Privacy Policy

Purpose:

The purpose of the Privacy Policy of Able To Wellbeing (We) (ABN: 85 523 328 276) is to outline how we collect, store, use and disclose personal information and what types of information we collect. This Policy also outlines how you can make a complaint about your privacy, what types of personal information We may collect and how you can request access to your information.

Able To Wellbeing are committed to ensuring the safety and protection of your personal information, and we take your privacy seriously. We comply with the *Privacy Act 1988 (Cth)*, the *Australian Privacy Principles* and state legislation where applicable. We are also bound by the requirements set out in the *National Disability Insurance Scheme Act 2013 (Commonwealth).*

We understand that as a health care provider, we are often working with health information about our participants and clients, and we understand that health information is sensitive in nature and needs to be treated carefully.

Scope:

This applies to all staff, contractors, clients, participants, contractors and students.

Definition of personal and health information:

All personal information collected in the course of providing a health service in considered health information.

As defined by the Office of the Australian Information Commissioner, personal information (B.88-B.93) is broad and my include information, or an opinion that may identify and individual. It is defined as 'information or opinion about an identified individual, or an individual who is reasonably identifiable':

- Whether the information or opinion is true or not; and
- Where the information or opinion is recorded in a material form or not.

Examples of personal information include recording of your name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

Definition of sensitive information:

Health information is a subset of personal information. Health information is considered sensitive as stated by the Office of the Australian Information Commissioner (B.141-B.144). Health information means (B.77-B.79):

- Information or an opinion about:
    - The health, including and illness, disability or injury (at any time) of an individual.
    - An individuals expressed wishes about the future provision of health services.
    - A health service provided, or to be provided, to an individual.

- Other personal information collected to provide, or in providing a health service to an individual. This includes personal information such as your name, address, admission and discharge dates and billing information.
- Genetic information about an individual in a form that is, or could be, predictive of the health of that individual or a genetic relative of the individual.

More specially, examples of health information are, as defined by the Office of the Australian Information Commissioner:

- Information about an individual's physical or mental health.
- Notes of an individual's symptoms or diagnosis and the treatment given.
- Specialist reports and test results.
- Physical or biological samples where they could be linked to a participant/client (for example where labelled with the participant/client's name or other identifier)
- Appointment and billing details.
- Prescriptions and other pharmaceutical purchases.
- Dental records.
- Records held by a fitness club about an individual.
- An individual's healthcare identifier when it is collected to provide a health service.
- Any other personal information (such as information about an individual's date of birth, gender, race, sexuality or religion), collected for the purpose of providing a health service.

Types of personal and health information we collect:

In order to be able to provide a high quality and safe service, we are required to collect information from you. The types of information we collect will vary depending on the services we provide to you and the relationship we have with you. Some examples are listed below, but are not limited to this list:

- Details of any other health professionals who may be providing you with a service such as your general practitioner, specialists and allied health professionals.
- Information from the government which may identify you for the purposes of the funding you receive, mainly National Disability Insurance Agency and National Disability Insurance Scheme.
- Details that assist in identifying you such as your name, age, date of birth and gender
- Contact information such as your name, address, phone number, email, guardian and next of kin or representative details.
- Health information which may include your medications, health history, family medical history, reports from other health professionals including pathology results and imaging results, appointment details, prescriptions, dental records, notes regarding your medical diagnosis or history including mental health or disability, observations made by staff.
- Information which will assist in claiming payment through the relevant funding body.
- Information regarding the supports you receive or need to receive.
- Bank account details.

- Undertaking compliance or auditing activities.
- Information regarding feedback (complaints or compliments).

We may also contract out some of our services and where this occurs, we will be required to collect information from contractors to assist in meeting our obligations. This information may include:

- Contractors contact information such as business name, ABN, phone, address, email.
- Mandatory compliance information such as blue card, police check, qualifications, licenses, insurance, NDIS worker screening.
- Information that is not mandatory for compliance such as additional qualifications, quality standards information, policies and procedures.
- Pricing information specific to our business and service delivery.
- Information which will assist in claiming payment through the relevant funding body.
- Health information such as vaccination status.
- Undertaking compliance or auditing activities.
- Information regarding feedback (complaints or compliments).

We may also employ staff to deliver services and where this occurs, we will be required to collect information from employees to assist in meeting our obligations. This information may include:

- Contact details such as name, phone, email, next of kin or emergency contact, address details.
- Mandatory compliance information such as blue card, police check, qualifications, licenses, insurance, NDIS worker screen.
- Health information such as vaccination status and health information.
- Resume, job application and referee information.
- Bank account details.
- Employee records.

