided[8]. This check meets the requirements of Information Assurance according to the Identification Management Standards 2020.

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

Healthcare Provider Check

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

---

[6] The list of documents that can be used for verification are listed on the Te Whatu Ora My Health Account website.
[7] Third-party services are Cloudcheck from Verifi and a Kiwi Access Card verification service from CentraPass.
[8] Information about how third-party services retain and manage data in accordance with the Privacy Act can be found here: https://www.verifidentity.com/legal/#privacy and https://kiwiaccess.co.nz/privacy-statement/.

The Consumer-supplied information is used to find and validate the user's NHI number and their patient record in the National Enrolment Service (NES)[9]. If a matching patient record is identified for the Consumer, and if the patient record includes a Mobile phone number, the Consumer can request that My Health Account send a Time-limited One Time Passcode (TOTP) to that Mobile number via SMS. The Consumer is shown the last four digits of the phone number on the My Health Account screen (with the other details obscured) so that they can determine if they still have access to the phone with that number.

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

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

RealMe® Verified

Consumers who have signed up via a RealMe®[10] 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 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.

---

[9] 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.

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

If a uniquely-matching NHI record is identified, the NHI number for the active NHI record[11] is stored against the Consumer's My Health Account record.

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

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

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

Adding HPI number (CPN)

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

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

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

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

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

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

Parent-to-child / children relationships

Consumers can choose to establish a relationship with specific family members so that they can share in their health and wellbeing outcomes by accessing their health information online. The current feature only allows for parent-to-child / children relationships for children up to 12 years of age.

Parents wishing to establish a relationship with their 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.

[11] 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'.

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 parent-to-child feature. This will ensure that no confidential information, such as a physical address, is surfaced through the parent-to-child relationship 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 and 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.

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 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.

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

Note: this functionality has been built but is not yet visible to Consumers until further notice.

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

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

Auditing

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

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

Information Storage

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

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

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

The main identity store is where the system uses Consumer data for providing account services, such as enabling 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. Te Whatu Ora uses this store for decision-making. The insights the information provides assist in the planning of new features and functionality.

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

In addition to secure data storage, the My Health Account system is also designed to be highly available, thereby allowing 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)
- Family Member NHIs: (Remove)
- 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)
- Family Member NHIs: (Suspend)

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 parent-to-child relationship feature that may compromise the privacy, safety, or security of either of the parents or child / children when a relationship is established between a parent and child through this feature
- meeting security assurance requirements.

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

Consent and Sharing Attributes

Once made available, 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 is combined with other demographic data linked to the NHI (including age, district, ethnicity, and gender) in order to understand parts of the community where access to digital health information can be improved. Any reports use aggregated data and cannot be used to identity Consumers personally.

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

Information Disposal

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

Note: Family Member 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.

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

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

Process for Managing Information Compromise

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

- Cases where there is evidence of fraud may be passed to Police for further investigation, and evidence of an offence under the Privacy Act 2020 will be addressed with the Privacy Commissioner[12].
- 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.

[12] 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).

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 Te Whatu Ora Privacy Officer
- Governance by the Digital Health Identity Product Governance Board for collection, management, authorised use and disclosure, and deletion of data.

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

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 services.

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

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

All services authorised to connect with My Health Account must confirm that their applications or services will 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	Purpose of collection of health information - Only collect health information if you really need it	*Purpose* My Health Account's purpose is to enable Consumers to verify their identity information to the level required to access the health-related services with which they wish to engage. *Necessary* My Health Account has analysed the minimum identity information that can reliably be used for identification at different identification levels. A summary of the Identification Levels is contained in Appendix One. My Health Account has endeavoured to balance the amount of information necessary to meet identification requirements with the risk posed by incorrectly assigning an identification level that could enable the wrong person to access sensitive information. There is an initial level of access to generic health information (Identification Level 1), which can be enabled by providing a verified email address only. This does not need to be linked to the Consumer in any identifiable way. To access services that require a higher Identification Level, it is necessary for 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: • Name* (including given and family names) • Date of Birth* In addition, depending on the verification method or process selected, Consumers may need to provide additional information, such as: • Document type* • Document number	**Low**

		• 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* Of the above information, only those with an asterisk (*) next to them are retained along with verification method and the result of the verification (i.e. success / failure). Adding an NHI number or HPI number (CPN) to a My Health Account is optional, but necessary if Consumers wish to engage with Digital Health Services that do not have the ability to locate those identifiers themselves. Adding a mobile number is an option for 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.	

