Privacy Policy

Please read carefully:

This policy describes how Jenni Suen trading as Cardiovascular Dietetics (ABN: 512 367 298 97) (referred to as 'Cardiovascular Dietetics', we and 'our') is committed to protecting and managing the privacy of Personal Information collected about you through our website (www.cardiovasculardietetics.com.au), email correspondence, at in person and online personalised dietetic services, through GP correspondence and social messaging services as applicable.

Cardiovascular Dietetics is a health service provider operating in Australia and therefore is bound by the legal requirements of the Australian Privacy Principles set out in the Privacy Act 1988 of the Commonwealth. These principles govern the way health service providers collect, use, store, disclose and dispose of personal information in order to provide your a health service and protect your privacy.

Prior to accessing our services, please read this policy and ensure you are fully aware about our practices in protecting and managing Personal Information of our clients and users of our services. If you do not wish for your Personal Information to be collected as outlined in this policy, we may not be able to provide our services to you. To provide health services we are required to correspond with identified individuals and therefore many aspects of the Personal Information we collect are required. In some circumstances detailed in this policy, there will be an option for providing anonymous or pseudonymous information.

If you have any queries or concerns about our management of your Personal Information, please contact Jenni Suen at hello@cardiovasculardietetics.com.au.

Personal Information Collection & Purpose

Our primary purpose of collecting personal information and sensitive information is to provide personalised dietetic consultations and marketing to potential clients. We never sell or rent personal or sensitive information we collect.

We may collect the following types of personal information from our clients, potential clients, website visitors, email subscribers, social media followers or subscribers, service providers and employment applicants. Information collected are for the following purposes:
(1) the administrative purposes of running a dietetic practice (such as contacting and communicating with clients and potential clients, booking consultations and ensuring accurate and safe provision of services, communicating with other health providers

involved in client's care to ensure safe health care),
(2) billing purposes including compliance to the requirements of Medicare, Department of Veterans Affairs, National Disability Insurance Scheme and Private Health Insurance organisations
(3) to conduct activities related to service improvement such as audits, client satisfaction surveys, staff education & staff training,
(4) for marketing our products and services to you and others. This could include updating our clients through emails, invitations or newsletters where an 'Unsubscribe" option will be available to allow you to opt out at any time. Technology that allows us to display advertising to you through the internet such as Google, Facebook and Instagram advertising services could also be used.
(5) in line with ACT and NSW legislation, health information will be kept for a minimum of 7 years after last contact was made, and
(6) as required by law.

Personal information may be collected also when someone (1) visits our website, (2) makes a verbal or written enquiry to us via phone, email, social media, (3) engages with our social media platforms (4) provides contact information as a result of a marketing campaign, (5) completes a New Client Registration Form, (6) purchased a service from us, (7) participates in a program or service provided by us, or (8) completes a survey or questionnaire produced by us.

<u>The types of personal information we may collect from you includes:</u>

- Identifiable personal information: Full Name, Date of Birth, Addresses, Email addresses, Contact numbers, Emergency Contacts, and payment details
- Demographic data: Age, location, occupation
- Transaction data (details about payments and services you have purchased)
- Technical analytic data (captured by our website host or social media platforms such as internet protocol (IP) address, browser type and version, operating system and platform, time-zone and location, aged and gender, devices used to improve the user experience and troubleshoot issues)
- Marketing and communications data (details about your preferences in communication, preferences in receiving marketing and where you heard about us)
- Profile data (including your interests, preferences, feedback and survey responses). Some feedback questionnaires and surveys have the option for providing anonymous or pseudonymous information.
- Satisfaction data (information about your thoughts of our service may be collected as part of our commitment to good quality health care). This data can be provided anonymously or pseudonymously.

Sensitive health information about clients or potential clients is usually only collected from (1) clients we are providing services to, (2) health professionals referring clients to

our services and (3) potential clients who have requested our services. Sensitive health information enables us to provide dietetic care that meets your needs. The information you provide could be disclosed to others involving your health care including treating doctors, specialists, health professionals, carers or family outside of Cardiovascular Dietetics with consent from you or your legal guardian.

Types of sensitive health information we may collect:

- Identifiable information: Full Name, Date of Birth, Addresses, Email Addresses, Contact numbers, Emergency Contacts, Ethnicity, Martial status, Gender, Medicare Card Details, DVA Card Details, Private Health Insurance Details and payment details
- Health information: Medical history, medications, family history, risk factors, allergies, intolerances, adverse events, vaccination history, special dietary choices, social history in relation to diet and exercise and nutrition related history.
- Details of other health providers involved in your care (e.g. Referring Doctor, Usual General Practitioner, Usual Specialists, Exercise Physiologist, Physiotherapist, Nurse Practitioners etc.): Name of health provider, practice and contact information.
- Referral letters, medical reports or information, pathology results, imaging reports, health reports or analyses from you or health providers involved in your care.
- Health information in your digital health record including your healthcare identifier (if you participate and consent to this).

Cookies

Cookies are small data files sent from a website's server to your web browser to be stored on your device. Essential cookies are automatically stored on your device when you access a website to enable data to be transmitted online which is necessary operation of websites. Non-essential cookies or other technologies are placed on your device such as by analytic tools, advertising tools or third-party widgets, with your consent.

