Te Whatu Ora
Health New Zealand

My Health Account Workforce

Privacy Impact Assessment

Date: 20 April 2023

Te Whatu Ora
Health New Zealand

Document Approval

	Name/Title	Sign-off date
Approved by Senior Responsible Officer	Gerard Keenan	30/03/23
Approved by Chief Privacy Officer, Te Whatu Ora	Viv Kerr	20/04/23

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 Workforce services will operate.

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

Contents

Section One – Executive Summary

1. My Health Account Workforce is the Health Workforce Digital Identity service for Aotearoa New Zealand's Health Workforce members. It is developed by Te Whatu Ora – Health New Zealand[1].

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

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

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

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

    4.2. for non-Registered Workforce members.

5. My Health Account Workforce does not confirm the person's role (other than as identified with the CPN) nor their workplace.

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

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

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

7. Te Whatu Ora has recognised that there are potential privacy risks, not just to Health Workforce members contributing their information to obtain a My Health Account Workforce, but also in relation to some of the Digital Health Services that seek to connect to My Health Account Workforce if they involve Consumer information. Te Whatu Ora is aware that it needs to carefully balance these risks against the benefits of

[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.

enabling Health Workforce members to securely assert a digital identity to Digital Health Services.

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

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

    8.2. Information about Health Workforce members who use My Health Account Workforce Services is stored by Te Whatu Ora. That information will only be shared with any other agencies (Government or otherwise) when explicit Health Workforce member consent is obtained, or it is authorised by law (such as in compliance with the rules in the Health Information Privacy Code 2020 and other enactments that require or allow information to be used or disclosed).

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

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

9. Te Whatu Ora consulted with the Office of the Privacy Commissioner and the Government Chief Privacy Officer prior to finalising this Privacy Impact Assessment.

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

Scope of Assessment

11. The current Assessment covers:

11.1. The work-related, demographic, and anonymous[2] information to be collected from the Health Workforce member to create a My Health Account Workforce.

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

12. This Assessment does not address:

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

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

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

Assessment content

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

15. Section Three contains the Privacy Analysis.

Recommendation Summary

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

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

17.1. My Health Account Workforce is a 'doorway' to approved Digital Health Services.

17.2. Te Whatu Ora oversees how My Health Account Workforce controls are managed within Digital Health Services, via its Onboarding process, and retains control for Health Workforce members within their My Health Account

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

Workforce, by enabling choice about which Digital Health Services the Health Workforce member uses.

17.3. There is a danger of function creep if:

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

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

17.4. Privacy risks associated with My Health Account Workforce are successfully managed by Health Workforce member-applied controls, security measures, and strong governance oversight. Digital Health Services controls are expected to be applied via Onboarding processes.

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

Recommendations:

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

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

	the My Health Account Workforce application or by direct email to all email addresses verified by My Health Account Workforce processes.	statement on the website)
PIA-03	The Onboarding process will be reviewed to ensure that Digital Health Services: • have completed a PIA and incorporate a relevant privacy statement as part of the Health Workforce Onboarding processes • will operate at an Identification Level appropriate with My Health Account Workforce settings • can apply the under 16-year-old exclusion process • can independently confirm role and employer if that is required for the Digital Health Service's operation • can independently confirm the status of any Health Practitioner registration required to allow the Health Practitioner to access that Digital Health Service • understand the limitations applicable to the Health Workforce Digital Identity established (in terms of exactly what is, and is not, verified by the My Health Account Workforce, particularly in relation to the Non-registered Workforce).	To be finalised prior to go-live in each case of additional services
PIA-04	Service Providers (who are Onboarded for their Digital Health Services) must be bound to appropriate Terms of Use that confirm the permitted purposes for use of any information accessed, to ensure Service Providers are clear about expectations for use, and limitations on use of this work-related information.	Prior to service providers being permitted to interact with My Health Account Workforce
PIA-05	Strong governance is required to ensure that My Health Account Workforce and any connecting Digital Health Services remain consistent with the My Health Account Workforce expectations set out in this Privacy Impact Assessment.	Ongoing governance oversight

Section Two – My Health Account Workforce

Background

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

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

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

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

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

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

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

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

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

My Health Account Workforce

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

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

- Health Workforce members can sign up directly from the My Health Account Workforce website, but initially, most accounts will be created when a Digital Health Service the Health Workforce member wishes to use, such as a reporting tool or patient management system[3], refers them to My Health Account Workforce to establish their identity and Identification Level.

- Before signing up to My Health Account Workforce, Health Workforce members are provided links to the Privacy statement[4] and Terms of use[5] (as per current drafts in Appendix Three and Four). The website will also provide access to advice and guidance[6].

