Alisha Weston
PRIVACY POLICY

Alisha Weston Pty Ltd ACN 634 154 760 its subsidiaries, related affiliates in Australia trading as *Alisha Weston* (referred to as "*Alisha Weston*", "we" or "us") are committed to protecting and managing personal and health information in accordance with the Australian Privacy Principles (known as the **APPs**) established under the *Privacy Act 1988* (Cth) (**Privacy Act**) and in accordance with other applicable privacy laws.

The APPs provide a privacy protection framework that supports the rights and obligations of collecting, holding, using, accessing and correcting personal information. The APPs consist of 13 principle-based laws and apply equally to paper-based and digital environments.

This document is referred to as our **Privacy Policy**. It describes how we manage and protect the personal and health information of any individuals from whom we collect information from (referred to as "you" or "your"). This Privacy Policy details how *Alisha Weston* collects and uses your information and how it handles, stores, transmits and discloses your information.

Broadly speaking, when we are referring to 'personal information', we are referring to information or an opinion about you, or information that is reasonably recognisable as you, such as your name, date of birth, contact details and Medicare number. It also includes information or an opinion that may or may not be accurate and recorded in a hardcopy form or electronic.

When we refer to sensitive 'health information', we are referring to certain personal information that is more sensitive in nature and includes information or an opinion about your health information, your physical or mental health, any symptoms, diagnosis and treatment given, genetic or biological samples and information, and other information concerning your health and wellbeing needs and ongoing care. Under the APPs, health information is afforded a higher level of protection. It requires us to obtain your consent before collecting this type of information.

This Policy is effective as of 25/10/2023. From time to time, we may need to change it and will post the updated version on our website www.alishaweston.com/privacy-policy. The updated version will take effect immediately when posted on our website. Please check this Policy and our website regularly for any updates.

About *Alisha Weston*

Alisha Weston is a health service provider based in Toowoomba, Queensland, Australia. *Alisha Weston* provides holistic health services, integrative medicine and other health and wellbeing related activities and programs. We collect health information necessary for these health management activities, such as activities reasonably necessary for the ordinary running of a health service and supporting the community's expectation that an appropriately high standard of quality and safety will be maintained.

What types of information do we collect and hold?

The types of information that we collect will vary depending on the circumstances of collection and the nature of our relationship or dealings with you. The information we collect about you will include only information that is:

- reasonably necessary for us to engage with you in the usual course of our business.
- necessary to provide you with services.
- required for administrative and internal business purposes and activities related to the services we provide to you or necessary for the ordinary running of a health service.

The types of information that we collect include:

- Contact Information: your name, date of birth, sex, contact information (address, email address, telephone details) and occupation.
- Health Information: your clinical and health-related information, imagery and diagnostic information and medication details, information about a health service that has or is being provided to you, and details of your religion, nationality, racial or ethnic background and sexual preferences and practices.
- Lifestyle Information: your health information relating to your lifestyle and medical history relevant to providing healthcare services.
- Government Related Identifiers: your Medicare number, Department of Veterans' Affairs file number, individual healthcare or private health insurance number or patient identifier.
- Billing Information: your payment and bank details to process billing and any applicable claims for health rebates.
- Identification Documents: your driver's licence, passport or other photographic identification documents for verification purposes.
- Photographs & Videos: pictures, videos, sound recordings and other audio-visual recordings that you provide to us or authorise us to take of you.
- Employer & Profession: your professional details and information about your employer or an organisation you represent and your qualifications or registrations.
- Social Media Accounts & Handles: your social media accounts, handles, and other personal websites and profiles.
- Location-based information: your location information.
- Cookies & Other Browser or Device Information: your session cookies and persistent cookies when you visit our website or equipment, and other information regarding your device, browser, Internet Protocol (IP) address and URL information. Cookies that we place may be removed by following instructions that are provided by your browser.
- Interaction & Behavioural Information: your interactions, use, habits, behaviours when dealing with us, our website and other applications.
- Employee & Recruiting Information: your qualifications and work history, tax file number, bank details, superannuation information and other information necessary to conduct background checks to determine your suitability for certain positions (for example, positions that involve working with children).
- Other information: any other administrative and additional information that you provide to us directly or provided by the business that employs or engages in facilitating the provision of health services or as a part of your interaction with us.

