

Boab Health Services & Outback Care Privacy Policy

1. Purpose

Boab Health Services and Outback Care are committed to protecting the privacy of all individuals we work with. This policy explains how we collect, use, share, store, and protect personal information in line with:

- Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth)
- Notifiable Data Breaches (NDB) scheme
- Western Australia's new Privacy and Responsible Information Sharing legislation (2025)

The purpose of this privacy policy is to:

- Clearly explain Boab Health's personal information practices
- Help individuals and staff understand what personal information is held and how it is handled
- Describe compliance with privacy laws
- Detail data breach management procedures

Our goal is to assure clients, staff, and partners that their information is protected, respected, and handled responsibly.

2. Scope

This policy applies across all areas of Boab Health Services and Outback Care, to all staff, students, contractors, and volunteers.

3. Definitions

Term	Description
Privacy legislation	Privacy Act 1988 (Cth), Privacy Amendment (Enhancing Privacy Protection) Act 2012, Australian Privacy Principles (APPs), Privacy Amendment (Notifiable Data Breaches) Act 2017
Australian Privacy Principles (APPs)	Summary available from Office of the Australian Information Commissioner's website: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/
Personal Information	Any data that can identify you (name, address, DOB, contact details)
Health Information	Medical history, treatment notes, reports from clinicians
Sensitive Information	Details about your race, culture, religion, or beliefs
Biometric Information	Face scans, fingerprints, or voice recognition data
Location Information	GPS, check-ins, or other geolocation data
Inferred Data	Information generated by analytics, profiling, or AI systems
Cookie	A small text file our website may place on your computer as a tool to remember your preferences
Data Breach	Unauthorised access, disclosure, or loss of personal information

4. Governance & Responsibilities

- CEO: accountable for compliance.
- Privacy Officer: responsible for day-to-day privacy management, monitoring compliance, and reporting.
- Annual Review: Boab Health Services will review this policy each year and publish this policy.

5. Description

What is personal information?

Type of Information	Examples
Personal information	Your name, Your address, Your date of birth
Health information	Reports from doctors, Reports from other clinicians or health professionals, Information from other health or specialist services such as medications and health conditions
Sensitive information	Your racial or ethnic origin, Your culture, Your religion

Why does Boab Health Services collect information?

Boab Health Services collects personal information only when necessary for our operations. Examples include:

- when you provide information (e.g., consent forms, training registration, complaints, service enquiries)
- to deliver requested products or services (e.g., email subscriptions, buying medical equipment)
- for employment or job applications
- from service providers
- to improve services through website data analysis (see section 7.1)

Where is this information stored?

We keep your personal information safe. Only authorised staff who need to see it will have access. If you stop receiving services, we ensure your information remains secure. All data and documents are stored on secure servers within Australia.

How can I access my personal information?

You can request access by contacting the CEO or Privacy Officer using the details in section below. You may also request access from a treating clinician where practical.

How can I change my personal information?

You can update your details by contacting our Reception (08 9192 7888, reception@boabhealth.com.au) or asking your treating clinician.

Communications and Social Media

Boab Health may use subscriber lists (e.g., Newsletter). These always include an unsubscribe option.

Boab Health manages information on social media responsibly and will never publish another person's personal information without explicit (informed) consent.

6. Training and Education

Audience	Frequency	Format	Platform / Resources
All staff	On commencement and annually	Self-paced + Induction	OAIC e-learning – Privacy in Practice (3 short modules: Module 1 , Module 2 , Module 3) + internal induction modules
Managers & Privacy Champions	Annually + as needed	Workshops + Case studies	OAIC Privacy Officer Toolkit (case studies, breach guidance, PIA support) + Privacy Officer-led sessions
Privacy Officer	Ongoing CPD	Advanced training	OAIC Privacy Officer Toolkit + OAIC video library + OAIC e-learning hub (incl. PIA course) + sector updates

7. How We Collect & Use Information

Directly from you	Treating clinicians or health professionals	Boab Health Services and Outback Care websites and digital services	Use of information for secondary purposes
forms, consent, conversations, services provided	with your consent	analytics, cookies	never without consent, unless required by law

8. Information Sharing

- We may share information with trusted partners (e.g. WA Health, other agencies) only under information-sharing agreements that meet WA's new responsible sharing rules.
- Data will never be sold or provided to third parties for commercial purposes.
- Social media: Boab Health Services and Outback Care will only publish personal information with **explicit (informed) consent**.

8.1. Privacy on the Website

In complying with privacy legislation Boab provides the following advice to users of our websites (www.boabhealth.com.au and www.outbackcare.com.au):

What personal information is collected on the website?

Unless the website asks for specific personal information to respond to requests or register for services, only the following information will be collected:

- your server address
- your top-level domain name (e.g., .com, .gov, .au)
- the date and time of your visit
- the pages you accessed, and the documents downloaded
- the previous site you visited
- the type of browser you are using

This information is collected for analytical purposes and to help us understand and improve website traffic and usage.

Who is collecting personal information on the website?

The above information is collected by our Internet Service Provider and website management service. Where the site specifically asks for personal information, it will only be collected by Boab Health staff responsible for those services.