Identification Levels

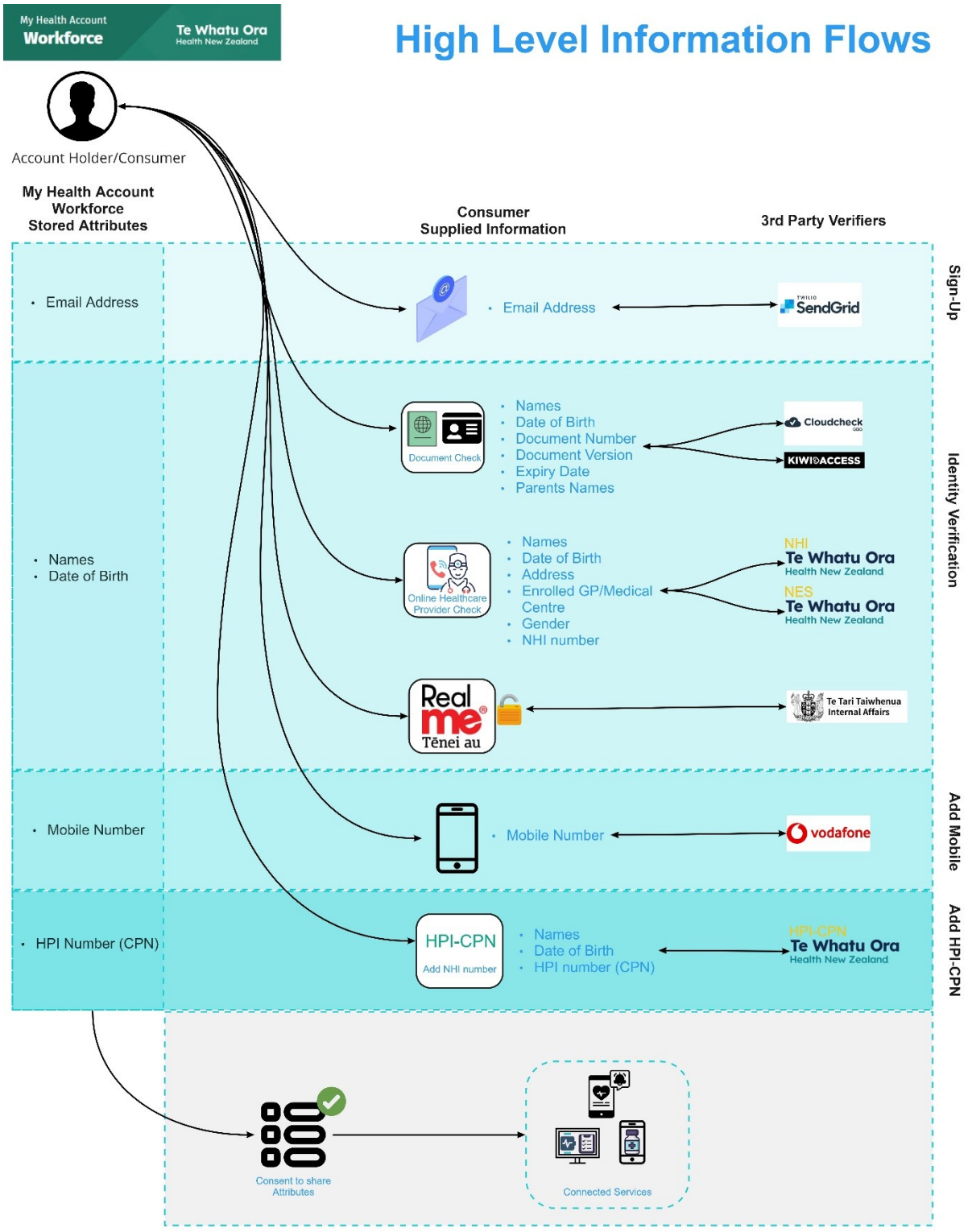
Before Health Workforce members can use My Health Account Workforce, their identity must be verified. This verification process involves several steps, and the 'Identification Level' achieved reflects the increasing assurance that can be placed on each step.

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

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

[3] Noting that My Health Account Workforce will be providing only the identification verification at the relevant Identification Level, and the existence of a corresponding CPN, if provided. The Digital Health Service would need to manage any applicable role-based access or current employment matters.
[4] https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/privacy-statement
[5] https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/terms-of-use
[6] Advice on creating your My Health Account Workforce: https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/creating-your-account and advice on how to get the most from your account: https://www.tewhatuora.govt.nz/for-the-health-sector/my-health-account-workforce/getting-the-most-from-your-account

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



Information Collected during sign-up processes

Sign-up

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

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

Identification Level 1 is only a verified email account.

My Health Account (health consumer) check

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

My Health Account Workforce will only retain the Health Workforce member's first name, middle name / s (if any), last name, date of birth, and the method they used to verify their identity for their My Health Account, as well as their HPI number (CPN) if it has been added to their My Health Account. No other details from their My Health Account will be stored in their My Health Account Workforce.

Identity Document Check

Health Workforce members can claim identity information in My Health Account Workforce by verifying an official document, such as a Passport or Driver Licence[7]. Health Workforce members are required to provide information as recorded on the selected document type, including name, date of birth, document/card number and, depending on the type of document used, other details such as expiry date or document version.

The Health Workforce member-supplied information is checked against the source records (e.g. those held by DIA or Waka Kotahi) via third-party services[8] to ensure that there is a record of an official document that matches the details provided[9]. This check meets the requirements of Information Assurance according to the Identification Management Standards 2020.

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

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

Healthcare Provider Check

Health Workforce members can choose to verify their identity using information already held about them in Te Whatu Ora records. Health Workforce members are required to provide information about themselves including their name, date of birth, address and the General Practice or Medical Centre with which they are currently enrolled. They also have the option to provide their gender and NHI number as part of this check process. However, the gender and NHI number details are not retained by My Health Account Workforce[10].

The Health Workforce member-supplied information is used to find and validate the user's NHI number and their patient record in the National Enrolment Service (NES)[11]. If a matching patient record is identified for the Health Workforce member, and if the patient record includes a Mobile phone number, the Health Workforce member can request that My Health Account Workforce send a Time-limited One Time Passcode (TOTP) to that Mobile number via SMS. The Health Workforce member is shown the last four digits of the phone number on the My Health Account Workforce screen (with the other details obscured) so that they can determine if they still have access to the phone with that number.