There may be instances that information is collected without your consent such as:

- We are required to or authorised by or under an Australian law or a court/tribunal order.
- Where there is a serious threat, and it is unreasonable or impracticable to obtain consent to the collection, and we reasonably believe the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
- When providing a health service and the information is necessary to provide a health service to a participant/client, and either:
    - The collection is required or authorised by or under an Australian law, or
    - It is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which are binding on us.

- In order to undertake a medical history, we can collect information from a participant/client about another individual, without that individuals consent where:
    - It is part of the participant/client's family, social or medical history, and
    - That history is necessary to provide a health service to that participant/client.
- To conduct research, compiling or analysis statistics, management, funding or monitoring of a health service. For example, the collection is necessary for research or statistical activities relevant to public health or public safety, or for the management, funding or monitoring of a health service. Where information is collected under this circumstance and we want to disclose the information, we will take reasonable steps to de-identify the information before disclosing it.
- Taking appropriate action in relation to suspected unlawful activity or serious misconduct.
- Locating a person reported as missing.
- Where it is reasonably necessary for establishing, exercising or defending a legal or equitable claim, or for a confidential alternative dispute resolution process.

How is information collected:

Information will be collected in the format that best supports your preferences and needs, also ensuring it is collected lawfully. This could be in person, via email, through online platforms or forms, social media, or over the phone. Information will not be collected unless it is necessary to be able to deliver services to you.

We aim to only collect information directly from the participant/client, unless it is not reasonable or practical to do so. Examples where collecting health information directly from a participant/client may not be reasonable or practical include:

- In an emergency we may need to collect the participant/client's background health information from relatives.
- Where a participant/client is a child, or an adult who lacks capacity, we may need to collect the information from parents, guardians or relatives, or
- Where a pathologist collects a specimen and related information from a referring provider.

Who do we collect information from:

How information is collected will depend on the various situations or the types of information we need to collect.

Examples of who we may collect information from are:

- Information may be provided directly by you such as contracts you sign with us, forms or documents you fill in, information you provide over the phone or email or other forms of writing or surveys/questionnaires you may complete.
- Information may be provided to us by contract providers.
- If you are an employee for the purposes of your employment
-

- Information from family, friends, representatives, next of kin, Enduring Power of Attorney, police, ambulance services.
- Information from health professionals who provide you with health care such as general practitioners, allied health professionals, specialists, other service providers.
- Other government or non-government organisations connected to your care such as the National Disability Insurance Scheme, National Disability Insurance Agency, My Aged Care, other community-based organisations.
- For prospective employees, prior employers, referees or medical or health professionals.
- Anyone else who you permit us to collect information from.

Responsible person:

Where a participant/client does not have the physical and/or mental capacity, information may be collected and disclosed by a 'responsible person'. A responsible person may be (Guide to health privacy (oaic.gov.au) – page 5):

- A parent of the participant/client.
- A child or sibling of the parent (who is at least 18 years old).
- Spouse or de facto partner of the participant/client.
- A participant/client relative (who is over 18 years old and part of the participant/client household).
- The participant/client guardian.
- A person exercising an enduring power of attorney granted by the participant/client that is exercisable in relation to decisions about the participant/client health.
- A person who has an intimate personal relationship with the participant/client or
- A person nominated by the participant/client to be contacted in the case of an emergency.

A responsible person also includes step relationships, in-laws, adopted relationships, foster relationships and half-brothers and sisters.

How is information used and disclosed:

We may collect, hold, use and disclose personal and health information which enables us to deliver safe and quality care. Information is only used or disclosed for the primary purposes with which it was collected for. Examples of how it may be used or disclosed include, but are not limited to:

- Accessing and reading a participant/client medical file.
- Determining treatment based on a participant/client health information.
- Passing information from our organisation to another organisation, for example, we may share information with other service providers or health care practitioners involved in your care.
- To organise payment for the delivery of services with the relevant funding body or organisation/individual responsible for making payment.
- Communicating with participant/client or representatives.
- Reporting of information which is de-identified.

- Sharing information with government and non-government organisations relating to your care such as the National Disability Insurance Scheme and National Disability Insurance Agency or other community organisations.
- To family members, representative/s, friends, next of kin, emergency contact, enduring power of attorney, emergency services including police.
- Any other party that you consent or request us to share information with.
- Searching electronic records for a participant/client's health information.

For contractors, information may be used or disclosed for the purposes of ensuring the delivery of care, compliances, reporting and in order to make and receive payment for services.

For employees, information is used for the purposes of commencing and maintaining employment such as:

- Making payments for work completed.
- Training and compliances.
- Staff safety and wellbeing including in emergencies.