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

Rule 3	Collection of information from individual - Tell them what you're going to do with it	The current Privacy statement is contained in Appendix Three and the current Terms of use in Appendix Four. The documents are stored on the My Health Account website. Both documents are linked from the initial sign-up page on My Health Account and are in the footer of the application. The Privacy Materials provided are of central importance in ensuring 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. 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 services that can be accessed via My Health Account In addition, advice and guidance can be found on the My Health Account website, providing additional context about some My Health Account features.	**Low**
Rule 4	Manner of collection of information	Consideration has been given to the minimum age of potential account holders and those who may not have full legal capacity to act on their own behalf as My Health Account develops over time. RealMe permits individuals aged 14	**Low (but medium if additional**

	- Be considerate when you're getting it	years and over to create an account. Currently, My Health Account permits those aged over 12 years to create their own account. • The manner of collection of information for a My Health Account is not considered inappropriate for 12- to 15-year-olds, and it remains a voluntary process for users to join My Health Account. For those who are not yet old enough to have a driver licence or other age-related form of identification, the birth certificate is also an option for Cloudcheck or, alternatively, the Healthcare Provider check can be used. • It will be important to remain alert to new applications / Services being added to ensure that any age-appropriate limits are applied if necessary, or alternatives offered. The Privacy statement and Terms of use confirm a parent or legal guardian may assist 12- to 15-year-olds to complete the registration process for My Health Account if they wish to obtain assistance, or the young person can complete it themselves. This area will require ongoing focus if additional applications are, in future, able to use My Health Account identity services. While a parent having access to the My Covid Record of their 14-year-old (if they have set up their My Health Account) is unlikely to access particularly sensitive information, this may be quite different if more extensive access were to be available to the medical records of those 14- or 15-year-olds in the future. Careful consideration will need to be given to: • Expanded access to additional applications with more sensitive information. • How to limit access of a parent who set up an account, as the 12- to 15-year-old ages, and becomes more capable of managing their own information. • It might be a requirement of a young person to independently see a Trusted Witness to make sure that they are sufficiently competent to access information at that level, and that they have the choice to limit access by others, such as their parents, if they choose. Various solutions are currently under active consideration and once finalised will be incorporated into My Health Account. Customer support services are being investigated to address alternative methods of obtaining Identification Levels for those who may not have easily accessible identity documentation or may find Cloudcheck challenging to use. The RealMe identification process is available as an alternative, but it may also be a challenge to achieve for that same group of Consumers. 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).	**services become available that under 12-year-olds may access)**
Rule 5	Storage and security of information - Take care of it once you've got it	Storage and processing of the information on My Health Account is managed by third-party IT vendors, and My Health Account will use its Authority to Operate (ATO) processes to ensure it has done everything reasonably in its power to prevent unauthorised use or disclosure of information. The IT component of My Health Account has been subject to full Ministry of Health and Te Whatu Ora Certification and Accreditation processes, together with independent third-party testing and an Authority to Operate (ATO). Future releases of significance will be subject to this same level of security scrutiny. Section 11 of the Privacy Act 2020 will apply to the hosting of My Health Account, as the information will be held on behalf of Te Whatu Ora for safe custody and processing. All services authorised to connect to My Health Account are required to provide evidence that they meet Te Whatu Ora Privacy and Security requirements. This includes evidence of Security Testing and completion of a Privacy Impact Assessment. For the parent-to-child relationship 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	**Medium**