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

My Health Account Workforce retains the Health Workforce member-supplied name and date of birth (where not already stored) along with verification details in line with what is described under the My Health Account (health consumer) check

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

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

[10] Health Workforce members are unable to add their National Health Index (NHI) number to their My Health Account Workforce. This creates a clear line of separation between their personal health information and work-related information.
[11] 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.

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

Identity Document Check above. No information related to the Health Workforce member's NHI number or their enrolment with a general practice or healthcare provider is retained or stored.

RealMe® Verified

Health Workforce members who have signed up via a RealMe[12] account with a 'Verified' status can choose to allow RealMe to share their 'Verified' information with My Health Account Workforce.

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

My Health Account retains the name and date of birth along with verification details in line with what is described under the My Health Account (health consumer) check

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

My Health Account Workforce will only retain the Health Workforce member's first name, middle name / s (if any), last name, date of birth, and the method they used to verify their identity for their My Health Account, as well as their HPI number (CPN) if it has been added to their My Health Account. No other details from their My Health Account will be stored in their My Health Account Workforce.

Identity Document Check above.

Adding HPI number (CPN)

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

My Health Account Workforce will use the verified information (names and date of birth) stored against the Health Workforce member's record to search for a matching HPI record. Health Workforce members must provide the HPI number (CPN) but can edit the name

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

information that is used in the search, in case the name on their Annual Practising Certificate is different to the name used on their identity document.

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

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

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

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

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

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

HPI number (CPN) and My Health Account

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

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

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

Other Personal Information

Preferred Name

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

Mobile Number

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

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

Cookies

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

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

Statistical Information

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 Health Workforce member personally.

Auditing

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

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

Information Storage

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

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

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

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

The analytical store (or data warehouse) holds an aggregated view of My Health Account Workforce information. 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 Workforce system, with full encryption of all information and rigorous access controls.

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

Information Updates / Correction

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

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

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

- HPI number (CPN): (Remove)

Information Use and Sharing

Onboarding Digital Health Services

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

- restricting access to only those Health Workforce members who meet the agreed criteria (e.g. Identification Level and Health Workforce member's age is 16 years old or over[13])
- compliant with the Privacy Act 2020 and Health Information Privacy Code 2020 (which includes only requesting attributes for which it has a valid business need)
- meeting security assurance requirements.

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

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

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

Consent and Sharing Attributes

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

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

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

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

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

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

Analytics and Reporting

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

My Health Account Workforce User information will remain securely contained in Te Whatu Ora systems and only aggregated information (without names, HPI number (CPN), or other

individually-identifiable information) will be used in created reports, to preserve individual health workforce member privacy.

Information Disposal

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

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

Reverification of Details

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

Process for Managing Information Compromise

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

- Cases where there is evidence of fraud may be passed to Police for further investigation, and evidence of an offence under the Privacy Act 2020 will be addressed with the Privacy Commissioner[14].

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

- Notifiable privacy breaches will be reported to the Privacy Commissioner (and affected individuals or the public, where required) as soon as practicable as required by the Privacy Act.
- A warning has been incorporated into Privacy Materials to ensure Health Workforce members are aware of the seriousness of misrepresenting their identity or assuming the identity of another. Health Workforce members are expected to agree to Terms of use, and this is incorporated into those terms.

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

Governance

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

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

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

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

Governance includes:

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

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

Section Three – Privacy Analysis

The purpose of this Assessment is to review the process of collection, storage, use and sharing of personal and contact information for the purposes of My Health Account Workforce against the 13 Rules in the Health Information Privacy Code (HIPC).

The pattern established for My Health Account, has been followed in My Health Account Workforce, minimising the amount of information retained to establish the Health Workforce Digital Identity. My Health Account Workforce has several privacy-enhancing features. Users are informed about what information will be shared with each Digital Health Service and are asked to give consent to that information being shared with that service. They have the option to decline to share information, in which case they will not be given access to that Digital Health Service. They can also log in to their My Health Account Workforce, at any time, and revoke access for their information to be shared with a Digital Health Service from that time forward. Security of the My Health Account Workforce environment effectively replicates that of My Health Account (and will be subject to similar Certification and Accreditation review by the Te Whatu Ora security team, and appropriate third-party testing).

A key difference will, however, be that the My Health Account Workforce will operate in the health workforce environment through Digital Health Services and may, therefore, involve access to information about health Consumers, rather than just enable access to information about the Health Workforce member themselves. This is a significant difference.

It is important to note that this Assessment only addresses the Health Workforce Digital Identity component of My Health Account Workforce. It does not review any of the connected Digital Health Services that are, or may in the future, be used with My Health Account Workforce.

- Digital Health Services wishing to connect to My Health Account Workforce are required to complete an Onboarding process, which includes the completion of a Privacy Impact Assessment. Both privacy and security requirements must be met, prior to connection to My Health Account Workforce being offered.
- Although it will be the responsibility of the Digital Health Service to manage any access it provides to information about other health Consumers (if that is its purpose), it is crucial that My Health Account Workforce is very clear about the scope of the Health Workforce Digital Identity, and the implications of what is able to be confirmed via the Identification Levels.
- It is also noted that in terms of Non-registered Workforce members only the identity of the person is established at any of the Identification Levels. If a person who was not in the Health Workforce chose to create a My Health Account Workforce account, My Health Account Workforce would not be able to identify that fact.
- It is strongly recommended that the Onboarding processes are stringent in terms of refusing access to Digital Health Services that cannot demonstrate the full solution for appropriate management of Consumer health information, such that the Service complies with the Health Information Governance Guidelines. My Health Account Workforce is likely to be only a single component of that full solution.