Consent

As a result of the wide spectrum of information collected and handled by us, this Privacy Policy will apply to many different individuals, which may include clients, healthcare professionals, contracted service providers, students, trainees, suppliers, employees and other individuals with whom we engage in the course of our usual business operation. We may collect personal information about other individuals who are not clients of ours. If you are participating in an event we are managing or delivering; we may take images or audio-visual recordings which identify you.

By providing information to us, or becoming a client of ours, using or receiving health services from us, by participating in a program (including registering as a user of our virtual health services program) or at an event, or being employed or engaged by us, you acknowledge and consent to us collecting, using and disclosing your personal information as described in this Policy, including your health information.

If we need to use your information for anything else, we will seek additional consent from you to do this. In some circumstances, where it is not reasonable or practical for us to collect this information directly from you, responsible persons (for example, a spouse or partner, close family member, parent or guardian, emergency contact or enduring medical power of attorney) can give consent for collection on your behalf. For example, this may occur if a person lacks the capacity to give their consent or communicate their consent on a permanent or temporary basis.

We may also be given information about you by accident or without having requested such information. Therefore, this Policy will apply. Alternatively, we may choose to destroy or de-identify the unsolicited information as soon as practicable, provided if it is lawful and reasonable to do so.

How do we collect personal information?

Generally speaking, we gather, acquire or obtain information about you or your organisation if we receive the information from you directly or from another source. We will usually collect your personal information directly from you by email, telephone, writing, in person, or through our website or social media accounts (such as Facebook and Instagram).

We may also receive information about you that we have taken no active step to collect. If this occurs, then we may keep records of this information or choose to destroy or de-identify the information.

Third Parties

Where it is not reasonable or practical for us to collect this information directly from you, we may collect information about you from a third party. We collect information from third parties that may include:

- other health service providers if they have referred you to us or are otherwise directly involved in your care - such as healthcare professionals, allied health professionals, hospitals and health services, clinics and other pathology practices.
- your responsible persons or authorised persons - such as a parent, guardian, relative or carer.
- our internal records and software management systems to link your information.
- the Australian Digital Health Agency's "My Health Record" system operated under the *My Health Records Act 2012* (Cth) if you have chosen to participate or register.
- health insurers, relevant courts, tribunals or regulatory authorities and law enforcement bodies or other government instrumentalities.
- our affiliated and related entities and organisations.
- our agents, suppliers and contractors who assist us in operating our business and providing services to you.
- recruitment service providers and any referees provided on employment applications.
- payment and debit service providers who process and manage the transaction on our behalf.
- your family and friends through any marketing or promotional activity that we conduct.

Minors

We may collect personal information about children and minors, which may occur when a minor participates in a program run by us. The Privacy Act does not specify an age after which individuals can make their own privacy decisions. As a general principle, a patient under the age of eighteen (18) has the capacity to consent provided they have sufficient understanding and maturity to understand what is being proposed. We assess a minor's capacity to consent on a case-by-case basis factoring in different circumstances.

Where those children and minors do not have sufficient maturity and understanding to make decisions about their personal information, we will require a responsible person to make decisions on their behalf, such as a parent or guardian. In some circumstances, we may be required to keep the health information of a minor in confidence if requested to do so by that minor, which includes where a parent seeks the information.

Where we are unable to distinguish the age or identity of a person accessing and using our services or attending our events or programs, then we may unknowingly collect information from a minor without the consent of a responsible person. If this does occur, we recommend that you contact us as soon as possible.

Dealing with us anonymously

In certain circumstances, you may have the option of dealing with us anonymously or by using a pseudonym. However, this may limit the services that we can provide to you or how we engage with you. It may also limit your ability to claim a health fund or Medicare rebate. In some circumstances, it may be impracticable for us to deal with you in such an unidentified manner.

Additionally, you can decline to give us any personal information that we request from you. However, that may mean we cannot provide you with some or all of the services you have requested or provide you with ongoing care. If you have any questions or concerns about the personal information that we have requested from you, please let us know as soon as possible.

How do we use your information?

We will only use or disclose your personal information for the primary purpose for which it was collected or for a related secondary purpose where it is reasonably expected or directly related to the primary purpose. We can only use or disclose your personal information for another purpose with consent or in certain circumstances.