		situation that disclosure of address or contact details may enable one parent to locate the other, without the consent of that other parent. All account access and all account updates or changes by Consumers will be tracked, as will all access by system administrators and call centre support. This helps Te Whatu Ora administrators to resolve queries raised by 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.	
Rule 6	Access to personal information - People can see their health information if they want to	It is expected that most of the information held in My Health Account will be easily viewable by the Consumer on their own device. For information not available directly via My Health Account, the My Health Account Privacy statement outlines how to obtain access to it. My Health Account only holds information related to the service it provides and will need to refer requests for information related to other Services on to those services. This will be managed with existing privacy team processes.	**Low**
Rule 7	Correction of information - They can correct it if it's wrong	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.	**Low**
Rule 8	Accuracy etc. of information to be checked before use - Make sure health information is correct before you use it	Accuracy is very important to the allocation of the unique digital health identity that will be associated with each My Health Account. Third-party processes or checking are involved in management of Identification Levels 2 and 3 (with Cloudcheck, or other approved verification partners including RealMe) or checking against an established NES record used in the provision of healthcare to the Consumer. This should assist with accuracy in assigning a correct identity to the relevant My Health Account. It is noted that the Consumer name provided to other services using My Health Account for verification will be the name that matches the documented identity attributes, not the NHI name, if there is a difference between the two. This is likely to align the legal identity of the 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. There is also the ability to seek manual input from the specialist NHI team if an NHI number does not match during the digital processes applied. The accuracy-related issues in other services that interact with or use My Health Account will need to be carefully reviewed in the Privacy Impact Assessments for those other features.	**Low**
Rule 9	Retention of information - Get rid of it when you're done with it	Only information necessary for the effective administration of the account will be retained. A summary of the information retained is recorded in Appendix Two. If a My Health Account is closed by the Consumer (or because of an administration process – e.g. on notification that a Consumer is deceased) a record of the fact that there was an account, the email used to establish the account, the Identification Level (and related dates it was obtained), and any linked NHI or health identifier number. These details will be required as an audit record of authorisation for activity related to their files. A Consumer's verified attributes need to be reverified every five years. If a Consumer fails to reverify their attributes, then access to the account may be suspended and verified information deleted after due process.	**Low**

Rule 10	Limits on use of information - Use it for the purpose you got it	The purpose of My Health Account is to allow 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. This PIA does not address the use of information by Digital Health Services, however: • Digital Health Services must pass various security testing and compliance requirements before 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. 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.	**Low**
Rule 11	Limits on disclosure of information - Only disclose it if you have good reason	The disclosure enabled via My Health Account during the verification process is signalled in advance to Consumers, who may then choose to proceed with the disclosures (for example, to Cloudcheck or other authorised third-party identity services). The information disclosed to Digital Health Services about 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 are approved for disclosure to the Digital Health Service. 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. Subsequent controls on disclosure that may be associated with My Health Account will need to be carefully reviewed in future releases, prior to incorporating and enabling those activities. A Framework, within which other services may authorise disclosures, will need to be provided so that other 'enabling' services (such as Hira) fully address disclosure implications to make sure the My Health Account role is fully considered, and any authorisation matches the My Health Account Identification Levels. An area that needs to be specifically addressed in future is how to manage Rule 11(5) obligations in terms of s22F of the HIPC (as an information request may be refused if it would be contrary to the individual's interests or there are reasonable grounds for believing that the individual does not or would not wish the information to be disclosed). This will be a particular challenge with those 12- to 15-year-olds who may have had the assistance of their parent to establish their My Health Account and now wish to exclude their parent from access to sensitive records if services making those available may be authorised by My Health Account in future. Failure to address this risk in future would result in the Residual Risk profile rising to high. The parent / child feature, enabling access by parents to some information about their young children, will need to be monitored to ensure that address and contact details remain masked so that there is no risk of stalking or locating a former partner via this service. This will include interactions with other 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	**Low**

