1800 645 809
hello@medowiehealthhub.com.au
PO Box 264, Medowie NSW 2318

Privacy Policy

1. INTRODUCTION

1.1 The Health Hub by Lotus Assist ("the Company") is required to collect, hold, use and/or disclose personal information relating to individuals (including, but not limited to its clients, contractors, suppliers and workers) in the performance of its business activities.

1.2 The information collected by the Company will, from time to time, be accessible to certain individuals employed or engaged by the Company who may be required to use the information in the course of their duties.

1.3 This document sets out the Company's policy in relation to the protection of personal information, as defined, under the *Privacy Act 1988* (Cth) the ("**Act**"), which includes the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)* and the Australian Privacy Principles ("**APP**"). The APPs regulate the handling of personal information.

1.4 The obligations imposed on the Company under this policy are also imposed on any individual employed or engaged by the Company ("**Workers"**).

1.5 This policy outlines the Company's requirements and expectations in relation to the handling of personal information.

2. PURPOSE

2.1 This policy aims to provide information to clients, on how their personal information (which includes your health information) is collected and used within the Company and the circumstances in which the Company may share it with third parties.

2.2 The policy complement other Company procedures such as complaint resolution and breach notification procedures.

2.3 The policy covers:

- Practice procedures
- Worker responsibilities
- Patient/Client consent
- Collection, use and disclosure of information
- Access to information

3. SCOPE

3.1 This policy applies to all clients and their families/caregivers seen by the Company.

3.2 This policy also applies to all Workers, including but not limited to employees, independent contractors, consultants and other workers engaged by the Company and who have access to personal information in the course of performing their duties.

4. WHY AND WHEN IS CONSENT NECESSARY

4.1 When a person registers as a client/patient of the Company, they are providing consent for our individual practitioners, allied health staff and practice staff to access and use their personal information so they can provide the client with the best possible healthcare. Only Workers who need to see the client's personal information will have access to it. If the Company needs to use their information for anything else, the Company will seek additional consent from the client to do this.

4.2 The Company will need to collect the client and if required the client's family/guardian's personal information to provide healthcare services to them. The Company's main purpose for collecting, using, holding and sharing client personal information is to manage the client's health. The Company may also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (e.g staff training).

5. WHAT IS PERSONAL INFORMATION

5.1 Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

6. KINDS OF INFORMATION THAT THE COMPANY COLLECTS AND HOLDS

6.1 The Company collects personal information that is reasonably necessary for one or more of its functions or activities or if the Company has received consent to collect the information. If the Company collects sensitive information (as defined below), the Company must also have obtained consent in addition to the collection being reasonably necessary.

6.2 The type of information that the Company collects and holds may depend on an individual's relationship with the Company, for example, if a person is a client of the Company, the Company may collect and hold information including the client's name, address, email address, contact telephone number, gender and age and other sensitive information. The information the Company may collect regarding the client may include, but is not limited to:

- Names, date of birth, addresses, contact details of client and their parent/guardian if the client is a child
- Medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- Healthcare identifiers
- Health fund details

6.3 The Company will only collect sensitive information where an individual consents to the collection of the information and the information is reasonably necessary for one or more of the Company's functions or activities. Sensitive information includes, but is not limited to, information or an opinion about racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, membership of a trade union, sexual preferences, criminal record, health information or genetic information.

7. HOW THE COMPANY COLLECTS AND HOLDS PERSONAL INFORMATION

1800 645 809
hello@medowiehealthhub.com.au
PO Box 264, Medowie NSW 2318

7.1 The Company (and the workers acting on the Company's behalf) must collect personal information only by lawful and fair means.

7.2 The Company may collect personal information in a number of ways, including without limitation:

i. When a client makes their first appointment, our practice staff will collect their personal and demographic information via their registration or in person at their first consultation.
ii. While providing medical services, the Company may collect further personal information.
iii. The Company may also collect personal information through the Company website or by technology that is used to support communications between individuals and the Company such as when a client sends an email or SMS or telephones the Company directly.
iv. In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from the client directly. This may include information from:
    - Other family members or guardians
    - Other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services, pathology and diagnostic imaging
    - Out of home care providers, caseworkers, and The Department of Community and Justice
    - Client's health fund, Medicare or Department of Veterans Affairs (as necessary)
v. The Company may also collect personal information through transactions; lawful surveillance means such as a surveillance camera or through publicly available information sources (which may include telephone directories, the internet and social media sites)

7.3 When the Company collects personal information about an individual through publicly available information sources, it will manage such information in accordance with the APPs.