- All Digital Health Services authorised to connect with My Health Account Workforce must confirm that their applications or services will comply with the agreed Identification Level expectations set by My Health Account Workforce.

My Health Account Workforce will implement changes incrementally, through a series of Releases. Each change of significance will be subject to Privacy Impact Assessment activity.

Health Information Privacy Code Rules		**Background and Key Controls**	**Residual risk**
Rule 1	Purpose of collection of health information - Only collect health information if you really need it	*Purpose* My Health Account Workforce's purpose is to enable Aotearoa New Zealand's Health Workforce to verify their identity information to the level required to access the work-related Digital Health Services with which they wish to engage. *Necessary* My Health Account Workforce has analysed the minimum identity information that can reliably be used for identification at different Identification Levels. A summary of the Identification Levels is contained in Appendix One. My Health Account Workforce has endeavoured to balance the amount of information necessary to meet identification requirements with the risk posed by incorrectly assigning an Identification Level that could enable the wrong person to access sensitive information. There is an initial level of access to generic health information (Identification Level 1), which can be enabled by providing a verified email address only. This does not need to be linked to the Health Workforce member in any identifiable way. To access services that require a higher Identification Level, it is necessary for Health Workforce members using My Health Account Workforce to supply additional information that can then be verified against other sources of information. The base information that needs to be verified is: • Name* (including given and family names) • Date of Birth* In addition, depending on the verification method or process selected, Health Workforce members may need to provide additional information, such as: • Document type* • Document number • Expiry Date • Parent's names • Enrolled GP practice • Address • Gender • HPI number (CPN)* Of the above information, only those with an asterisk (*) next to them are retained along with verification method and the result of the verification (i.e. success / failure). Adding an HPI number (CPN) to a My Health Account Workforce is optional, but necessary if Health Practitioners wish to engage with Digital Health Services that do not have the ability to locate those identifiers themselves. Adding a mobile number is an option for Health Workforce members if they prefer to receive second-factor authentication challenges via SMS rather than	**Low**

		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 Workforce processes involve the Health Workforce member supplying most information directly to My Health Account Workforce themselves, except for those activities it authorises My Health Account Workforce to undertake, as follows:
		• The HPI number (CPN), which the Health Workforce member authorises My Health Account Workforce to search for and match to their verified information
		• Information related to background processing, such as results of verification processes (i.e. success / failure), including:
		  ○ Document Identity checking
		  ○ Healthcare Provider checking
		  ○ My Health Account (consumer) checking
		  ○ HPI number (CPN) matching
		• The mobile number used in the Healthcare Provider Check, which needs to be sourced from the National Enrolment Service (NES) to complete the verification process
		• The details from RealMe that populate My Health Account Workforce (after express authorisation from the Health Workforce member within the RealMe application).
		Provided the Privacy Materials that accompany My Health Account Workforce remain appropriate and consistent with the expressed intent, Rule 2(2)(a) will apply – the individual authorises collection of the information from someone else.
			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 Workforce website. Both documents are linked from the initial sign-up page on My Health Account Workforce and are in the footer of the application. The Privacy Materials provided are of central importance in ensuring have a clear understanding of what My Health Account involves, and how they may control the amount of information collected, and their interaction with services that can be accessed via My Health Account. The Privacy statement is updated regularly as changes are made in My Health Account Workforce. Te Whatu Ora's website contains the most current list of services that can be accessed via My Health Account Workforce. In addition, advice and guidance can be found on the My Health Account Workforce website, providing additional context about some My Health Account Workforce features. If a third-party Consumer's information is accessible to a Health Workforce member through a Digital Health Service, My Health Account Workforce's Onboarding process will require a Privacy Impact Assessment and Privacy Statement to be completed by that Digital Health Service.	**Low, subject to appropriate Onboarding Controls being applied to connected Digital Health Services**
Rule 4	Manner of collection of information - Be considerate when you're getting it	Consideration has been given to the minimum age of potential account holders as My Health Account Workforce develops over time. • RealMe permits individuals aged 14 years and over to create a RealMe account. Currently, My Health Account Workforce permits those aged over 16 years to create their own Workforce account. Sixteen years is considered the youngest age when it is most likely that Non-registered Health Workforce members would hold an employment role and could be expected to comply with the Terms of Use. If it is identified that there is an equity issue for younger Health Workforce members, the relevant age settings will be reconsidered. It is noted, however, that there are no technical controls on My Health Account Workforce to prevent a younger person between 12 and 16 years creating an account – it is	**Low**