Cookies and analytics

Our website uses Google Analytics, which collects traffic data but does not identify individuals. Reports help us improve the site. You can refuse cookies in your browser, though some features may be limited. By using our site, you consent to Google processing your data per their Privacy Policy. To opt out, disable cookies, JavaScript, or use Google's opt-out tool.

Our site also connects with social media platforms. If you share or like content, please review those services' privacy policies.

How is personal information used?

Personal information collected on this website will only be used for the purposes stated at collection. It will not be added to mailing lists or used for any other purpose without consent.

9. Storage, Retention & Disposal

- All personal information is stored on secure Australian servers.
- Retention follows WA legislation for health and corporate records.
- When information is no longer required, it will be securely destroyed or permanently de-identified.

10. Access & Correction

- You can request access to or correction of your information by contacting the Privacy Officer or CEO.
- We will respond within 30 days.
- If we cannot provide access, we will explain why and outline review options.

11. Children & Vulnerable Persons

We apply extra safeguards when handling personal information about:

- Children and young people.
- Aboriginal and Torres Strait Islander clients.
- People in vulnerable circumstances.

Consent will be sought from parents, guardians, or legal representatives where appropriate.

12. Privacy by Design

- All new systems, programs, or technology will be assessed with a [Privacy Impact Assessment \(PIA\)](#).
- Projects will follow a “privacy-first” approach to minimise risks before launch.

BEST PRACTICE IT SECURITY MEASURES TO PREVENT BREACHES:

- Use multi-factor authentication (MFA) for all systems
- Ensure strong password protocols and regular updates
- Implement screen-lock policies
- Restrict access based on role (least privilege principle)
- Create a strong information management framework
- Conduct simulated phishing exercises
- Train staff
- Do not open suspicious emails or links, notify external IT provider (Best IT)
- Use endpoint protection via Microsoft Defender and Sophos
- Maintain secure SharePoint access and discourage personal storage of client data

12.1. Use of Artificial Intelligence (AI)

Boab Health may use AI tools and automated systems to support service delivery, internal operations, analytics, and digital communications. Where AI is used:

- Personal information will only be processed in compliance with privacy legislation and ethical standards.
- AI-generated inferences or recommendations will be de-identified if they could identify or affect an individual and will be protected as personal information.
- Individuals have the right to request human review of decisions significantly affecting them if such decisions were supported by AI systems.
- Boab Health will apply additional safeguards and conduct Privacy Impact Assessments where AI projects involve sensitive information.

13. Data Breaches

Boab Health Services follows the Office of the Australian Information Commissioner's (OAIC) best-practice approach to managing data breaches. A data breach occurs when personal information is lost or subjected to unauthorised access or disclosure.

FOR EXAMPLE:

- A device containing client information is lost or stolen
- A staff email is compromised through phishing
- Personal information is mistakenly sent to the wrong person

BOAB'S RESPONSE PROCESS:

Step 1: Contain the breach

- Immediately isolate the affected system or device (e.g., revoke access, change passwords)
- Notify IT support to begin investigation and secure systems
- Alert the Privacy Officer and CEO

Step 2: Assess the breach

- Identify the type and sensitivity of the information involved
- Determine how many people are affected and the potential harm (e.g., identity theft, reputational damage)
- Engage IT support to perform a digital audit and trace the breach path
- Complete an internal privacy breach report template

Step 3: Notify if required

- If the breach is likely to result in serious harm, Boab must notify the individuals affected and the OAIC under the Notifiable Data Breaches (NDB) scheme
- Use the OAIC's Notifiable Data Breach statement form to report the incident
- Notify all affected clients with practical support and information

Step 4: Review and prevent

- Conduct a post-incident review with the Privacy Officer, IT, and leadership
- Update internal controls or protocols where needed
- Deliver targeted staff training to address identified weaknesses

14. Complaints Handling

How can I make a complaint about privacy?

You can make a complaint if you are unhappy with how we:

- Collected your personal information
- Store your personal information
- Share your personal information

How to lodge a complaint

To make a complaint or request about privacy, please contact our CEO or Privacy Officer:

- Phone: 08 9192 7888
- Email: reception@boabhealth.com.au (Attention: CEO)
- Post: PO Box 1548, Broome WA 6725

Complainants are usually required to submit written, identified complaints. If not resolved immediately, Boab Health will respond in writing within 30 days. If unsatisfied, individuals may contact the OAIC at 1300 363 992 or <https://www.oaic.gov.au/privacy/privacy-complaints/>

15. Documentation

Boab Health Services

- Complaints Management Policy and Procedure
- OAIC guidance material
- Google Analytics Privacy Policy (external site)
- Google opt-out tools (external site)

Summary of Changes (v4)

Update Area	Description of Change
Definitions	Added biometric, location, and inferred data definitions.

Governance Introduced Privacy Officer role and annual review/reporting requirement.

Consent Replaced implied consent with explicit (informed) consent.

Children & Vulnerable Persons New section outlining extra safeguards.

Retention & Disposal Retention schedules aligned with WA requirements; commitment to secure destruction.

Privacy by Design New section committing to Privacy Impact Assessments for new projects.

Use of AI Added section on AI, including safeguards, human review rights, and de-identification of AI-generated inferences.