7.4 At or before the time or, if it is not reasonably practicable, as soon as practicable after, the Company collects personal information, the Company must take such steps as are reasonable in the circumstances to either notify the individual or otherwise ensure that the individual is made aware of the following:

i. the identity and contact details of the Company;
ii. that the Company has collected personal information from someone other than the individual or if the individual is unaware that such information has been collected;
iii. that collection of personal information is required by Australian law, if it is;
iv. the purpose for which the Company collects the personal information;
v. the consequences if the Company does not collect some or all of the personal information;
vi. any other third party to which the Company may disclose the personal information collected by the Company;

vii. the Company's privacy policy contains information about how an individual may access and seek correction of personal information held by the Company and how an individual may complain about a breach of the APPs; and

viii. whether the Company is likely to disclose personal information to overseas recipients, and the countries in which those recipients are likely to be located.

7.5 Unsolicited personal information is personal information that the Company receives which it did not solicit. Unless the Company determines that it could have collected the personal information in line with the APPs or the information is contained within a Commonwealth record, it must destroy the information to ensure it is de-identified unless the Company determines that it is acceptable for the Company to have collected the personal information.

8. USE AND DISCLOSURE OF PERSONAL INFORMATION

8.1 The Company may also collect, hold, use and/or disclose personal information if an individual consents or if required or authorised under law.

8.2 The Company may use and/or disclose personal information in regard to client service management, training and events, surveys and general research and business relationship management. This may include, but is not limited to sharing a client or their parent/guardian's personal information:

- with third parties who work with the Company for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with Australian Privacy Principles and this policy
- with other healthcare providers, allied health or NDIS providers
- while providing medical services, through My Health Record (e.g., via Shared Health Summary, Event Summary)
- with out of home care agencies, caseworkers and The Department of Community and Justice
- when it is required or authorised by law (e.g., court subpoenas)
- when making a mandatory child protection notification
- when it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the client/patient's consent
- To assist in locating a missing person
- To establish, exercise or defend an equitable claim
- For the purpose of confidential dispute resolution process
- When there is a statutory requirement to share certain personal information (e.g. some diseases require mandatory notification)

8.3 Direct marketing:

i. the Company may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing (for example, advising a client about new goods and/or services being offered by the Company);

ii. the Company may use or disclose sensitive information about an individual for the purpose of direct marketing if the

individual has consented to the use or disclosure of the information for that purpose; and

iii. an individual can opt out of receiving direct marketing communications from the Company by contacting the Privacy Officer in writing or if permissible accessing the Company's website and unsubscribing appropriately.

9. DISCLOSURE OF PERSONAL INFORMATION

9.1 The Company may disclose personal information for any of the purposes for which it is was collected, as indicated under clause 6 of this policy, or where it is under a legal duty to do so.

9.2 Disclosure will usually be internally and to related entities or to third parties such as contracted service suppliers.

9.3 If a worker discloses personal information to a third party in accordance with this policy, the worker must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPs in relation to the information.

9.4 Only third parties who need to access to a client's information will be able to do so. Other than while providing medical services or as otherwise described in this policy, the Company will not share personal information with any third party without a client's consent.

9.5 The Company will not share client personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without a client or their parent/guardian's consent.

9.6 The Company may use client personal information to improve the quality of the services we offer to our clients through research and analysis of our client/patient data.

9.7 The Company may provide de-identified data to other organisations to improve population health outcomes. The information is secure, cliemts cannot be identified, and the information is stored within Australia. Clients can let Company reception staff know if they do not want their information included.

10. ACCESS TO PERSONAL INFORMATION

10.1 If the Company holds personal information about an individual, the individual may request access to that information by putting the request in writing and sending it to a Company Director. The Company will respond to any request within a reasonable period, and a charge may apply for giving access to the personal information where the Company incurs any unreasonable costs in providing the personal information.

10.2 There are certain circumstances in which the Company may refuse to grant an individual access to personal information. In such situations the Company will provide the individual with written notice that sets out:

- the reasons for the refusal; and
- the mechanisms available to you to make a complaint.

11. CORRECTION OF PERSONAL INFORMATION

11.1 If the Company holds personal information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, it must take steps as are reasonable to correct the information.

