

Privacy Policy

Introduction

Plena Healthcare and its related bodies recognise the importance of protecting the privacy and the rights of individuals in relation to their personal information. This document is our privacy policy and it explains how we collect, manage and utilise your personal information.

This policy is written in simple language. The specific legal obligations of Plena Healthcare are outlined in the Privacy Act 1988 (Cth) (**Privacy Act**) and in particular in the Australian Privacy Principles (**APPs**) found in that Privacy Act.

This Policy outlines how we comply with all applicable privacy laws, including the Privacy Act, when we collect, hold, use and disclose your personal information.

Overview

This Policy applies if you:

- are one of our customers, clients, contractors or suppliers;
- use any of our products and services;
- visit our website at www.plenahealthcare.com.au or any of our affiliated websites; or
- are employed by us or seeking employment with us,

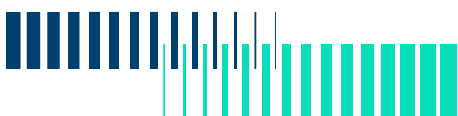
(referred to as **you** and **your**).

By providing us with your personal information, you consent to that personal information being collected, held, used and disclosed in accordance with this Policy.

This Policy is in addition to any other applicable terms and conditions that may apply to your relationship and/or engagement with us.

Personal Information

Personal information is any information that can be used to personally identify you such as your name, address, telephone number, email address and profession or occupation.



If information personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information.

Sensitive Information (Including Health Information)

Sensitive information is a subject of personal information, that is given a higher level of protection by privacy laws. It includes information about an individual's health and includes genetic and biometric information. It also includes information about race or ethnic origin, political opinions, membership of political, professional or trade associations or trade unions, religious beliefs, sexual orientation or practices and criminal record. In this Policy when we talk about personal information, we include sensitive/health information.

Dignity

Plena Healthcare policy and procedures are designed to keep information private and to assist Plena Healthcare representatives in upholding and promoting dignity at all times, for all customers and staff.

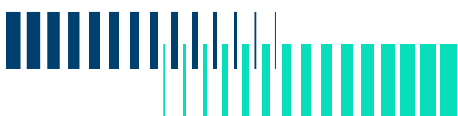
Collection

What information we collect

The personal information we collect will vary depending on the types of services that you request, or your dealings with us. The information collected may include:

General: information as required for our relationship with you, such as:

- Name, address (postal and email) and telephone numbers;
- Gender, date of birth, marital status, occupation and next of kin;
- Your health and medical information, including medical history, condition and treatment plan, contact details for your medical practitioners and treatment providers, and information we are provided with or collect in the course of providing our services;
- Where relevant to your care, information about your racial or ethnic origin, religious beliefs, political opinions or sexual orientation or practices;
- Financial information such as credit card details, health fund and health insurance cover details, workers compensation or other insurance claim details, Medicare details, concession card details;
- Citizenship or residency details
- Driver's licence and passport details



- Information we create in the course of our relationship with you, such as details or evaluations of your interactions with us, including photographs and videos for clinical/care provision purposes)
- CCTV footage from any of our premises;

For current or prospective employees, contractors, suppliers and/or visitors to our premises/sites: information for the purpose of commencing and conducting a business or employment relationship with you. This may include:

- information about your occupation, employment history, education and suitability for the role or relationship, including criminal history, social media profiles and whether you hold any licences/permits required for the role;
- name and details of emergency contacts;
- your car registration information;
- information about your performance in the role or relationship, including results of drug testing (if applicable).
- information for the purpose of health and safety compliance and/or complying with COVID-19 guidelines set down by the Australian Government and Australian State and Territory Governments, to enable Plena Healthcare to make informed health and safety decisions. This may include recent personal health history including details regarding communicable diseases; recent overseas travel, contact with any person(s) who have travelled overseas in the preceding 14 days, have tested positive for COVID-19 or are awaiting test results, or are experiencing any COVID-19 symptoms.

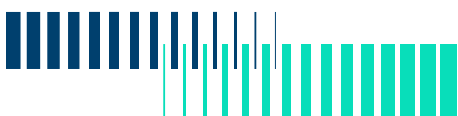
If you have chosen to opt-in to Australia's eHealth record system, then we are required to collect and use your personal information in accordance with the My Health Records Act 2012 (Cth). For more information please visit www.health.gov.au.