The exceptions to this are if you have consented to another purpose or if we are permitted or required to do so by law, which may include:

- to coordinate and communicate with healthcare providers, allied health professionals and hospital and health services involved in your treatment and care.
- to coordinate and communicate with non-healthcare providers.
- to obtain additional healthcare services on your behalf (such as referrals to other service providers or when obtaining second opinions).
- to conduct activities related to quality assurance, improvement processes, accreditation, audits, risk and claims management, client satisfaction surveys and staff education and training.
- to liaise with your health fund, Medicare, the Department of Veterans' Affairs, the Department of Indigenous Affairs, Department of Health, Queensland Health, or another payer or contractor of services.
- to fulfil regulatory and public health requirements, including liaising with regulatory or health authorities, as required by law.
- to send you standard reminders (for example, for appointments for follow-up care and account management) by text message, mail or email to the number or address which you have provided to us or last known to us.
- to provide advice or general information to you about products, services, programs, activities, treatment options, research and statistical activities and clinical trials relevant to you.
- to handle a complaint or respond to anticipated or existing legal actions.
- to obtain feedback about our services.
- for billing and payments.
- to engage you (as a contractor) to provide products or services to us.
- to consider your application for employment with our business.
- when required by law to respond to enforcement related activities conducted by, or on behalf of, an enforcement body.

We will not seek your consent to use your personal information for the purposes listed above.

<u>Research</u>
We may collect information from you where it is relevant to public health or public safety and necessary for research, clinical trials, for the compilation or analysis of statistics. When undertaking research or statistical activities, we may engage or affiliate with third party organisations, such as Universities or Health and Hospital Services. Where such research and statistical activities are directly related to the primary purpose that we collected your information, then we may use your personal information for this purpose, provided it is reasonable to do so and following the APPs.

Where we disclose your information to third party organisations for research, clinical trials, or for the compilation or analysis of statistics, we must obtain your consent. We may do this without consent where it is impractical to do so or where we collect the information in such a way that it is de-identified. However, we may also disclose identifiable information where we reasonably believe that the recipient will not disclose the information, or the personal information derived from it. We may obtain confirmation from that recipient as to the requirement of non-disclosure.

We may de-identify or aggregate the personal information that we collect to carry out research and statistical activities, clinical research, quality assurance or customer service improvements, health

outcome and other business analytics. We may use electronic processes when we use your personal information as specified above. We may link, combine or share personal information about you held in various databases created by any, or all, of our businesses.

Direct Marketing

We may use your personal information for marketing and promotional purposes, which is directly related to our services or to inform you about our services, upcoming promotions and events, or other opportunities that may interest you. By doing so, we must comply with applicable laws regarding direct marketing communications, such as the Privacy Act and *Spam Act 2003* (Cth). We may engage third parties, under contract, to provide marketing services on our behalf. If you do not wish to receive direct marketing and promotional material from us, then you may advise us of your marketing preferences at any time by contacting us or by using the opt-out facilities provided in our marketing communications that you receive. If you opt-out of receiving marketing material from us, we may still contact you concerning our ongoing relationship with you.

You can always decline to give us your personal information, but that may mean that we cannot provide you with some or all of the services you have requested.

How do we disclose your personal information?

During the course of providing services to you or otherwise engaging with you, we may disclose your personal information to trusted third parties, including:

- our affiliated and related entities.
- healthcare service providers or other relevant parties involved in your treatment or care, and when requesting services on your behalf (including for the purpose of obtaining second opinions or making referrals for specialist medical services on your behalf). Our providers utilise practice management and clinical software, which may send or share information, referrals and other data. However, only relevant medical information will be shared.
- statutory registries or bodies where requested to do so by you or as required by law (such as national cancer registries).
- commercial partners, universities and hospitals and health services under an agreed information sharing arrangement and for market, research and statistical activities and clinical trials.
- approved and trusted contractors, agents, suppliers or trainees/students, under agreement or contract, as engaged by us to provide professional or administrative services (such as debt collection, information and communication technology providers, specialist clinical services).
- our professional advisors, such as our lawyers, accountants and financial advisors.
- relevant courts, tribunals or regulatory authorities and law enforcement bodies.
- other third parties or organisations, if required by, and to comply with, our legal obligations.

Third Party Disclosure

We recognise that we may release subsequent handling of your information from our effective control when we engage with third parties. Therefore, we take reasonable steps to ensure that the third parties we engage take reasonable steps to protect your personal information following the APPs and in a similar manner with this Privacy Policy. Where we make information accessible to others outside our organisation, or where we outsource any of our services or hire contractors to perform professional services, we will require those third parties, under contract, to comply with the Privacy Act or other relevant privacy legislation and, where applicable, our Privacy Policy. Additionally, the third parties to whom we have disclosed your personal information may contact you directly to let you know they have collected your personal information and to give you information about their privacy policies.

