# Personify Care Pty Ltd - NZ Privacy Policy

## Your Privacy is important

This privacy policy outlines how Personify Care Pty Ltd ABN 95 601 519 573 and its related bodies corporate and associates (Personify Care, we, us or our) collects, holds, uses and discloses personal information as required by the New Zealand Health Information Privacy Code 2020 as amended and the privacy rules contained in the Privacy Act 2020 as they relate to health information.

This Privacy Statement applies to the use of the Personify Care websites (Sites) and application for mobile devices (Application), including which of our pages or other webpages you have visited, as well as how and what you use the Application for. The Sites and the Application will be collectively referred to herein as the Service.

Personify Care is a platform that allows your clinical teams to provide ongoing support and monitor your recovery beyond your hospital stay or visit to the clinic.

This Privacy Statement is in two parts, Part A deals with Privacy generally and Part B specifically addresses the Health Information Privacy Rules prescribed in the New Zealand Health Information Privacy Code 2020 (as amended) published by the New Zealand Privacy Commissioner.

By using the Service you agree to be bound by this Privacy Statement and the Terms of Use.

## Part A – General Privacy Statement

### Collection of your personal information

We will generally collect personal information about you directly by way of forms and other documents or information you submit to us (whether in paper or electronic form), correspondence you provide to us and telephone calls or meetings with you. We will also collect the information you submit to us through using the Service, such as the information and data that you may enter into the Sites or the Application. We may also collect personal information about you as submitted by your health professionals that are using the Service. However, we will only collect personal information from you after you have chosen to register onto the Service through your healthcare professional and provided us with your consent to collect your information from your healthcare professional.

### Storage of information

We hold personal information in electronic form. We have in place steps to protect the personal information we hold from misuse, interference and loss and from unauthorised access, modification or disclosure.

### Security

When any information is uploaded to your Personify Care account, it sends it over the Internet using Secure Sockets Layer (SSL). This method encrypts the information to help prevent others from reading it while it's in transit from your device to Personify Care.

The health information held is encrypted within the Personify Care system. Further information about the security measures used is contained under the heading Rule 5 – Storage and Security of Health Information in Part B of this statement.

If you're using Personify Care to upload sensitive data, you should properly secure your device. To help do this, you can use anti-spyware and virus protection software. You can also restrict access to your device.

Personify Care has incorporated all reasonable measures to protect your information, however, we are reliant upon you to do the same. Personify Care cannot be held liable in any way for events beyond our control or in any way for accidental or unauthorised access of your information. Unauthorised access could involve someone who is known to you guessing your password or a stranger gaining access to your login details. To prevent this never give your access details to anyone, this includes your password.

## Breach Notifications

As per the Privacy Act of 2020, we are committed to disclosing any potential security breaches that could result in your personal information being disclosed to unauthorised parties. In the unlikely event of such a breach, Personify Care will notify the Privacy Commissioner and the affected individuals (as long as we are not precluded to do so by a law enforcement agency or other legitimate organisation).

## Sharing your personal information

We may disclose personal information to the following kinds of entities for the relevant purposes mentioned above:

- our contractors, consultants, advisers, associates and related entities;
- any industry body, tribunal, court or otherwise in connection with any complaint made by you about us;
- if you have provided us with referees to assist with the assessment of a potential contract between you and us, the referees you have provided;
- if you have provided us with consent to share your health information with your healthcare provider or clinical teams; and
- other entities with your consent or as permitted or required by law.

We may disclose the kinds of personal information listed above to overseas countries. As at the date of this privacy policy the recipients are only located in Australia and New Zealand although the countries in which the recipients are located may change over time.

## How we may use your personal information

We will only use personal information for the following purposes unless otherwise required or permitted by law:

- to provide you with the best possible access to the Service;
- to answer any questions or inquiries you direct to us;
- to allow your health professionals to communicate with you about your care;
- to provide you with marketing materials in relation to offers, specials, products and services we have available from time to time that may be of interest to you;
- to allow you to share health information and other information about you with other Personify Care users that you have already authorised to access such information (e.g.

healthcare professionals providing you with health care services) or otherwise in accordance with the settings that you choose for the Service;
- for our internal management purposes, to manage our relationship with you, and to manage the payment and recovery of amounts payable to us by you or an entity related to you (as applicable); and
- for other purposes which are reasonably necessary in connection with our normal functions and activities.

If we are unable to collect personal information relating to you, we may be unable to provide you with the Service or continue our relationship with you.