Protection and Management of Personal Information Collected

All Personal Information collected is stored on or within:

- Dedicated information storage software such as Client Relationship Management (CRM) software (e.g. Halaxy), nutrition software (e.g. Foodworks Online, Easy Diet Diary), payment/billing software (e.g. Medipass, HICAPS) and secure online health professional correspondence platforms (e.g. Medinexus, Healthlink).
- Any health and medical information emailed to us by others (e.g. clients or health professionals or admin staff), will be downloaded to upload to the CRM, before being erased.
- Personal Information collected is either (1) uploaded to a Client Relationship Management software system and disposed of via a Confidential Document Destruction bin or electronically erased, or (2) numerically or pseudonymously de-

identified and stored for research, where any identifying information is destroyed through disposing via a Confidential Document Destruction bin or electronically erased, or (3) stored in a locked filing cabinet only accessible to staff prior to being destroyed through disposing via a Confidential Document Destruction bin, or (4) stored electronically as a password locked file, until electronically erased.
- The backend of the Cardiovascular Dietetics website
- The backend of our social media accounts such as Facebook, Instagram, Youtube and Twitter.

If we are to use an Artificial Intelligence (AI) medical scribe, we will only use a scribe that is compliant with the Australian Privacy law to protect medical information. We will also obtain your written signed consent via a consent form, separate to the usual registration form.

Cardiovascular Dietetics has contracted Advanced Vascular Care Pty Ltd (ACN: 636 710 355) to provide administrative services to all clients or potential clients who access Cardiovascular Dietetics services at Advanced Vascular Care for in personal consultations. Clients or potential clients that (1) seek information from AVC about Cardiovascular Dietetics and/or (2) are provided care at Advanced Vascular Care (AVC) will have Personal Information stored in AVC's Client Relationship Management software (e.g. Gentu by Genie Solutions) and systems that are owned and operated by AVC staff and protected by their Privacy Policy. AVC is legally responsible for the information collected and stored on their CRM software and devices. Cardiovascular Dietetics will use AVC software and devices when conducting consultations at AVC. AVC software and devices used also meet the security precautions below.

<u>Security of Personal Information</u>

We undertake the following precautions to protect stored personal and sensitive information provided to Cardiovascular Dietetics:

- Our website host provides HTTPS (Hyper Text Transfer Protocol Secure) secure access meaning that the website is protected by SSL (Secure Sockets Layers) technology for keeping an internet connection secure and safeguarding data sent between systems which prevents criminals from reading and modifying any information transferred including personal details.
- All software we use stores your data in Australia and is backed up & encrypted with SSL/TLS.
- Payment details provided are tokenised and encrypted end to end similar to systems systems employed by leading banks.
- The Online Video Consultation platform we use is (1) compliant to Health Insurance Portability and Accountability Act (HIPAA) - which sets the standard for sensitive patient data protection, (2) provides each client with a unique authorisation token required to join the session to prevention unauthorised access and eavesdropping,

and (3) fully encrypts audio and video in transit to AES 256-bit standards including Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Datagram Transport Layer Security-Secure Real-Time Transport Protocol (DTLS-SRTP).
- All conversations including the discussion of personal information take place in private settings where conversations cannot be overheard by unauthorised personnel.
- The backend of our website, online software access accounts and social media accounts are password protected.
- The devices we use are password protected and only accessible to authorised personnel.
- Our devices and locked paper-based document storage are stored in secure premises only accessible to authorised personnel.
- If we no longer need personal information, we take reasonable steps to delete, destroy or de-identify the information.
- De-identified data is stored on secure cloud servers.

Access to your Personal Information

You have the right to request access to personal information collected about you under Privacy Act 1988 of the Commonwealth. In order to protect your Personal Information we will require indication from you or as a legal guardian before releasing the requested information.

For more information on (1) how to request access and (2) examples of valid reasons that access requests are denied, visit https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/access-your-personal-information.

We will respond to any request for access to personal information within 30 days. How access can be provided will be negotiated as required. In most cases we provide access to your personal information, free of charge, but if your request requires significant effort or expense on our part, we might explain this to you and ask for a reasonable administrative fee.

Correction of your Personal Information

It is important to us that your information is up to date to provide you safe and accurate health care. If you believe that any information we hold about your is out of date, inaccurate, incomplete or misleading, please advise us through contacting Jenni Suen at hello@cardiovasculardietetics.com.au as as soon as practicable. This will enable us to update our records and ensure we can continue to provide quality services to you.

Deletion of your Personal Information

You have the right to request for Personal information that is not health information can be deleted. Please advise us through contacting Jenni Suen at hello@cardiovasculardietetics.com.au if you have this request and we will do our best to meet your request within a reasonable timeframe. If your request requires significant effort or expense on our part, we might explain this to you and ask for a reasonable administrative fee.

Privacy Policy Updates

If we decide to change our Privacy Policy, we will let you know through posting our most up to date policy on our website. When published on our website, changes to our policy will take immediate effect and your continued use of our website, social media platforms and services indicated your acceptance of the revised policy.

Privacy Policy Concerns and Queries

If you have any queries or concerns about our management of your Personal Information, please contact Jenni Suen at hello@cardiovasculardietetics.com.au.