We may also use Google Analytics to help us understand how our customers and clients use our platforms, products and services. You can read more about how Google uses your Personal Information via https://www.google.com/intl/en/policies/privacy/. You may also opt-out of Google Analytics here: https://tools.google.com/dlpage/gaoptout.

We may use electronic processes to disclose your personal information as specified above, where available or relevant. We will not seek your additional consent to disclose your personal information for the purposes listed above.

How do we hold, store and secure your personal information?

We take the protection of your personal information very seriously and is committed to keeping it secure. We take precautions to protect your personal information from misuse, interference and loss and from unauthorised access, modification or disclosure. For example, we may maintain computer and network security, use firewalls and other security methods and other security systems such as user identifiers and passwords to control access to our computer systems.

Please be aware that there is no method of transmission of information over the internet or through electronic storage that is fully secure and safe. We cannot guarantee the security of your personal information that we hold. Still, we do take reasonable steps to protect your information and are committed to keeping it secure. If we are required by law to inform you of any misuse, interference, loss or unauthorised access of your personal information, then we will notify you by either email, telephone, post or by providing notice on our website.

We hold and store your personal information in paper-based files, other electronic record-keeping methods in secure databases (including trusted third party storage providers based in Australia and overseas), which may include cloud-based storage providers.

Paper-based Storage
Personal information may be collected in paper-based documents and converted to electronic form for use or storage (with the original paper-based documents either archived or securely destroyed). We take reasonable steps to protect your personal information from misuse, interference and loss and unauthorised access, modification or disclosure.

Electronic Storage
Your personal information is generally collected in electronic form for use or storage with the third-party storage provider that we engage. Where we use a third-party storage provider, we cannot ensure that your personal information will remain secure as we will not have control over the third-party provider's policies and procedures concerning your information. However, we do take reasonable steps to protect your information and are committed to keeping it secure.

Our websites, applications or email systems may not use encryption or other technologies to ensure the secure transmission and receipt of information via the internet. Anyone using our website or receiving an email from us is encouraged to exercise care in sending personal information or depositing money via the internet. We recommend that you refrain from clicking any unsecured links or opening unknown attachments. If you hold any concerns or become suspicious of any misuse, interference, loss or unauthorised access to our website, our email systems or to our business more generally, we ask that you contact us immediately to verify your concern or suspicion.

Telehealth Healthcare Services

Telehealth is healthcare delivery or related activities that use any form of technology as an alternative to face-to-face consultations. It includes, but is not restricted to, videoconferencing, internet and telephone. It does not refer to the use of technology during a face-to-face consultation. Not all healthcare services are appropriate for telehealth. It is about transmitting voice, data, images and information rather than moving care recipients, health professionals or educators.

Telehealth services may be offered by us to clients. These facilities may involve third-party software, applications and devices that are not controlled by us. When you participate or register for these services, we may disclose your personal information through telehealth services and platforms. We will also collect, handle, disclose and upload and store your health information electronically to our practice management system or other computer-based programs. This is how we offer these services and

provide our ongoing treatment and care. Where possible, we take reasonable steps to ensure those third-party providers who own or manage the software, applications and devices comply with privacy obligations similar to this Policy and in accordance with the APPs.

What are the choices that you can make about your personal information?

At any time, you can request us to:

- delete or destroy your personal information; or
- de-identify your personal information; or
- access or correct your personal information; or
- provide you with a copy of your personal information.

Please understand that we may not be able to entertain your request if it is unlawful to do so or is otherwise impractical or unreasonable to do so at our discretion.

Retention

Until you request for your personal information to be deleted or destroyed, your personal information is kept by us for as long as necessary until it is no longer needed for the purpose for which it was collected and for legitimate or essential business purposes, such as complying with our accreditation standards or legal obligations or to settle disputes. This means that your personal information can be held for some time. In some instances, we may choose to permanently de-identify your personal information instead of destroying it.

Remaining Anonymous & De-Identification

If you contact us with a general question, we will generally not ask for your name unless we need it to handle your question adequately. In other circumstances, we may require you to provide specific details and information to enable us to provide our services to you. We try to provide everyone with the opportunity of staying anonymous or using a pseudonym in their dealings with us where it is lawful and practical to do so. Typically, it is not possible for us to deal with you anonymously or pseudonymously on an ongoing basis. If we do not collect your personal information, we may not be able to handle your enquiry, request or complaint fairly and efficiently.

