The Bodhi Physio PTY LTD ACN: 694 663 664

The Bodhi Physio
ABN: 266 9466 3664

Privacy Policy

September 2026

What this document is:

- Explains how you collect, use, store, disclose and protect patient information.

Privacy Policy of The Bodhi Physio PTY LTD, operating as The Bodhi Physio in Canberra ACT and NSW, operated by Victoria Tatham as a sole practitioner, who is an APA Title Musculoskeletal Physiotherapist, updated April 2026

Our commitment to your privacy

We are committed to handling personal information about you, including your health information, in accordance with the requirements of the *Privacy Act 1988*.

In this policy, we explain:

- what kind of information we collect and hold about you
- how and why, we collect it
- what we do with your information, who we share it with and when
- your right to seek access to, and if required correction of, the records we hold about you
- your right to make a privacy complaint, to us and others
- whether we disclose information about you to overseas recipients.

What kind of personal information do we collect about you?

We collect and hold the following kind of information:

- your name, address, date of birth, email and contact details
- information about your family or relatives
- information about other health professionals involved in your care
- any government identifiers such as Medicare number, DVA number, Comcare. However, we do not use these for the purposes of identifying you in our practice
- *If you are involved with insurance, like NDIS, other insurance details workers*.
- digital identifiers, such as IP addresses, collected during online services like telehealth.
- other health information about you such as:
- a record of your symptoms
- your relevant medical history
- the diagnosis made and the treatment we give you
- specialist reports
- test results
- your appointment and billing details

- your prescriptions
- your healthcare identifier
- your health fund details
- other information about you collected for the purposes of providing care to you.

How do we collect and hold your personal information?

We collect personal information:

- directly from you when you give us your details (eg, face-to-face, over the phone, via registration form or an online form through Halaxy)
- from a person responsible for you
- from a third party where we are permitted by law to do so (eg, other health care professionals involved in your care, from your health insurer, from the My Health Record system etc.).

We hold your information securely using technical and organisational measures, such as encrypted databases, secure telehealth platforms and restricted-access systems, in line with the *Privacy Act*'s updated security requirements. If you use My Health Record, we access or upload your information securely as permitted by law.

Communication and Referral Information

The Bodhi Physio may receive referrals and communicate with patients, referrers and other healthcare professionals by telephone, email, post and secure electronic messaging.

Where appropriate, clinical information and referrals are recorded and managed through our practice management system, Halaxy. We aim to use secure communication methods for the transmission of sensitive health information.

Patients and referrers should be aware that ordinary email may not provide the same level of security as secure clinical messaging. Where sensitive health information is sent by email, we recommend using an appropriate secure email service or secure file transfer method.

The Bodhi Physio may receive paper referrals by post at its practice PO Box. Paper records are stored securely and managed in accordance with applicable health-record retention and privacy requirements.

Patient contact details are accessed and managed through our practice management system where practicable. We take reasonable steps to prevent unauthorised access to patient information held on mobile devices, computers and other systems used for practice operations.

Legal Compliance Framework

All health information managed by **The Bodhi Physio** complies strictly with the *Privacy Act 1988* (Cth), the NSW *Health Records and Information Privacy Act 2002*, and the ACT *Health Records (Privacy and Access) Act 1997*.

Cloud Storage Security Architecture

- **Centralised Cloud Vault:** Patient clinical records, history profiles, and invoices are hosted directly inside **Halaxy**, a secure, banking-grade practice management system.
- **Zero Local Footprint:** No patient data is stored locally on computer hard drives or unsecure desktop folders. This isolates records from physical device theft or local network hacks.
- **Access Controls (APP 11.3):** System access requires strict user authentication backed by **Two-Factor Authentication (2FA)** and a mandatory **15-minute inactivity auto-logout** protocol.

Secure Transmission Protocol

- **Server-Side Encryption:** Any record requiring external electronic transmission is sent via a premium **Microsoft 365** encrypted mail stream.
- **Identity-Verified Portal:** Non-Outlook recipients securely open documentation using a single-use 6-digit passcode delivered to their verified inbox.