11.2 If the Company holds personal information and an individual makes a request in writing to correct the information, the Company must take steps as are reasonable to correct the information and the Company will respond to any request within a reasonable period.

11.3 From time to time, the Company will request that client's verify that their personal information is correct and current. A client may also request that the Company corrects or updates their information.

11.4 There are certain circumstances in which the Company may refuse to correct the personal information. In such situations the Company will give the individual written notice that sets out:

- the reasons for the refusal; and
- the mechanisms available to the individual to make a complaint.

11.5 If the Company corrects personal information that it has previously supplied to a third party and an individual requests the Company to notify the third party of the correction, the Company will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

12. INTEGRITY AND SECURITY OF PERSONAL INFORMATION

12.1 The Company will take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that it collects is accurate, up-to-date and complete.

12.2 Workers must take steps as are reasonable in the circumstances to protect the personal information from misuse, interference, loss and from unauthorised access, modification or disclosure.

12.3 If the Company holds personal information and it no longer needs the information for any purpose for which the information may be used or disclosed and the information is not contained in any Commonwealth record and the Company is not required by law to retain the information, it will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified.

13. DATA BREACHES AND NOTIFIABLE DATA BREACHES

13.1 A "Data Breach" occurs where personal information held by the Company is accessed by, or is disclosed to, an unauthorised person, or is lost. An example of a Data Breach may include:

i. Lost or stolen laptops or tablets;

ii. Lost or stolen mobile phone devices;

iii. Lost or stolen USB data storage devices;

iv. Lost or stolen paper records or documents containing personal information relating to the Employer's clients or workers;

v. Workers mistakenly providing personal information to the wrong recipient (i.e. payroll details to wrong address);

vi. Unauthorised access to personal information by an worker;

vii. Workers providing confidential information to the Employer's competitors;

viii. Credit card information lost from insecure files or stolen from garbage bins;

ix. Where a database has been 'hacked' to illegally obtain personal information; and

x. Any incident or suspected incident where there is a risk that personal information may be misused or obtained without authority.

13.2 If a client or a Worker is aware of or reasonably suspects a Data Breach, they must report the actual or suspected Data Breach to a Director of the Company as soon as reasonably practicable and not later than 24 hours after becoming aware of the actual or suspected Data Breach.

13.3 A "**Notifiable Data Breach"** occurs where there is an actual Data Breach, and:

i. a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation); or

ii. in the case of loss (i.e. leaving an unsecure laptop containing personal information on a bus), unauthorised access or disclosure of personal information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation).

13.4 A Notifiable Data Breach does not include a Data Breach where the Company has been successful in preventing the likely risk of serious harm by taking remedial action.

Assessment

13.5 If the Company is aware of any actual or suspected Data Breach, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that the Data Breach is a Notifiable Data Breach or not.

Notification

13.6 Subject to any restriction under the Act, in the event that the Company is aware of a Notifiable Data Breach, the Company will, as soon as practicable, prepare a statement outlining details of the breach and notify:

i. the individual whose personal information was part of the Data Breach ; and

ii. the Office of the Australian Information Commissioner.

14. ANONYMITY AND PSEUDONYMITY

14.1 Individuals have the option of not identifying them self, or using a pseudonym, when dealing with the Company in relation to a particular matter. This does not apply:

i. where the Company is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

ii. where it is impracticable for the Company to deal with individuals who have not identified themselves or who have used a pseudonym.

14.2 However, in some cases if an individual does not provide the Company with the personal information when requested, the Company may not be able to respond to the request or provide you with the goods or services that you are requesting.

15. COMPLAINTS

15.1 Individuals have a right to complain about the Company's handling of personal information if the individual believes the Company has breached the APPs.

15.2 If a worker becomes aware of an individual wanting to make such a complaint to the Company, the worker should direct the individual to first contact a Director of the Company in writing. Complaints will be dealt with in accordance with the Company's complaints procedure and the Company will provide a response within a reasonable period.

15.3 Individuals who are dissatisfied with the Company's response to a complaint, may refer the complaint to the Office of the Australian Information Commissioner.

16. BREACH OF THIS POLICY

16.1 A worker directed by the Company to do an act under this policy, and which relates to personal information, must ensure that in doing the act they comply with the obligations imposed on the Company. A worker directed by the Company who fails to do an act in accordance with this policy will be deemed to have breached this policy and will be subject to formal counselling and disciplinary action, up to and including possible termination of the worker's employment.