If you are a customer at one of our facilities, we may collect your Individual Healthcare Identifier from the Healthcare Identifiers Service Operator and use it for the purposes authorised under the Healthcare Identifiers Act 2010 (Cth).

How we collect your information

We collect personal information from individuals directly where it is reasonably practical to do so. This often takes place in the ordinary course of delivery of a healthcare service such as:

- Through access and use of our website;
- Completing any documentation in order to receive a service;
- Voluntarily providing us with personal information, in person or by telephone, email or other means; or
- By accessing your eHealth record



If Plena Healthcare collects personal information from a third party (i.e. not directly from you), we will take reasonable steps to ensure that you are or have been made aware of our collection of personal information.

We may also collect personal information from third parties such as:

- Where the patient has a Medical Treatment Decision Maker or Support Person;
- From an individual's health service provider including specialists;
- From a health professional who has treated the individual;
- From an individual's health insurer or other insurer;
- From an individual's family;
- Australia's eHealth record system operated by the Commonwealth Department of Health, if you have chosen to participate;
- To assess job applicants (e.g. Criminal History Checks, employment reference checks and Professional Bodies e.g. AHPRA information);
- From publicly available sources.

If you have provided us with information about another person, you warrant that you have that person's permission to do so. Your obligations under Privacy Laws may also mean that you need to tell that person about the disclosure and let them know that they have a right to access their personal information and that we will handle their personal information in accordance with this Policy.

Anonymity

Where it is lawful and practicable to do so, individuals may deal with us anonymously or by using a pseudonym (e.g. when inquiring about services generally). However, if you wish to make a booking with our service, the service will require the provision of personally identifiable information.

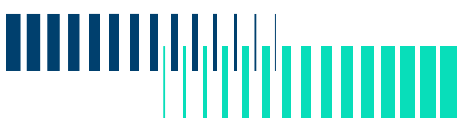
When you request anonymity, Plena Healthcare staff will explain to you or your authorised representative any potential/actual impact this choice has on Plena Healthcare's ability to provide services.

Use and disclosure

Why we collect your information

We collect, hold, use and disclose personal information to:

- To verify your identity;
- To provide our services, including healthcare services and ongoing treatment options to you, and to communicate with you in relation to the products and services we provide;



- To provide information to our related bodies, contractors, allied healthcare service providers or other third parties (such as health care funds) for us to provide health care services to you;
- Comply with applicable laws, regulations, rules, reporting requirements, regulator directions or in response to any lawful request for production of information;
- Undertake accreditation, quality assurance or clinical audits;
- To actively manage and respond to any complaints;
- To undertake billing and debt recovery;
- For the review and development of our products and services;
- Contact individuals to respond to feedback and enquiries;
- To assess suitability of potential employees or contractors;
- To manage and improve our website; and
- Communicate with individuals about our services or offers from our other integrated care providers.

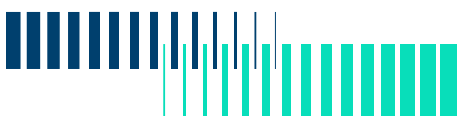
In addition, CCTV footage specifically may be used for the following purposes:

- Detecting and deterring unauthorised access to, and criminal behaviour on, our premises;
- Monitoring the safety and security of our customers, employees, contractors, suppliers and visitors;
- Completing incident investigations; and
- Reviewing the actions of our employees and contractors.

How and when we disclose your information

Subject to any consent exemptions you have given, we may disclose your personal information to third parties such as:

- Treating medical practitioners / general practitioners and related health services;
- Allied health services including pathology, radiology etc;
- Third party contractors who are performing services for us, or on our behalf;
- Government regulator / funding bodies including regulator audits;
- Health funds / Medicare for the purposes of accounting, invoicing, billing and associated reporting / audit requirements;
- Our contractors or sub-contractors for the purpose of providing services to you, or who provide services to us in connection with your services;
- To our related companies in connection with the purposes set out in this Policy;
- Consultancy services, such as accountants, solicitors, business advisors and consultants;
- Authorised third party external audit providers.