		legitimate concern is raised with the My Health Account Customer Service team.	
Rule 12	Disclosure of personal information outside New Zealand	My Health Account information is hosted in Australia but is held only by Microsoft Azure and Amazon Web Services (AWS) as an agent for the Te Whatu Ora and the information may not be used by that contracted provider for its own purposes. Cloudcheck is based in New Zealand but interacts with Australian-based government APIs to check Australian documents, if requested by the Consumer. CentraPass is based in New Zealand but the services that My Health Account interact with are hosted in Australia (AWS). There will be no disclosure of information made outside New Zealand under the rules identified in Rule 12 for My Health Account.	**Low**
Rule 13	Unique identifiers - Only assign unique identifiers, where permitted	The National Health Index (NHI) number is the unique identifier for patients who receive healthcare in New Zealand and 'is the cornerstone of clinical and administrative patient-related information'. It is not used as the account identifier. My Health Account's use of the NHI number in the health sector is for the purpose of unique identification of the individual concerned. The applications / Services seeking to use My Health Account NHIs should be restricted to those that comply with the requirements of the HIPC (as per Rule 13(3) (noting that the agencies approved to assign the NHI number have been updated to include the new agencies under the Pae Ora Act). All parties interacting with My Health Account (other than Consumers) will be consistent with Schedule 2 of the HIPC. The Health Provider Index (HPI) – Common Person Number (CPN) is the unique identifier for some health practitioners in New Zealand and links them to the Health Provider Index. My Health Account allows 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). 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.	**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, parents name)	Until document is successfully verified.
Enrolled General Practice or Medical Centre	Until General Practice or Medical Centre enrolment is successfully verified.
Address	Until General Practice or Medical Centre enrolment is successfully verified / Until NHI successfully added to account.
Gender	Until NHI successfully added to account.
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).
CPN (HPI number)	For the duration of the My Health Account (or until removed by an Administrator).
Relationship information (including Parent NHI, Child NHI, child/relationship nickname, expiry date)	For the duration of the relationship (or until changed or removed by the Consumer or Administrator). **Note:** Deleting the My Health Account that established the relationship does not automatically delete the relationship information.
Audit records	For a minimum of five years from creation of each record. **Note:** Access to audit records is strictly controlled and limited to Te Whatu Ora staff who are responsible for maintaining security standards and resolving customer support queries

Appendix Three – Privacy statement

My Health Account Privacy statement

Effective 1 February 2023

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

- It's voluntary for you to sign up for an Account.
- My Health Account is designed to make it easy for you to access your health information, and to connect with New Zealand digital health services.
- If you are 12 years or older, you can create your own My Health Account.
- Your parent or legal guardian can also create it on your behalf, with your permission, if you are aged 12 to 15 years old.
- Once the service becomes available, a parent or legal guardian may also access some information about their child or children aged under 12 years if they establish a Family Member account.
- 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.

If you are a consumer of healthcare services, you can add your National Health Index (NHI) number to your account if you wish. If you are a health practitioner, you can add your HPI number (CPN) to your account if you wish.

Identification Level 1

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

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

Identification Level 2

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

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

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

Identification Level 3

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

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

To reach Level 3, you must use:

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

Identification Level 2N or 3N

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

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

Identity document check

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

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

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

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

Healthcare provider check

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

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

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

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

Health workforce

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

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

Health workforce members can set up a health consumer My Health Account (for when they are receiving health services) and a My Health Account Workforce (for when they are operating in their health workforce role to deliver services). We will only provide the details related to one of those roles at a time (that is, we will not provide your NHI if it is a health workforce-related application, and we will not provide your CPN if it is a health consumer service application).

How we use your information

Your My Health Account information is used to:

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

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

- You need to review relevant information from those other services before you sign up to them, and grant permissions to sharing your information with those other services at the time you first access the services.
- We disclose to those participating apps and services your documented identity attributes, such as your first name, middle name, preferred name (if one is provided), last name, date of birth, email address, mobile phone number, NHI number, HPI number (CPN), related family member NHI numbers (if applicable), and identification level associated with your account.

- Attributes will only be shared with digital health services as necessary for that service. If the details are not necessary for operation of the application, they will not be supplied.
- The list of which attributes digital health services can receive is agreed upon and configured during the application onboarding process. My Health Account will ask you to grant permissions when first accessing the service and those permissions will be displayed to you as part of the Account services.
- You can also choose to stop sharing your information within your My Health Account to an application if you have previously given permission. They may retain any information supplied about you while the permission was granted but will not be able to access your Account information in future.
- Some services that require My Health Account verification apply age restrictions. If your date of birth is outside the permitted age range, you will be refused access to those services.
- Services currently approved to integrate with My Health Account include:
    - My Covid Record
    - Vaping Retailer Regulatory Platform
    - End-of-Life Choice Regulatory Platform
    - Workforce Requests
    - Aotearoa Immunisation Register
    - New Zealand Health Terminology Services (NZHTS)

Please see the full Privacy Impact Assessment (PIA) for details of how these services use Consumer information.