		governed by a requirement in the Terms of Use. It will, therefore, be made an Onboarding requirement for any relevant Digital Health Service that it can restrict Users to the appropriate age groups. • The manner of collection of information for a My Health Account Workforce is considered appropriate for those over 16 years old, and it remains a voluntary process for Health Workforce members to join My Health Account Workforce. • It will be important to remain alert to new Digital Health Services being added to ensure that any age-appropriate limits are applied, if necessary, or alternatives offered. Ongoing focus will be required if additional applications are, in future, able to use My Health Account Workforce Digital Health Identity services. Careful consideration will need to be given to: • Expanded access to additional Digital Health Services with more sensitive information. • It might be a requirement of a young person under 18 years of age to independently see a Trusted Witness to make sure that they are sufficiently competent to access information at that level. Various solutions are currently under active consideration and once finalised will be incorporated into My Health Account. Customer support services are being investigated to address alternative methods of obtaining Identification Levels for those who may not have easily accessible identity documentation or may find Cloudcheck challenging to use. The RealMe identification process is available as an alternative, but it may also be a challenge to achieve for that same group of Consumers.	
Rule 5	Storage and security of information - Take care of it once you've got it	Storage and processing of the information on My Health Account Workforce is managed by third-party IT vendors, and My Health Account Workforce will use its Authority to Operate (ATO) processes to ensure it has done everything reasonably in its power to prevent unauthorised use or disclosure of information. The IT component of My Health Account Workforce has been subject to full Te Whatu Ora Certification and Accreditation processes, together with independent third-party testing and an Authority to Operate (ATO). Future releases of significance will be subject to this same level of security scrutiny. Section 11 of the Privacy Act 2020 will apply to the hosting of My Health Account Workforce, as the information will be held on behalf of Te Whatu Ora for safe custody and processing. All Digital Health Services authorised to connect to My Health Account Workforce are required to provide evidence that they meet Te Whatu Ora Privacy and Security requirements. This includes evidence of Security Testing and completion of a Privacy Impact Assessment. All account access and all account updates or changes by Health Workforce member Users will be tracked, as will all access by system administrators and call centre support. This helps Te Whatu Ora administrators to resolve queries raised by Health Workforce members and maintains a record of who has looked at or changed which details. These audit records will be maintained for a minimum of five years and are to be monitored by system administrators.	**Low**
Rule 6	Access to personal information - People can see their health information if they want to	It is expected that most of the information held in My Health Account Workforce will be easily viewable by the Health Workforce member on their own device. For information not available directly via My Health Account Workforce, the My Health Account Workforce Privacy statement outlines how to obtain access to it. My Health Account Workforce only holds information related to the Digital Health Identity service it provides and will need to refer requests for information related to other Services on to those services. This will be managed with existing Te Whatu Ora privacy team processes.	**Low**

Rule 7	Correction of information - They can correct it if it's wrong	Health Workforce members can correct some information about themselves directly within My Health Account Workforce. For other information, Health Workforce member can request updates to their My Health Account Workforce information by contacting Te Whatu Ora customer services for support and/or can arrange to update information on the HPI service by contacting their Responsible Authority, as per current processes.	**Low**
Rule 8	Accuracy etc. of information to be checked before use - Make sure health information is correct before you use it	Accuracy is very important to the allocation of the unique Health Workforce Digital Identity that will be associated with each My Health Account Workforce. Third-party processes or checking are involved in management of Identification Levels 2 and 3 (with Cloudcheck, or other approved verification partners including RealMe) or checking against an established NES record used in the provision of healthcare to the Consumer or checking against the Health Workforce member's My Health Account (health consumer). This should assist with accuracy in assigning a correct Digital Health Identity to the relevant Identification Level in the User's My Health Account Workforce. It is important that the Digital Health Services clearly understand the implications of 'accuracy' in terms of the information available in the Digital Health Identity provided by the My Health Account Workforce. For a Non-registered Workforce member, only the person's identity can be established – the fact that they are an account holder does not actually establish that they are a Health Workforce member, nor the role they might hold if they are a Health Workforce member, nor their employer. It is noted that the Health Practitioner name provided to other Digital Health Services using My Health Account Workforce for verification will be the name that matches the documented identity attributes. The Health Practitioner's name stated on their Annual Practising Certificate (APC) – i.e. the one attached to the HPI number (CPN) – may be different. Health Practitioners can use the 'Change' feature in the My Health Account Workforce profile page to update their Preferred name so that it matches the name stated on their APC. This additional 'nickname' attribute can then be shared with Digital Health Services. If a connected Digital Health Service needs the Health Practitioner's name to match the Health Practitioner's name attached to the HPI number (CPN), then they can query the Health Provider Index directly. There is also the ability to seek manual input from the HPI team if an HPI number (CPN) does not match during the digital processes applied. The accuracy-related issues in other services that interact with or use My Health Account Workforce will need to be carefully reviewed in the Privacy Impact Assessments for those other features.	**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 Workforce is closed by the Health Workforce member (or because of an administration process – e.g. on notification that a Health Workforce member is deceased) a record will be retained of the fact that there was an account, the email used to establish the account, the Identification Level (and related dates it was obtained), and any linked CPN or health identifier number. These details will be required as an audit record of authorisation for activity related to their files. A Health Workforce member's verified Digital Health Workforce Identity attributes need to be reverified every five years. If a Health Workforce member fails to reverify their attributes, then access to the account may be suspended and verified information deleted after due process.	**Low**
Rule 10	Limits on use of information - Use it for the purpose you got it	The purpose of My Health Account Workforce is to allow Health Workforce members to create a trusted Health Workforce Digital Identity, which they can use to securely access Digital Health Services that link them with the work-related health information they are authorised to access.	**Low**