We will only disclose information for a purpose other than the primary purposes (above) if:

- You have consented to or requested the disclosure; or
- You would reasonably expect us to use or disclose the information for the other purpose as it is directed related to the primary purpose of collection (i.e. provision of care services to you);
- We believe the disclosure is necessary to prevent or lessen a serious threat to the life, or health or safety of any individual or to public health or public safety; or
- The disclosure is required or permitted by law

We will disclose your personal information to an authorised representative only where written authority has been provided or where evidence has been provided that nominated individuals can act on an individual's behalf. We cannot provide an authorised representative with access to your personal information unless they can demonstrate that they have your consent or have legal authority to do so.

What happens if we can't collect your information

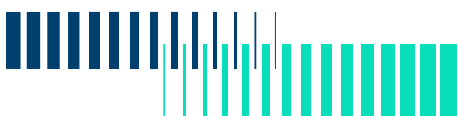
If you elect not to provide us with your information, the following may occur:

- We may not be able to provide the requested products or services to you, including health/care services, either to the same standard or potentially at all;
- We may not be able to provide you with information about the health/care services or products that you want, including information about treatment, contractual obligations, discounts, sales or special promotions; and
- If you are a job applicant, we may not be able to process your application for a position at Plena Healthcare.

Further information regarding the potential impact of choosing not to provide information can be obtained by discussing your concerns with the Privacy Officer.

Data Security and Retention

We take all reasonable steps to protect personal information we hold from misuse and loss and from unauthorised access, modification and disclosure in accordance with applicable legal and regulatory requirements. Plena Healthcare comply with the notifiable data breaches scheme established under the Privacy Act. We regularly assess the risk of loss, misuse, unauthorised access, interference or disclosure of information we hold, assessing and implementing improvements to address identified risks.



All private and health information, whether held in paper, electronic, film, video or audiotape format will be protected. No one is entitled to access any personal information except where such access is in accordance with a person's professional or administrative role.

Personal information is retained for the period of time required for the purposes set out in this Policy, and when no longer required is disposed in a secure manner determined by applicable laws.

Accessing or correcting your information

You are entitled to access the personal information we hold about you at any time and may do so by contacting our Privacy Officer.

Where possible, an access request must be in writing and must provide the name and address of the applicant making the request, provide sufficient information to identify the information to which access is sought, provide a return address (can be email) and note the way in which the individual wishes to have access. We may need to verify your identity before we allow you to access your personal information.

Where we hold your information, we will provide access in a form or manner suitable to your needs, except where we are permitted or required by law to refuse access, such as:

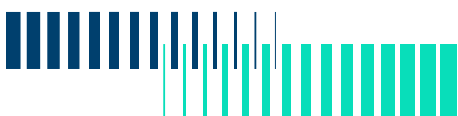
- Providing access would pose a serious threat to the life, health or safety of any individual or to public health or public safety;
- Providing access would have an unreasonable impact upon the privacy of other individuals;
- The request is frivolous or vexatious; or
- Providing access would be unlawful.

We may elect to charge you for our reasonable costs involved in providing access.

We will endeavour to advise you in advance if a charge will be imposed, and the likely amount of the charge. You will be invited to consider other forms of access to minimise cost.

If any of your details have changed please ensure to advise your applicable Plena Healthcare contact or the Privacy Officer to ensure our information is current and complete. If you believe your information we hold is incorrect you may request for it to be updated.

If we refuse access or decline to make a correction then we will provide a notice which sets out the:



- reasons for refusal (except where it is unreasonable to set that out); and
- mechanisms available for you to complain about the refusal.

Access Requests – Legal Representatives

We will disclose your personal information to an authorised representative only where written authority has been provided or where evidence has been provided that nominated individuals can act on an individual's behalf. We cannot provide an authorised representative with access to your personal information unless they can demonstrate that they have your consent or have legal authority to do so.

Cross Border Disclosure of Personal Information

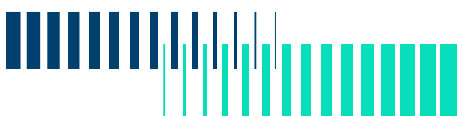
As at the date of this Policy, we are only likely to disclose personal information to our related companies and third parties located in Australia, and a third-party service provider located in the Philippines. We will not otherwise disclose your personal information to anyone located overseas.