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

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

How we protect your privacy

We take your privacy seriously.

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

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

How we secure your information

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

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

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

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

We use Google reCAPTCHA v3 during the account sign-up stage 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 family member NHI numbers are also retained until the relationship is removed (not when the My Health Account that established the relationship is deleted). These details are supplied to authorised services connecting to the My Health Account service as identified in the PIA for each of those services (and as approved by the My Health Account service).

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

Tips to keep your My Health Account secure

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

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

Viewing or changing your information

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

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

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

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

Giving feedback

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

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

Statistical information

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

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

The website uses cookies so we can monitor website usage. A cookie is a piece of code that creates a file on your computer to track the pages that you view on our website. The cookies do not collect personal information. You can disable them or clear them out of your web browser without affecting your ability to use the website.

Cloudcheck also collects statistical information about visitors to its websites, such as the number of visitors, pages viewed, types of transactions conducted, time online and documents downloaded. It also collects cookies that you may disable or delete from your computer after they have been created – see more details here.

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

My Health Account Terms of use

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

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

What you are agreeing to

By accepting these terms, you understand and agree:

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

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

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

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

Anyone who knowingly accesses or uses, or attempts to access or use, any My Health Account or related Te Whatu Ora, Ministry of Health, or third-party provider service for an unlawful purpose

(including but not limited to fraud or attempted fraud or hacking or attempted hacking), may be liable to prosecution under New Zealand Law.

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

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

Privacy and how we use your information

You can make choices about how much information you provide to the service, and what level of identity verification you wish to complete. Some digital health services are restricted to stronger verification requirements. We will guide you through your options.

We will securely hold and manage the information you provide to us through the service. You can make choices within your account to decide how your information may be managed.

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.

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).

Security

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 February 2023

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

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

Glossary

The following are definitions used in this Assessment:

Terms	Description, relationship, and business rules
Authorised Private Entity	An entity authorised to participate as a Service Provider in the health information sector after completing authorisation processes established by Te Whatu Ora / the Ministry of Health. This includes both providers of health services and health IT services.
Cloudcheck	This is the electronic identity verification service used to verify an identity document as part of My Health Account processes. More information can be found here: https://www.verifidentity.com/cloudcheck/
Common Person Number (CPN)	A unique identifier given to some health practitioners. The CPN is a separate identifier given to the practitioner – it is different to the NHI number used by them as a health Consumer.
Digital Health Services	A service or application offered by a Service Provider that has been onboarded to use My Health Account as an identity provider.
Consumer	Each user who registers to use My Health Account services as their unique Digital Health Identity
Consumer Terms of use	The terms that the Consumer will accept as part of signing up to use the My Health Account service
Digital Health Identity	The entity information that is bound to the My Health Account used by the Consumer. Informally – an individual's My Health Account. Non-identity accounts are also available as an information channel.
Hira	This is a Ministry initiative. It will be the national health information platform programme and will be designed to enable accessibility of health information from many sources and provide a range of digital services that make health information easier to access, use and share (with appropriate controls around privacy and security). Hira Website.
Health Provider Index (HPI)	The central national database for use by the New Zealand health and disability sector which uniquely identifies health practitioners, health provider organisations and facilities.
Identification Level	The level of identification confirmed by My Health Account for the Consumer, as further described in Appendix 1.
Microsoft Azure B2C	Microsoft Azure Business to Consumer product is the underlying technology used by My Health Account
Ministry	Manatū Hauora – the Ministry of Health
My Health Account	The Te Whatu Ora application that enables Consumers to obtain, and assert, a digital health identity.
Onboarding	The formal process (including the security and privacy aspects of the service or application) a potential Connected Health Service must complete prior to being permitted to use My Health Account services.
Privacy Statement Materials	Material to be prepared to inform Consumers in compliance with relevant rules in the Health Information Privacy Code 2020, including rule 3 in particular.

Terms	Description, relationship, and business rules
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 / Digital Health Service	A government agency (including Te Whatu Ora) or Authorised Private Entity that 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 interact with My Health Account services
Te Whatu Ora – Health New Zealand	A Crown agent established under section 11 of the Pae Ora (Healthy Futures) Act 2022