Information may be used or disclosed for secondary purposes if the below applies:

- The participant/client would reasonably expect us to use or disclose the information for that purpose, and
- The purpose is directly related to the primary purpose of collection.
- Where the participant/client has provided us with consent to share information.

Other situations where information may be used or disclosed for secondary purposes includes (B.131-B.140 and C.1-C.32):

- We are required or authorised by law to use or disclose the information. Examples may include mandatory reporting of child abuse (under care and protection laws) and mandatory notification of certain communicable diseases (under public health laws).
- Situations where we reasonably believe that using or disclosing information is necessary to lessen or prevent a serious threat to life, health or safety of any individual, or to public health or safety.
- Where we reasonably believe that the use or disclosure is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body. Enforcement bodies include Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect public revenue or to impose penalties or sanctions. Enforcement related activities include the prevention, detection, investigation and prosecution or punishment of criminal offences, and intelligence gathering and monitoring activities.
- Where necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety.
- Sharing of genetic information to prevent a serious threat to the life, health or safety of a genetic relative/s.

- Disclosure to a responsible person where the participant/client lacks capacity to consent.
- To take appropriate action in relation to suspected unlawful activity or serious misconduct.
- To locate a person reported as missing.
- Where reasonably necessary for establishing, exercising or defending a legal or equitable claim.
- Where reasonably necessary for a confidential alternative dispute resolution process

There may be situation where your information is shared without your consent. These situations include (C.1-C.32):

- To take appropriate action in relation to suspected unlawful activity or serious misconduct.
- To locate a person reported as missing.
- Where reasonably necessary for establishing, exercising or defending a legal or equitable claim.
- Where reasonably necessary for a confidential alternative dispute resolution process

How do we protect your information:

We have processes and systems in place to ensure the safety and security of your information. Steps include:

- Access and release of information is only on a need-to-know basis and to those people authorised.
- Hardcopy information is stored in a locked area.
- Electronic information is stored securely on an electronic system which is password protected.

We take reasonable steps to ensure the safety and security of your information, including to ensure it is not misused or lost, disclosed without your consent or accessed by an unauthorised person.

Should there be unauthorised access to your data, data lost or disclosed without your consent or information misused, we will notify you as soon as reasonably practicable where it is likely to result in serious harm to you.

De-identification of data[1]:

At times, data may be de-identified. Where robust de-identification of data occurs, then data is no longer considered personal information and is not subject to the *Privacy Act 1988 (Commonwealth)*. Where data is de-identified and no longer considered personal data, it can be used or shared in ways that may not have otherwise been permitted under the *Privacy Act 1988 (Commonwealth).* Personal information is "about an identifiable individual, or an

[1] De-identification and the Privacy Act | OAIC

individual who is reasonably identifiable". De-identified means information has undergone a process of de-identification and no longer falls within this definition.

Reasons why we may wish to de-identify data include:

- To enable the sharing or release of information, for example:
    - We hold sensitive information, which can only be used for a particular, specific purpose. However, another part of the business wants to access that data and use it for an unrelated research or policy purpose. De-identification would allow that data to be shared for a secondary purpose.
    - A government agency wants to make data available for use by researchers and others outside that agency, to:
        - Enable better public participation in government processes.
        - Inform policy and program development and design, or
        - Drive innovation and economic growth by creating new opportunities for commercial enterprise.
- When required by the Australian Privacy Principles.
- When an entity wants to share data or information, but this would not be permitted under the Australian Privacy Principles.
- For other risk-management purposes, or
- To build trust and meet community expectations around the handling of data.

De-identification is the process of removing or altering personal identifiers, followed by the application of any additional techniques or controls required to remove, obscure, aggregate, alter and/or protect data in some way so that it is no longer identifiable (or reasonably identifiable).

Deidentification involves two steps:

- The removal of direct identifiers, such as a name, address or other directly identifying information.
- The second is taking one or both of the following additional steps:
    - Removing or altering other information that may allow an individual to be identified (for example, because of a rare characteristic of the individual or a combination of unique characteristics that that enable identification), and/or
    - Putting controls and safeguards in place in the data access environment, which will appropriately manage the risk of re-identification.

It may also include:

- The use of controls and safeguards in the data environment to prevent re-identification.

Request to remain anonymous:

There may be times where you may request to be anonymous, such as when lodging a complaint. We may be able to accommodate this where it is lawful and practicable to do so. When contacting us, you are able to remain anonymous however there may be instances

where this may not be possible to accommodate. For example, if you are to become a participant/client receiving services, we will require your personal and health information to register you as a recipient of care. We may be able to accommodate a pseudonym, however this may have impacts on our ability to claim payment which will ultimately result in us being unable to deliver services to you.