Halaxy: https://www.halaxy.com/

- "Your personal and health information is recorded and securely stored using our practice management system, Halaxy. Halaxy is a cloud-based healthcare management platform. Information may also be processed by third-party service providers where necessary to provide our services.
- Halaxy says its Australian services are subject to the **Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs)**, as well as relevant state/territory health-record legislation.
- Halaxy says it uses:
  - encryption in transit and at rest
  - TLS/SSL
  - AWS hosting
  - daily backups
  - protected data centres
  - physical and technical security measures
  - access controls
  - anonymisation features
  - secure messaging integrations

- Halaxy states that **your data is stored in Australia** and that its Australian data is hosted on **Amazon Web Services (AWS)**. It says the data is protected by encryption both at rest and in transit, and that backups are performed daily.
- *However, **not everything necessarily stays in Australia**. Halaxy's privacy policy says that personal information may be disclosed to overseas recipients where necessary. For example, if you integrate Halaxy with Xero, Xero stores data in the USA. Payment providers can also involve overseas entities.
- Halaxy's Australian practitioner terms say that **ownership/title and intellectual property rights in information you enter remain yours**. You give Halaxy a licence to use, copy, transmit, store and back up that information for providing its services and related purposes.
- Halaxy also states on its website that its software meets **ISO 27001 and healthcare data management standards**.
- Further information about Halaxy's privacy and security practices is available in its privacy policy." https://www.halaxy.com/privacy/au

Why do we collect and use information about you?

We primarily collect and use personal information about you to provide our physiotherapy services to you and to communicate with you and others involved in your care in relation to those services.

We also sometimes use that information for other purposes, including:

- to help us manage our accounts and administrative services, including billing, arrangements with health funds, pursuing unpaid accounts, management of our IT systems
- to conduct accreditation, quality assurance or internal audits.

We may also use de-identified data (where you cannot be identified) to improve our services, such as analysing treatment outcomes for quality assurance.

When and why might we share information about you with others?

We may disclose information about you to others outside of our practice as permitted or required under law. This will include situations where we disclose information about you to:

- comply with our legal obligations (eg, mandatory reporting under legislation, responding to a court order or subpoena)
- consult with other health professionals involved in your healthcare
- get test results from diagnostic and pathology services
- claim on insurance

- communicate with your health fund, with government and other regulatory bodies such as Medicare
- help us manage our accounts and administrative services (eg. billing or debt recovery, arrangements with health funds, pursuing unpaid accounts etc.)
- If you consent to us using your My Health Record, we can upload and download personal information from it.
- lessen or prevent a serious threat to a patient's life, health or safety or a serious threat to public health or safety
- help in locating a missing person
- establish, exercise or defend an equitable claim through the My Health Record
- prepare the defence of anticipated or existing legal proceedings
- discharge notification obligations to liability insurers
- share limited information during a data breach to reduce harm, as directed by law under the 2024 amendments.

We never share your information maliciously (eg, through doxxing, which is now a criminal offence) and only disclose what is necessary for the purpose.

Third-Party Software and Service Providers

The Bodhi Physio uses third-party software and service providers to support the delivery, administration and operation of its physiotherapy practice. These may include:

- **Halaxy:** Practice management, appointment scheduling, clinical record management and related healthcare administration.
- **Healthlink**: Is Australia's largest and most trusted Secure Message Delivery (SMD) network. It acts like a highly encrypted, digital postal service specifically for healthcare professionals. Instead of using unsecure methods like fax, email, or paper post, GPs, specialists, and allied health providers use HealthLink to seamlessly swap referrals, clinical reports, and pathology results.
- **VALD:** Exercise prescription and rehabilitation software, where used, to support the delivery of prescribed exercise programs.
- **Wix:** Website hosting, website administration and online enquiries.
- **Xero:** Accounting, invoicing and financial administration.
- **Australian postal service:** Australian Postal Corporation, ownership**:** Australian Government-owned corporation.

- **Outlook Mail:** is officially called Microsoft Outlook.

These providers may process personal information on behalf of The Bodhi Physio, including information necessary to provide their services. The information shared with each provider is limited to what is reasonably necessary for its intended purpose.