## How we use aggregate information and statistics

We may use aggregated information from the Service to improve the quality of Service and for marketing the Service. This aggregated information is not associated with any individual account. We do not use your individual account and individual information for marketing without first asking for and receiving your opt-in consent.

## Record access and controls

You may obtain access to personal information which we hold about you by contacting us using the contact details set out below. When you request copies of your personal information held by us we will endeavour to provide you with such personal information as soon as reasonably practicable. We may require you to verify your identity and specify what information you require. There may be occasions when access to personal information we hold about you is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others.

## Sharing information with applications

We may provide you with information about applications that connect with Personify Care. You can view the applications and should examine their privacy statements and terms of use prior to using them or allowing them access to any of your health information. In order to access Personify Care, the application provider must commit to protecting the privacy of your health data.

No application has access to your information through Personify Care unless and until you opt in to grant it access. You control what health information you allow an application to access and the length of time they can access the information.

## E-mail controls

To keep you informed of the latest improvements, we may send you informational updates from time to time. By creating an account you have given us your implied consent to send you such information. If you do not want to receive such information, you can unsubscribe at any time.

## Use of cookies

A cookie is a data file that a website transfers to your computer. This enables the website to track the pages you have visited. A cookie only contains information you supply. It cannot read data on your computer. There are many types of cookies that may be used for different purposes. For example, some cookies help a website to remember information about your visit, like your preferred

language and other settings while others may identify which pages are being visited or offer security features. Our website may use cookies. You can set your browser to refuse cookies, however, this may mean you are unable to take full advantage of our Service.

### Changes to this privacy statement

We may, from time to time, review and update this privacy policy to take account of new laws and technology, changes to our functions and activities, and to make sure it remains appropriate. We encourage you to review this privacy statement periodically to stay informed about how we are helping to protect the personal information we collect. Your continued use of the Service constitutes your agreement to this privacy statement and any updates.

### Enforcement of this privacy statement

We must comply with privacy legislation when dealing with personal information. If you would like any further information or have any queries, problems or complaints relating to our Privacy Policy or our information handling practices in general, please contact us at:

Privacy Officer, Personify Care Pty Ltd, Suite 31, Allied Health Building, Lot Fourteen, North Terrace, Adelaide, South Australia, 5000, Australia. Email: privacy@personifycare.com

## Part B – Compliance with the Rules contained in the Health Information Privacy Code

The New Zealand Health Information Privacy Code 2020 as amended modifies the privacy rules contained in the Privacy Act 2020 as they relate to health information. Each of these principles is addressed below.

### Principle 1 Purpose of Collection of Health Information

Information is collected and maintained for individuals for the purpose of preparing for treatment or a health procedure and / or tracking their recovery beyond their hospital stay or visit to the clinic. Use of the information for other purposes is not authorised. Express consent must be given by the individual if the information is used for any other purpose.

Aggregated information which has identifying information removed may be used to improve the quality of the services offered on Personify Care, for marketing of Personify Care and for general analysis or population health statistics.

Personify Care does not use your individual account and personal information from Personify Care for marketing without Personify Care first asking for and receiving your opt-in consent.

Personify Care doesn't collect any information other than such that is necessary for providing its services.

### Principle 2 Source of Health Information

The source of the information will come directly or indirectly from you.

This includes the information you authorise to be supplied by your doctor or other health professional.

Personify Care has no control over the content of the information which is provided to you by your Healthcare Provider or other authorised third parties.

## Principle 3 Collection of Health Information from Individual

Information submitted to Personify Care for collection must be specifically authorised by the individual.

Subsequent access to the information by third persons (such as health care professionals and family members) will only be accessible by those persons the individual specifically authorises to have such access.

## Principle 4 Manner of Collection of Health Information

The collection of information will always be undertaken in a manner that is lawful and with the specific authorisation of the individual.

Information entered by an individual (or on behalf of an individual eg. minor in their care) is entirely at their discretion.

If Information is provided on behalf of an individual, it is assumed the provider has the legal right to do so.

Extra considerations are given to collecting information from minors and provisions are available to allow their parents to manage and authorise their release of information (via proxy accounts).

## Principle 5 Storage and Security of Health Information

Storage of information is hosted in a secure environment by a commercially reputable hosting vendor using best practice security techniques.

The information is encrypted within the Service database.

Information delivered to Personify Care from your Healthcare Provider is encrypted during transmission. Your information provided to you via a web browser is encrypted during transmission using the Secure Sockets Layer (256-bit SSL) encryption, using RSA 2048 bits key.

Personify Care is protected by a reputable network Firewall.

Regular Backups are performed to allow system restores to be performed in a disaster recovery situation.