		• This PIA does not address the subsequent use of the Health Workforce Digital Identity information by Digital Health Services but notes that it is important for the integrity of this identity system that the Digital Health Services ensure they use the correct Identification Levels and that any use of My Health Account Workforce to access identifiable health Consumer information is appropriately supported by other Digital Health Service processes. • It is however noted that Digital Health Services must pass various Onboarding, security testing and compliance requirements before they are permitted to access any My Health Account Workforce information (which includes providing evidence to My Health Account Workforce of Privacy and Security due diligence) The Digital Health Services are required to meet the 'use' requirements described in the Privacy Statement for My Health Account Workforce as part of the Onboarding process: • Digital Health Services are asked to provide links to their Privacy statement and Terms of use so that these can be displayed to the Health Workforce member in My Health Account Workforce • My Health Account Workforce Users are asked for permission to share their attributes with each Digital Health Service prior to the initial connection with the Service • Digital Health Services are required by Terms of Use to advise My Health Account Workforce if their intended use of the information changes so that My Health Account Workforce can re-prompt Health Workforce members for their permission to share their attributes for the changed use • Health Workforce members can revoke their permission to share attributes with a Digital Health Service at any time. Health Workforce members also need to be made aware that standard uses of their work-related information (for example, for managing their access to Digital Health Services that they need to do their job) will continue to be managed by service providers in accordance with their usual processes and that My Health Account Workforce will not be able to control all access to and use of their work-related information.	
Rule 11	Limits on disclosure of information - Only disclose it if you have good reason	The disclosure enabled via My Health Account Workforce during the verification process is signalled in advance to Health Workforce members, who may then choose to proceed with the disclosures (for example, to Cloudcheck or other authorised third-party identity services). The information disclosed to Digital Health Services about Health Workforce members is first determined as part of the Onboarding process, following a Privacy Impact Assessment. Only information deemed necessary for the Digital Health Services about the Health Workforce member are approved for disclosure to the Digital Health Service. In addition, Health Workforce members are required to approve the disclosure of information to the Digital Health Service before it is shared on the first occasion on which they use the Digital Health Service. At any time, the Health Workforce member can choose to deny or revoke further disclosure of information in relation to that particular Digital Health Service.	**Low**
Rule 12	Disclosure of personal information outside New Zealand	My Health Account Workforce information is hosted in Australia but is held only by Microsoft Azure and Amazon Web Services (AWS) as an agent for Te Whatu Ora and the information may not be used by that contracted provider for its own purposes. Cloudcheck is based in New Zealand but interacts with Australian-based government APIs to check Australian documents, if requested by the Health Workforce member. CentraPass is based in New Zealand but the services that My Health Account Workforce interact with are hosted in Australia (AWS). There will be no disclosure of information made outside New Zealand under the rules identified in Rule 12 for My Health Account Workforce.	**Low**

Rule 13	Unique identifiers - Only assign unique identifiers, where permitted	All Digital Health Services connecting to My Health Account Workforce will be required to be consistent with Schedule 2 of the HIPC as part of the Onboarding process. The Health Provider Index (HPI) – Common Person Number (CPN) is the unique identifier for Health Practitioners in New Zealand and links them to the Health Provider Index. My Health Account Workforce allows individuals that have already been assigned an HPI number (CPN) to add it to their My Health Account Workforce, in order to uniquely identify themselves to Digital Health Services as a Health Practitioner. This complies with the requirements of Rule 13(4) such that any assignment must be by a health agency (in terms of applications / Services authorised to operate with My Health Account Workforce). My Health Account Workforce uses GUID number (globally Unique 32 hexadecimal characters) for its account identifier. It is used only by consuming systems to uniquely identify the User in such a way that the User can change their email address without affecting access to that consuming system in future. It is not shared with or displayed to the User. It is not shared with any party other than consuming applications in a 'behind the scenes' manner.	**Low**

Appendix One – Identification Levels

For My Health Account Workforce User

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

For Digital Health Services authorised to Onboard with My Health Account Workforce

Identification Level established by My Health Account Workforce User	What this Identification Level represents to a Digital Health Service about a My Health Account Workforce User	Information that My Health Account Workforce can share at that Identification Level (as approved during the Onboarding process)	My Health Account Workforce authentication of identity scope associated with this Identification Level
Level 1	This confirms only that the My Health Account Workforce User has a verified email address that has not been used by any other User.	Email address Preferred name (if provided) Mobile number (if provided)	Level 1 identification does not confirm the identity of the User.
Level 2	This confirms the My Health Account Workforce User has a verified email address, and that the User has established a Health Workforce Digital Identity in only one of the following ways: • Attributes: The User has presented an identity document that is verified as matching the User Account name and Date of Birth; OR • Authenticate: The User has been able to verify they have access to a device recorded in Te Whatu Ora records as belonging to a person with the User name. If an HPI number (CPN) is recorded this will have been verified against the Health Provider Index records held by Te Whatu Ora as correct for the person with that User name.	As per Level 1, plus: First name Middle name(s) Last name Date of birth HPI number (CPN) (if added)	Level 2 confirms EITHER that a User's name and date of birth has been confirmed with a document verification process OR that the User has access to a device known to belong to the named person. If a Health Practitioner adds their HPI number (CPN) to their account, Level 2 confirms that there is a match between the Health Practitioner and the HPI number (CPN) provided. Level 2 is not sufficient to authorise any Health Workforce member User to access a Digital Health Service that contains identifiable health information about a Consumer. The Digital Health Service is responsible for: 1. ensuring any onboarded Health Workforce member has an appropriate Identification Level 2. meeting all role-based access control requirements

			3. confirming that a Health Practitioner's annual registration is current. My Health Account Workforce does not show details of any employment role related to a Health Workforce member and, in the case of Non-registered Health Workforce members, does not confirm the person has a Health Workforce role.
Level 3	This level confirms that the My Health Account Workforce User has: • both Verified their name and date of birth attributes via a recognised identity document and authenticated their identity with a device known to be possessed by the User of that name; OR • confirmed their identity with RealMe Verified Services. If an HPI number (CPN) is recorded this will have been verified against the Health Provider Index records held by Te Whatu Ora as correct for the person with that User name.	As per Level 2, plus: HPI number (CPN) (if added)	Level 3 confirms the person has established their Health Workforce Digital Identity, and an HPI number (CPN) connected to that Health Practitioner (if one is provided). The Digital Health Service is responsible for: 1. ensuring any onboarded Health Workforce member has an appropriate Identification Level 2. meeting all role-based access control requirements 3. confirming that a Health Practitioner's annual registration is current. My Health Account Workforce does not show details of any employment role related to a Health Workforce member and, in the case of Non-registered Health Workforce members, does not confirm the person has a Health Workforce role.