The Bodhi Physio does not sell identifiable patient information or disclose it for unrelated marketing purposes. We take reasonable steps to ensure that third-party providers handle personal information securely and in accordance with applicable Australian privacy obligations.

Some third-party providers may store or process information outside Australia. Where applicable, The Bodhi Physio takes reasonable steps to comply with the requirements of the Privacy Act 1988 (Cth), including the Australian Privacy Principles concerning overseas disclosures.

Patients may contact The Bodhi Physio to request further information about the third-party providers used to manage their personal information.

Secure Electronic Transfer and Management of Clinical Records

Our practice prioritises the privacy, security, and confidentiality of your personal and health information. We handle referrals and clinical communications through the following secure methods:

- **Secure Messaging Networks (HealthLink):** We use **HealthLink**, a secure electronic messaging service, to receive digital referrals, clinical notes, and medical reports from general practitioners and other healthcare specialists. This system uses advanced point-to-point encryption to ensure your data cannot be intercepted during transit.

- **Physical Mail (Australia Post PO Box):** We accept physical, paper-based referrals sent via Australia Post to our **designated PO Box**. Our PO Box is locked and checked exclusively by authorised practice staff.

- **Secure Storage, Digital Verification, and Destruction:** All physical referrals received via our PO Box are promptly digitised and transferred into **Halaxy**, our cloud-based Practice Management Software (PMS). To maintain data integrity, we perform a strict digital verification process to ensure the electronic scan is complete, accurate, and perfectly legible. Once successfully verified and securely stored in Halaxy, the original paper source is immediately destroyed using high-security confidential shredding.

- **Data Retention Compliance:** Our practice strictly adheres to Australian health record retention laws. Verified digital patient records are maintained securely in Halaxy for a minimum of **7 years from the date of the patient's last consultation** (or, in the case of minors, until the patient reaches **25 years of age**), after which they are permanently and securely deleted.

Your right to seek access to and to seek correction of the information we hold about you

You have the right to seek access to and correction of the personal information we hold about you.

The request may incur a fee, which we have outlined below into separate categories. *Please note fees may have slight increase with the end of each financial year that is reasonable:

Patient request	**Fee ($AU)**
Transfer records to another treating practitioner for ongoing care.	Free
Send records to GP or Specialist care	Free
Correcting an error in their record	Free
Patient asks to access/view their records	*$18.95 for viewing a health record
Electronic copy of existing records	Health record fee: *$18.95 for electronic delivery
Hard copy up to 50 pages.	Health record fee: *$1.042 per page for hard copy, Maximum *$52.10 for a hard copy up to 50 pages. More than 50 pages attracts an additional *$0.45/page.
Patient wants to view/ discuss their records with you	Normal consultation fee
New assessment required to produce report	New consultation fee + report *fee

Patient request	**Fee ($AU)**
Detailed report/summary prepared specifically for the patient. Separate fee schedule for:	Specific fee's below:
Standard clinical letter/ report	*$104
Detailed clinical report	*$204
Insurer reports	*$204 per hour *understanding there a caps with insurance reports, which I will consider if possible to reproduce
NDIS report	*$204 per hour Complex $350 + *understanding there is a cap
Workers compensation reports	*$204 per hour
Medico-legal/ solicitor requests	*$204 per hour
Detailed functional capacity report	*$204 per hour
Court/ expert report	*$204 per hour

We will normally respond to your request within 30 days. To make the request, you should contact us in writing sending an email to The_Bodhi_Physio@outlook.com

- By Law, you can also request this verbally during our consultation or via phone call, however I would appreciate this also to be followed up in writing.

If you think that the information we hold about you is not correct, let us know in writing. We will take reasonable steps to correct your personal information where the information is not accurate or up to date. From time to time, we may also ask you to verify that the information we hold about you are correct and current. And please notify us if your contact details change.

See end of the document how to contact us via phone.

Security: how we hold your personal information

We take reasonable steps to protect the information we hold about you. These are designed to prevent unauthorised access, modification or disclosure and to prevent misuse and loss.