For customers based in Victoria or New South Wales, we will not disclose an individual's health information to an organisation or individual outside Victoria or New South Wales (as the case may be) except in accordance with the *Health Records Act 2001 (Vic)* and *Health Records and Information Privacy Act 2002*, such as where:

- The individual has given consent
- Plena Healthcare staff are satisfied that the organisation receiving it is subject to laws which are substantially similar to the existing laws
- The transfer is authorised or required by law
- The transfer is for the benefit of the customer or staff member, it is impractical to get consent but there is reasonable belief that consent would be given

Direct Marketing

You consent to receiving direct marketing communications from us via post, email, phone or SMS in order for us to provide you with information on products or services that you may be interested in or complimentary Plena Healthcare service offerings. Plena Healthcare will not provide your personal information to any third party for marketing purposes.



We will not use your sensitive information for direct marketing purposes without your express consent. If you no longer wish to receive marketing information from us you can notify us by:

- Contacting your service delivery nominated contact or the Privacy Officer;
- Submitting a request via the contact us function on our Sites; or
- Clicking the “Unsubscribe” function in any electronic communications.

Our Websites

Automatic collection of information

Visitors to our website do not disclose personal information unless they provide such information through the enquiry form. When individuals visit our website, non-personal information may be collected including but not limited to browser type, version and language, operating system, pages viewed while browsing the site, page access times and referring website address. This collected information is used solely internally for the purpose of gauging visitor traffic, trends and delivering personalised content to individuals while they are at this site.

Analytics Services

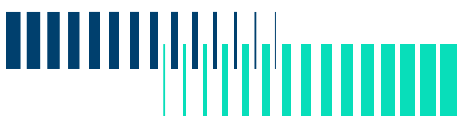
Plena Healthcare may engage third parties to perform functions on our behalf. Some of these third parties are the Google Display Network and Google Analytics. Plena Healthcare and third-parties make use of ‘cookies’ to gather non-personally identifiable information.

Cookies

When you visit one of our websites, a small file called a ‘cookie’ is placed on your hard drive. We use cookies to track your visit. Cookies do not personally identify you; your bank account details or your email passwords. Cookies can be used to collect non-personally identifiable information such as browser type, operating system, pages viewed while browsing one of our websites, referring website address and other metrics. You can set your browser to notify you when you receive a cookie, giving you the chance to decide whether to accept it.

Location based tools

Plena Healthcare may collect information regarding the general geographic location of your computer or mobile device for the purpose of improving location-based service information.



Amendments to this Policy

This Policy is current at **14 December 2020**. We may amend and update this Policy from time to time to take account of new laws and technology, changes to our operations and practices and the changing business environment. The most current version of this Policy is located at <https://www.plenahealthcare.com.au/privacy-policy/> and can be obtained by contacting our Privacy Officer via the details below.

Contacting us

You may contact us to:

- ask questions or give feedback about privacy and the way Plena Healthcare manages personal and health information;
- Request access to your information;
- Request corrections to your information held by Plena Healthcare should you feel it is inaccurate, incomplete, out of date, irrelevant or misleading;
- Seek more information about anything contained in this Policy;
- Request a copy of this Policy in a different format; or
- Make a privacy related complaint.

Our Privacy Officer can be contacted via;

Email: privacyofficer@zenitas.com.au

Telephone: 136 033

By Webform: <https://www.plenahealthcare.com.au/contact-us>

If you believe we have breached your privacy in any way, please contact our Privacy Officer in the first instance. We request that all privacy related complaints be made in writing so we can be clear regarding the details.

We will endeavour to respond to your complaint within 30 days of receipt of your complaint, usually in writing, to provide details of the outcome and invite a response to our conclusions regarding your complaint.

If you are not satisfied with the outcome you also have the right to make a complaint to the Privacy Commissioner via;

Phone: 1300 363 992

Email: enquiries@oaic.gov.au or in writing to:
Office of the Australian Information Commissioner
GPO Box 5218
Sydney, NSW 2001