Appendix Two – Retention of Identifiable Information

Information attribute	**Retention timeframe**
Email address	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
Mobile number	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
Preferred name	For the duration of the My Health Account Workforce (including changes to these details made by the Health Workforce member).
RealMe account token (identifier)	For the duration of the My Health Account Workforce.
Name (including first, middle, last name)	For the duration of the My Health Account Workforce.
Date of Birth	For the duration of the My Health Account Workforce.
Document check information (including document/card number, expiry date, version number, parent's name)	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
Enrolled General Practice or Medical Centre	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
Address	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
Gender	Only captured at the point of attempting to confirm identity. Information is not retained by the system.
HPI number (CPN)	For the duration of the My Health Account Workforce (or until removed by an Administrator).
Audit records	For a minimum of five years from creation of each record. **Note:** Access to audit records is strictly controlled and limited to Te Whatu Ora staff who are responsible for maintaining security standards and resolving customer support queries

Appendix Three – My Health Account Workforce Privacy statement

Privacy statement

Effective 20 April 2023

My Health Account Workforce is a health workforce digital identity service operated by Te Whatu Ora – Health New Zealand, for members of Aotearoa's health workforce. Find out what work-related information is collected about you if you use My Health Account Workforce, where it's kept, and who can access it.

About My Health Account Workforce

All of Aotearoa New Zealand's health workforce members can set up a health workforce digital identity using My Health Account Workforce. This allows them to connect with relevant digital health services in their health workforce role. This includes health practitioners with a current registration and Common Person Number (CPN), otherwise known as a Health Provider Index (HPI) Number, or other industry-recognised identifier, if approved by My Health Account for this purpose.

At My Health Account Workforce, we know how important privacy is to people in the health sector – both health workforce member information and information about the people to whom they provide healthcare services. This Privacy statement explains how we collect and use your work-related information for a My Health Account Workforce ('Account').

- It's voluntary for you to sign up for an Account.
- My Health Account Workforce is designed to make it easy for you to confirm who you are online and to connect with New Zealand work-related digital health services.
- If you are 16 years or older and a member of Aotearoa New Zealand's health workforce, you can create your My Health Account Workforce.
- The information and services you can access and share via your Account are limited by the level at which you have verified your identity and the Terms of use of any workforce-related digital health service with which you connect.

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

Health workforce members can set up a separate health consumer My Health Account (for when they are receiving health services) and a My Health Account Workforce (for when they are operating in their health workforce role to deliver services).

If you have previously added your CPN to your My Health Account and use it for both personal and work purposes, or if you currently have a separate My Health Account with your CPN added that you use for work purposes only, you will be given support to transition to My Health Account Workforce.

What information is collected

We collect information you provide to us as part of confirming who you are. The information you provide and how you verify your identity sets up a Workforce Account 'Identification Level' for your account. This enables you to connect with work-related digital health services that match your

Identification Level. The higher your Account Identification Level, the surer we can be about who you are, and the more services you can access.

If you are a health practitioner, you can add your HPI number (CPN) to your account if you wish.

Identification Level 1

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

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

Identification Level 2

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

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

You must use either the identity document check, the healthcare provider check, or the My Health Account (consumer) check to reach Level 2. If you provide your HPI number (CPN), we will verify it against our records.

Identification Level 3

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

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

To reach Level 3, you must use:

- your RealMe® Verified account, or
- the combination of the identity document check and the healthcare provider check
- The My Health Account (consumer) check if your consumer account is at Level 3.

Identity document check

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

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

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

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

Healthcare provider check

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

We check the details you give us against the NHI database to link those details to a unique NHI number. We do not retain this NHI detail on your My Health Account Workforce.

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

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

My Health Account (consumer) check

If you have a My Health Account and you have verified your identity to either Level 2 or 3 for your consumer account, you can enter the details of your My Health Account into My Health Account Workforce and the corresponding Identification Level of your consumer account will be applied to your My Health Account Workforce. We will only retain your first name, middle name / s (if you have any), last name, date of birth, and the method you used to verify your identity for your My Health Account, as well as your HPI number (CPN) if it has been added to your My Health Account. No other details from your My Health Account will be stored in your My Health Account Workforce.

Your HPI number (CPN)

If you are a registered health practitioner, you can add your HPI number (CPN) or other approved identifier to your account. Together with the name and contact details you have given us, this enables us to give you access to health workforce-related digital health services, and to record what health workforce-related digital health services you access.

How we use your information

Your My Health Account Workforce information is used to:

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

- protect against and identify fraud and other criminal activity. **Note:** it is an offence to falsely claim to be a health practitioner under section 7 of the Health Practitioners Competence Assurance Act 2003 and could result in a conviction and fine not exceeding $10,000. It is also an offence under section 212(2)(c) of the Privacy Act 2020 to falsely pretend to be an individual or falsely claim to be acting under their authority to obtain access to that individual's personal information.
- comply with and enforce applicable legal requirements, relevant standards, and our policies, including this Privacy statement.
- enable us to prepare reports of statistical information about how services are used (you will not be identified in the reports produced) so that we can monitor and improve the performance of My Health Account Workforce and monitor interactions with participating third-party applications and services using My Health Account Workforce.