We protect your information using technical measures with encrypted databases, secure telehealth platforms via Halaxy and strong passwords and organisational measures with, staff training, confidentiality agreements, access restricted to need-to-know. We store paper records in locked cabinets and digital records on secure servers or cloud storage compliant with Australian law. We also maintain a data breach response plan to act swiftly if unauthorised access occurs, in line with the *2024 Privacy Act* updates.

Concrete Technical & Organisational Measures

- **Encryption (Technical):** Sending clinical files/plans exclusively via your premium Outlook **Encrypt** portal.
- **Firewalls & Endpoints (Technical):** Enabling standard device firewalls and keeping operating systems updated on your work computer.
- **Staff Training (Organisational):** Reviewing data breach SOPs and practicing how to spot phishing/scam emails targeting allied health practices.
- **Access Controls (Organisational):** Locking devices when leaving them unattended and enforcing your newly activated **Multi-Factor Authentication (MFA)** for Halaxy and outlook email access and for work phone access.

APP 11.3 Data Security Audit Steps

- To satisfy APP 11.3 requirements for destroying or de-identifying data no longer needed, perform these actions:
- **Encryption Audit:** Double-check that your Outlook default signature is set to "Standard" and your "Patient Care" signature is manually paired with the **Encrypt** button during active use.

- **Access Control Audit:** Visit your Microsoft Security Dashboard once a month to review active login locations and remove any old, trusted devices.

Phone:

- **Secure Phone protocol.**
- Never save the patient/ client's name or number into the work iPhone
- **Outbound call to patient/ client:** Open the Halaxy via app or log phone's web browser. Search for the secure file to find their phone number. Tap the phone number inside Halaxy to initiate the call. The phone is using the Belong service network, but the patient's health identity remains safely locked inside the Halaxy cloud database.
- **Receiving an inbound call from a patient/ client:** Numbers are not saved in your phone, the will shoes raw mobile number. Answered the call professionally. 'Hello, The Bodhi Physio, 'Name' speaking.'
- **If leaving voice a voicemail:** Belong voicemail service will hold it securely on the network. We Listen to it, log any vital health requests into Halaxy, and immediately delete on your keypad to wipe it from the network.
- **End of Day iPhone Digital Purge:** To comply strictly with APP 11.3 standards and ensure zero local data storage. End of every working day recent calls are cleared.

Telehealth:

- We use telehealth via Halaxy which use secure, encrypted platforms for telehealth, complying with the Privacy Act's technical security requirements to protect your information during virtual consultations.'

Email Security:

Health Information Security & Electronic Communications Disclosure

At **The Bodhi Physio**, we take the privacy, confidentiality, and security of your personal and health information very seriously. This statement outlines our compliance obligations and the advanced technical measures we deploy to safeguard your data under Australian law.

We also will endeavour to communicate through Halaxy secure portals, message and email and integrated health link. However, on rare circumstances, we may use outlook with encryption and not store any clinical the information within Microsoft outlook.

1. Statutory Compliance & Legal Framework

Our handling of health information complies with the strict statutory requirements governing private allied health practices across the Australian Capital Territory (ACT) and New South Wales (NSW):

- **Commonwealth Jurisdiction:** The *Privacy Act 1988* (Cth) and the *Australian Privacy Principles* (APPs).
- **ACT Jurisdiction:** The *Health Records (Privacy and Access) Act 1997* (ACT) and its *Health Privacy Principles* (HPPs).
- **NSW Jurisdiction:** The *Health Records and Information Privacy Act 2002* (NSW) and its *Health Privacy Principles* (HPPs).

Under these laws, clinical records, treatment histories, invoices, and health communications constitute sensitive data that must be strictly protected against unauthorised access, alteration, or disclosure.

2. Digital Security Architecture (Microsoft 365 Premium)

To meet our legal obligations to secure health data in transit and prevent privacy breaches, we enforce digital data encryption using institutional-grade infrastructure:

- **Advanced Email Encryption:** All electronic communications containing clinical records, referrals, medical files, or personal identifiers are securely processed via a **Microsoft 365 Premium** environment.
- **In-Transit Protection:** When we dispatch communications to you, the email text and all digital attachments are locked within a secure cryptographic wrapper (AES-256 equivalent standard). This prevents unauthorised interception by third parties while moving across the internet.
- **Access Restricted Controls:** This protocol prevents data from being crawled, indexed, or casually viewed by intermediate mail servers or network operators.