Access to your account is provided through 2-factor authentication of your identity and creating your secure credentials and account sessions automatically logout users after a continued period of inactivity.

Information provided to you from your Healthcare Provider cannot be modified within the system.

We follow strict internal procedures in collecting, storing and disclosing information about you.

## Principle 6 Access to Personal Health Information

We will act reasonably to ensure you will have access to your information at any time.

The exceptions to this include:

- You have been denied access to the Service;
- The Service requires a planned outage;
- The Service experiences an unplanned outage. Such events are considered beyond our control but all reasonable efforts will be used to re-establish the service as soon as possible.

We offer no guarantees that access to your information is available at all times.

Access to your information will be limited to you and the registering Healthcare Provider eg. your doctor, including other clinicians within your Healthcare Provider organisation, other healthcare professionals you authorise and an optional list of individuals involved with your care that you grant access to, such as your family members.

## Principle 7 Correction of Health Information

Information entered by you can be modified at any time.

If you do modify your information you must consider what impact that may have on a person authorised by you who may have previously read the information and potentially acted on it. If this impact is significant you should inform the individual of the change.

You may request that we update or vary personal information that we hold about you using the contact details listed in this document.

## Principle 8 Accuracy of Health Information to be checked before Use

While we will endeavour to ensure that the personal information collected from you is up to date accurate and complete, we will assume that any personal information provided by you is free from errors and omissions. Human error cannot be easily identified by us. Therefore, before using any information all users must take such steps as are reasonable in the circumstances to determine its accuracy.

You may request that we update or vary personal information that we hold about you using the contact details listed in this document.

Users must not act if the information appears incorrect.

If any user acts without taking reasonable steps to determine its accuracy, that user is responsible for their actions and not necessarily the person who provided the information.

## Principle 9 Retention of Health Information

We will retain your information for as long as required or needed to deliver the Service to you.

If your account is blocked because you have abused your access privileges you will be offered the opportunity to obtain a copy of any legitimate health information you have entered.

## Principle 10 Limits on Use of Health Information

Access to your information by you and others is limited to the purpose of your healthcare. Use outside of this purpose is not permitted without authorisation.

Our terms and conditions authorise use of aggregated information which has identifying information removed. This aggregated information may be used to improve the quality of the Service, for marketing of the Service and for general usage analysis or population health statistics.

We do not use your individual account and information from the Service for marketing without us first asking for and receiving your opt-in consent.

## Principle 11 Limits on Disclosure of Health Information

Access to your information will be limited to you and the registering Healthcare Provider eg. your doctor, including other clinicians within your Healthcare Provider organisation, other healthcare professionals you authorise and an optional list of individuals involved with your care that you grant access to, such as your family members.

We may occasionally hire other companies to provide services on our behalf, such as web site hosting; packaging, mailing; answering customer questions about products and services; and sending information about our products, special offers, and other new services. If we provide personal information to such companies, we only provide the personal information they need to deliver the Service. They are required to maintain the confidentiality of the information and are prohibited from using that information for any other purpose.

We may disclose personal information if required to do so by law or in good faith believe that such action is necessary to: comply with the law, comply with legal proceedings served on us or; protect and defend the rights or property of Personify Care; or, act in urgent circumstances to protect the personal safety of users of Personify Care products or members of the public.

We will not otherwise disclose such information that allows you to be identified to anyone without your consent.

## Principle 12 Disclosure outside New Zealand

Any information stored outside the borders of New Zealand will be adequately protected and stored in countries with equivalent privacy protection laws. This guarantee is covered in all relevant contracts. Data will be stored in Australia, in security certified infrastructure, encrypted in transit and at rest.

Australia has comparable safeguards to New Zealand’s privacy laws.

## Principle 13 Unique Identifiers

The primary unique identifier used within the Service is your mobile phone number or email address of your choice, which you have authorised us to use to communicate with you. This identifier may be linked to your National Health Index number, if known, which is allocated to you when you use a service provided by a New Zealand District Health Board such as a public hospital. No other unique identifier is linked to you by Personify Care.

While a mobile number or email address is globally unique we cannot guarantee that it will always be assigned to the same person. If a mobile number or email address is no longer used by an individual it is then typically ‘made available’ to anyone else who wants to use it. In the case of children we allow the use of a parent’s mobile number or email address. Once an individual

becomes 16 years old they become responsible for maintaining their account access by other persons such as their parents.

We are aware that over time you may change your mobile number or email account hence you are allocated a unique system identifier which is inaccessible except by the system.

Updated on 15 December 2020