The Account allows you to connect with and use participating Te Whatu Ora – Health New Zealand or third-party work-related apps and services:

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

Visit our connected digital health services page on our website for details of how these services use Health Workforce information.

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

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

Account Workforce to allow you to give permission for that digital health service to communicate with you via text message.

How we protect your privacy

We take your privacy seriously.

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

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

How we secure your information

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

Any information you share with Te Whatu Ora – Health New Zealand will not be shared with other Government agencies without your permission or as authorised by law. It will not be used for enforcement purposes unless there is evidence of fraudulent use of the account, or it is required to establish which individual's Account was used to access digital health services in the event of a potential breach of privacy or for other inappropriate activities.

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

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

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

How long we keep your information

Once a My Health Account Workforce account is created, the following information is retained: Applicant name, date of birth, preferred name, email, mobile phone number, and supplied and verified HPI number (CPN). These details are supplied to authorised services connecting to the My Health Account Workforce service as identified in each of the respective service's PIA (and as approved by the My Health Account Workforce service).

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

Tips to keep your My Health Account Workforce secure

- Do not share your account details with other people.

- Keep your password safe.
- If you use a shared device in your workplace, ensure you log out of your account before anyone else uses the device.
- We recommend using a screen lock on your device.

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

Viewing or changing your information

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

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

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

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

Giving feedback

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

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

Statistical information

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

Your My Health Account Workforce details may be used for statistical reporting on the performance of My Health Account Workforce to enable performance monitoring and service improvement. It may also include interactions with integrating work-related applications to identify usage statistics. Your personal information will remain securely contained in our systems and only aggregated information (without your name details, HPI number (CPN), or contact details) will be used in reports created, to preserve individual privacy for reporting purposes.

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

If you have a privacy concern

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

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

Updates to this Privacy statement

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

Privacy Impact Assessment

My Health Account Workforce Privacy Impact Assessment (PDF file)

Download My Health Account Workforce Privacy Impact Assessment (PDF)

My Health Account Workforce Privacy Impact Assessment (Word document)

Download My Health Account Workforce Privacy Impact Assessment (Word)

Appendix Four – My Health Account Workforce Terms of use

Terms of use

My Health Account Workforce is the health workforce digital identity service operated by Te Whatu Ora – Health New Zealand for members of Aotearoa's health workforce. With a My Health Account Workforce, you can gain secure access to work-related digital health services for professional purposes and may be able to securely access health information (subject to the requirements of those digital health services). If you are a registered health practitioner, you can link your HPI number (CPN) to your account.

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

What you are agreeing to

By accepting these terms, you understand and agree:

- you are aged 16 years and over.
- we will act on your instructions without further enquiry provided you have successfully logged in.
- you consent to us sharing your validated My Health Account Workforce identity, and your HPI number (CPN) if you are a registered health practitioner, with the digital health services permitted to connect to My Health Account Workforce..
- the information you submit and verify will be true and accurate and is about you, in your professional capacity as a member of Aotearoa New Zealand's health workforce.
- to any terms and conditions that apply to any digital health services that you choose to use via your My Health Account Workforce.
- that My Health Account Workforce is intended for use by people who are ordinarily resident in New Zealand and are members of Aotearoa's health workforce and services may not be available outside New Zealand.

Note: As a member of the health workforce, you are not able to add your NHI number to your workforce account, nor are you able to access your personal health information or consumer-related digital health services from this account. If you wish to set up a digital identity so that you can access digital health services as a health consumer, you need to set up a separate My Health Account.

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

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

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

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

It is an offence to mislead an agency by impersonating an individual or falsely pretending to be an individual or acting under their authority for the purpose of obtaining access to that individual's personal information and could result in a conviction and fine not exceeding $10,000.

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

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

Privacy and how we use your information

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

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

My Health Account Workforce Privacy statement

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

Disclaimer

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

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

Continuity of service

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

- this is necessary to maintain the integrity or security of related services; or

- your login is being misused or has otherwise been compromised; or
- you breach these terms; or
- we decide to remove or reduce the services available.

Changes to these Terms of use

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

Security

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

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

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

Last updated: 30 March 2023

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

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

Glossary

The following are definitions used in this Assessment:

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

Terms	Description, relationship, and business rules
My Health Account Workforce	The Te Whatu Ora application that enables Health Workforce members to obtain, and assert, a Health Workforce Digital Identity.
Non-registered Health Workforce	Those individuals who are working in roles in Aotearoa New Zealand's health sector but who are not Health Practitioners.
Onboarding	The formal process (including the security and privacy aspects of the service or application) a potential connected Digital Health Service must complete prior to being permitted to use My Health Account Workforce services, which will include entering terms of use.
Privacy Statement Materials	Material to be prepared to inform Health Workforce members in compliance with relevant rules in the Health Information Privacy Code 2020, including rule 3 in particular.
RealMe® / RealMe® Verified	A Consumer-facing digital identity service for government agency use provided by the Department of Internal Affairs. More information at https://realme.govt.nz
Service Provider	A government agency (including Te Whatu Ora) or Authorised Private Entity that successfully completes the Onboarding process and is authorised for their Digital Health Services to connect with My Health Account Workforce to authenticate the identity of Health Workforce members.
Service Provider Terms of use	The terms that will apply to each Service Provider when allocated rights to connect to My Health Account Workforce services.
Te Whatu Ora – Health New Zealand	A Crown agent established under section 11 of the Pae Ora (Healthy Futures) Act 2022
Terms of use	See above **Health Workforce Terms of use**.
User	The individual Health Practitioner or Non-registered Health Workforce member who has obtained a My Health Account Workforce and uses it to interact with Digital Health Services.