Accessing your personal information

You are entitled to access or request a copy of your personal information by contacting our Privacy Officer. We must verify your identity to provide you with access, which means that you may be required to supply us with reasonable evidence of your identity. We may charge you or recover reasonable costs incurred by compiling and supplying your information to you.

In some circumstances, we may not be able to provide you with access to your information. This may occur if your request is unreasonable or impractical or where an exception applies under the Privacy Act, or where there is another relevant law to refuse or limit such access. The Privacy Act sets out ten grounds with which we can refuse to give you access to health information. For example, a refusal may occur if we reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety. If you ask us to give a third-party access to your health information, then we must obtain your written consent before giving them access.

Correcting your personal information

You are responsible for ensuring that your personal information held by us is accurate and updated regularly. We will take reasonable steps to ensure the information we hold about you is correct - and that it is not inaccurate, out-of-date, incomplete, irrelevant or misleading.

You can help us to do this by letting us know if you notice errors, inaccuracies or discrepancies in the information we hold about you and letting us know if your details change. It is likely that we will periodically request updates to your personal information or emergency contact details.

On occasion, we may decline your request to access or correct your personal information in accordance with the APPs. If we do refuse your request, we will provide you with a reason for our decision, and, in the case of a request for correction, we will include a statement with your personal information about the requested correction. We must respond to a correction request within thirty (30) days.

Does the European Union General Data Protection Regulation apply to us?

The European Union (the **EU**) General Data Protection Regulation (commonly referred to as **GDPR**) replaces national privacy and security laws that previously existed within the EU with a single, comprehensive EU-wide law that governs the use, sharing, transferring and processing of any personal data originating from the EU. The GDPR applies to the data processing activities of businesses, regardless of size, that are data processors or controllers with an establishment in the EU.

Consequently, Australian businesses of any shape and size may need to comply if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU. There are also some notable differences, including certain rights of individuals (such as the right to be forgotten), which do not have an equivalent right under the APPs and the Privacy Act at this moment in time. However, this may change as the laws surrounding privacy in Australia evolve over time.

Currently, the GDPR does not apply to our business as we do not currently offer our services to individuals located in Europe. Our website does not explicitly target customers located in the EU, nor do we monitor the behaviour of individuals in the EU.

What should you do if you have a complaint about the handling of your personal information?

You may contact us at any time if you have any questions or concerns about this Privacy Policy or about how your Personal Information has been handled. You may make a complaint to the Privacy Officer using the contact details set out below. We may need to verify your identity and ask for further information, in order to investigate and respond to your concern or complaint.

Complaint handling process

Our Privacy Officer will first consider your complaint to determine whether there are simple or immediate steps that can be taken to resolve the complaint. We will contact you within ten (10) days of the date we receive the written details of your complaint to acknowledge that we have received it. We may ask you to provide further information about your complaint and the outcome you are seeking.

Our Privacy Officer will review the way we dealt with your Personal Information, conduct an internal investigation (if necessary) into the complaint and will likely respond to you within fourteen (14) days of the date we acknowledged receipt of your complaint. We will then typically gather relevant facts, locate and review relevant documents and speak with individuals involved.

In most cases, we will investigate and respond to a complaint within thirty (30) days of receipt of the complaint. If the matter is complex or our investigation takes longer than anticipated, we will let you know.

If you are not satisfied with our response to your complaint, or you consider that *Alisha Weston* may have breached the APPs or the Privacy Act, a complaint may be made to the Office of the Australian Information Commissioner (**OAIC**). The Office of the Australian Information Commissioner can be contacted by telephone on 1300 363 992 or by using the contact details on the website www.oaic.gov.au.

Changes to this Privacy Policy?

We may amend this Privacy Policy from time to time. Any updated versions of this Policy will be posted on our website. We recommend that you visit our website regularly to keep up to date with any changes.

If there are any material changes to our Privacy Policy, we will take reasonable steps to notify you by email to your last known email address.

Our contact information

We welcome any comments or questions about our Privacy Policy. All enquiries should be directed to our Privacy Officer at the following contact details:

Attention: Privacy Officer
Telephone: 0408 385 441
Email: info@alishaweston.com

This Privacy Policy was last updated on 25/10/23.