3. Accessing Your Secure Patient Documents (Instructions for Recipients)

- If you do not utilize a Microsoft-hosted email client (such as a personal @outlook.com domain), your native email provider (e.g., Gmail, Bigpond, iCloud) will receive an unencrypted notification containing a secure, external access portal.
- **Access Link:** Open the email and select the link marked **"Read the message"**.
- **Identity Verification:** On the secure Microsoft webpage, choose **"Sign in with a one-time passcode"**.
- **Passcode Retrieval:** A temporary 6-digit pin code will instantly be generated and sent in a separate message to your regular inbox.
- **Decryption:** Enter that 6-digit code into the portal to securely decrypt, read, and download your clinical documents.

4. End-to-End Secure Continuity (Replies)

- Any digital reply initiated directly within an encrypted email thread sent from **The Bodhi Physio** is automatically wrapped in the same premium security protocol. Any patient notes, updates, or sensitive attachments you send back to us through that thread will remain legally compliant and securely encrypted.
- **Please note: Brand-new email threads started from a standard, non-encrypted personal account do not inherit these server protections until we safely ingest them into our secure network environment.**

Your right to receive treatment from us anonymously (or by using a pseudonym)

Where it is lawful and practicable for us to do so, you can be treated anonymously or through use of a pseudonym (a name other than yours).

Note that anonymity may not be possible for services requiring identification, such as Medicare or health fund claims.

Disclosing information about you overseas

We do not intentionally disclose your information overseas. If we use cloud storage, we ensure providers comply with Australian privacy laws and made best efforts to investigate where information is stored and used by third parties mentioned as above in the **Third-Party Software and Service Providers** section**.** Should we need to transfer your information abroad, we'll seek your consent unless required by law.

We may disclose your personal information to the following overseas recipients:

- any health professional who helps us to provide our physiotherapy services to you (eg, health professionals who treated you when you were overseas) or anyone else you authorise us to contact
- overseas cloud-based storage

What we will do if we have a data breach

If we suspect a data breach, we'll assess it promptly, notify the OAIC and affected patients within 30 days (or sooner if required) and take steps to prevent harm, as mandated by the *2024 Privacy Act* amendments.

If you have a privacy-related concern about us

If you're concerned about how we've handled your privacy, contact us in writing at The_Bodhi_Physio@outlook.com. We'll respond within 30 days. You may also complain to the Office of the Australian Information Commissioner (details below) or seek redress for serious privacy breaches under the *2024 Privacy Act* amendments, even without proving harm.

Office of the Australian Information Commissioner

Phone: 1300 363 992
Email: enquiries@oaic.gov.au
Post: GPO Box 5218 Sydney New South Wales 2001

Website: www.oaic.gov.au/privacy/privacy-complaints/

Updating this policy

We will update this policy from time to time, to reflect any changes in our information-handling practices or the law or both. We will notify you of changes to the policy by:

The Two-Step Approach

Step 1: Direct Email Broadcast (The Legal Anchor):

- Send a single, clean mass email to your current active patient list. This satisfies legal communication standards because it arrives directly in their personal custody.

Step 2: Website Homepage Resources (The Public Proof):

- On the website, a temporary notice banner at the very top of your homepage for 30 days. It will be linked directly to your updated Privacy Policy document.

Step 3: The Bodhi Physio business premises in Lyneham (Printed format).

- I have printed hard copy and is stored in the clinic location (Lyneham) or within my place of business and can show when requested.

How to contact us

To contact us about any privacy related issues, please approach:

Email: The_Bodhi_Physio@outlook.com

Phone: 0483 696 270

Website: www.thebodhiphysio.com.au

Mail Address: P0 Box 542 Dickson ACT 2602

Document created by

Victoria Tatham



Director of The Bodhi Physio

APA Titled Musculoskeletal Physiotherapist (MACP)

Effective Date: 15 September 2026
Policy Version: 2 .0
Review Date: August 2027