We may collect anonymous information for the purposes of understanding our business, marketing or social media. For example, we may collect anonymous information from our social media to see how many visits or comments have been made on posts. Or to review the number of visitors to our website. This assists us to make improvements to our services and offerings.

Sharing of information overseas:

It is not our intent to share your data with overseas organisations. However, we are unable to control if other organisations, such as those we may contract to share information outside of Australia. We expect that where information is shared with another organisation, that the organisation the information is shared with take all reasonable steps to ensure the overseas receiver of information complies with Australian laws and the Privacy Principles, and that they do not breach this. Our contracts with other providers will stipulate the same.

Use of social media and online platforms:

We use various social media including, but not limited to, Facebook, Instagram, LinkedIn, YouTube, X (Twitter), Tik Tok and Google platforms. This assists us in proactively marketing our business and sharing with the community the work that we do. Each social media platform has their own privacy policy which you can view through the relevant platform.

We have a website which will track information that supports our business in understanding information such as how many people have viewed our site, types of information accessed, documents downloaded, date and time of visit and search terms used to name a few. We will not attempt to identify who has accessed our website. However, if someone submits an online enquiry or provides feedback through our website, the information you provide on that form will be used for the purposes of the intent listed on the form.

Any information provided to us through forms will not be used for marketing or added to any mailing lists. Information will not be disclosed to anyone else, and email addresses and other information provided will only be used for the purposes of responding to the enquiry on the form.

Use of information for marketing or surveys:

Information will not be used for marketing, surveys or research unless you explicitly sign up for this. Where we do have marketing material or a distribution list, this will be a separate form which clearly outlines the purpose of collecting your information and you will have the option to unsubscribe. Where you do subscribe, information may be shared with you via email, text message, over the phone or through surveys.

Cookies:

A cookie is a data file that transfers onto a computer or other device by a website for the purposes of statistics and to improve user experience. The information collected by cookies is not generally your personal information, because you will not be identified by the cookie. You are able to disable cookies on your computer and you need to do this prior to visiting our website. We will not attempt to identify any anonymous users.

Incorrect data collection:

If you believe that the data we have collected about you is incorrect, outdated, incomplete, irrelevant or misleading, please contact us so your information can be updated. You will need to contact us in writing by emailing info@abletowellbeing.com and outline your request for the information to be corrected. Our aim is to ensure that the information we hold about you is accurate and complete.

We will process your request within 30 days. You may also request that we pass onto other agencies the need to update your data as requested.

If we are not in agreeance with changing your data, we will provide you with written notice of the decision and outline why the request was refused. You are able to lodge a complaint to have this further investigated. How to lodge a complaint is discussed further on in this policy.

Access to your information:

You are able to make a request to access your personal and health information that is held by us. This needs to be done in writing and by completing the 'right to information request' form. This needs to be emailed to info@abletowellbeing.com . You may be charged a reasonable cost for actioning your request, and the cost will be made known to you prior to processing your request so you are aware of the costs. In order to access information, you will be required to provide proof of identity, and you must either be the participant/client making the request, or the person make the request must be a representative or authorised by the participant/client to make the request. This ensures we are only sharing information with authorised people.

How to complain:

If at any time you believe we have breached this Privacy Policy, please inform us in writing by lodging a complaint to info@abletowellbeing.com . We aim to acknowledge your complaint within seven (7) days of it being lodged, and to finalise an outcome within 30 days of the submission of the complaint.

If you are unhappy with our response, we encourage you to lodge a written complaint to the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner is independent to Able To Wellbeing and is the regulatory agency on privacy matters. To make a complaint with the Office of the Australian Information Commissioner,

please visit https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us

References:

- Guide to health privacy by the Australian Government (Office of the Australian Information Commissioner). Guide to health privacy (oaic.gov.au)
- Office of the Australian Information Commissioner. OAIC
- Privacy Policy. NDIS Quality and Safeguards Commission. Privacy Policy | NDIS Quality and Safeguards Commission (ndiscommission.gov.au)
- Australian Privacy Principles. Australian Government (Office of the Australian Information Commissioner). Australian Privacy Principles | OAIC

Review:

This policy will be reviewed in two (2) years' time from the last version date or should there be any changes to the legislation.

Version History:

Version number	Date	Who	Summary of changes
1.0	18/12/2023	Chief Executive Officer	Creation of Privacy Policy
2.0	01/12/2024	Director	Update to Privacy Policy, review of content and formatting.