CLEAR HANDLING OF PERSONAL, SENSITIVE AND HEALTH INFORMATION

Privacy Policy

How PHOENIX SANCTUM collects, holds, uses, discloses, protects and disposes of information across enquiries, bookings, intake, services, products, reports and digital systems.

Status
ACTIVE

Version
24 August 2026

Policy owner
Steven / PHOENIX SANCTUM

Public audience
Clients, prospective clients and contacts

Supersedes
Privacy Policy v2026-07-22

Next review
16 January 2027, or earlier if practices or law change

Plain-language commitment
We collect only information reasonably needed for our work, apply extra care to sensitive and health information, keep material decisions under human review, and provide practical ways to ask questions, access records, request corrections or complain.

This policy describes PHOENIX SANCTUM's practices and applicable privacy framework. It is not a claim of regulator approval or legal certification.

1. About us and this policy

PHOENIX SANCTUM

ABN 94 991 399 634
4A Painters Parade, Dee Why NSW 2099
info@phoenixsanctum.com
phoenixsanctum.com

Who is covered

Website visitors, enquirers, subscribers, prospective, current and former clients, authorised representatives, carers and emergency contacts, referrers, suppliers, contractors and other business contacts.

PHOENIX SANCTUM provides complementary wellbeing services and holds health-related information. Australian privacy law therefore applies to our handling of that information. In NSW, private health-service-provider requirements may also apply.

Information we may collect

Category	Examples
Identity and contact	Name, date of birth, phone, email, country and state or region, emergency contact, authorised representative and communication preferences. A full street address is collected later only where operationally required.
Sensitive and health-related	Intake responses; self-reported symptoms, experiences and wellbeing concerns; heritage, ethnicity, origin, country of birth, childhood environment and places lived where relevant to health context and appropriate support; lifestyle or environmental history; voluntarily disclosed medications, supplements and sensitivities; safety or contraindication information.
Services and sessions	Bookings, attendance, consultation or session notes, preferences, programme history, reports, summaries, practitioner observations, communications and consent records.
Technical and remote services	Device outputs, scan or reverse-lookup results, resonance observations, programme or frequency selections, remote-service cycles, and links between a client record and an accepted dry sample or client-supplied medium.
Payment and business	Invoices, payment status, transaction identifiers and limited processor-supplied payment metadata. Card details are handled by the payment provider rather than intentionally stored by us.
Digital and marketing	IP address, device/browser data, pages viewed, cookies, form submissions, website security logs, subscription status, campaign interactions, and information sent through social platforms.

How we collect it

Directly from you through our website, the Tally new-client enquiry form, Square bookings or payments, email, calls, messages, consultations, products and services; from PHOENIX SANCTUM systems and service records; from an authorised representative or referrer; and from a provider or public source where lawful and reasonably necessary for verification, safety, fraud prevention or administration. Where practicable, we collect from you.

> **Recordings and biological samples need specific controls**
> Audio, video, photographs, transcripts, testimonials or case material require a separate permission where appropriate. The Sample Digitiser accepts only the approved dry or sealed non-fluid scope; receipt, use, return or disposal is recorded against a client code.

2. Why we handle information

We collect, hold, use and disclose information where reasonably necessary to:

- respond to enquiries and explain services;
- understand a person's health, cultural, developmental and environmental context;
- assess suitability, consent, safety and the type of support that may be appropriate;
- manage bookings, accounts and attendance;
- deliver products and requested in-person, online or remote services;
- maintain continuity and service history;
- communicate about appointments and support;
- take payment, invoice and keep tax records;
- manage samples and remote workflows;
- handle incidents, complaints and disputes;
- protect clients, systems and legal rights;
- improve operations and send permitted marketing.

Consent and sensitive information

Before the Tally intake collects health or other sensitive information, it presents an APP 5 collection notice and requires an explicit consent confirming that you have read the notice and agree to PHOENIX SANCTUM collecting and handling the information for the stated enquiry, contextual assessment, suitability, safety, service-planning and support purposes. This includes the heritage, ethnicity, origin, country-of-birth, childhood-environment and places-lived information you choose to provide. The form does not seek generic consent for research or artificial-intelligence use.

We seek a separate permission when the context requires it, including for recordings, identifiable testimonials, photographs, case material, disclosure to another practitioner or a materially different use.

You may withdraw consent for a future activity where consent is the basis for that activity. Withdrawal does not undo earlier lawful handling or require destruction of information that must be kept.

If information is not provided

You may choose not to provide information, but we may be unable to assess suitability, provide a service safely, complete a booking, identify the correct remote-service record, maintain continuity or meet a legal obligation.

When we disclose information

Disclosure is limited to the purpose for which the information was collected, a permitted related purpose, your consent, or another lawful basis. Recipients may include:

- the technology providers identified in section 3;
- an authorised representative, support person or another practitioner you nominate;
- accountants, insurers, lawyers, IT/security support and other advisers who need the information for their role;
- regulators, courts, tribunals, law-enforcement or government bodies when required or authorised by law;
- a successor in a genuine business transfer, subject to appropriate confidentiality and privacy controls.

We may act where necessary to lessen or prevent a serious threat to life, health or safety or to establish, exercise or defend a legal claim. We do not sell personal information to data brokers or third-party advertisers.

Direct marketing

We may send news, educational or promotional material where permitted. Sensitive or health information is not used for direct marketing unless legally permitted and any required consent is recorded. You can unsubscribe in the message or email us. Appointment, account, safety and service messages are not marketing.

3. Technology providers

We use a controlled set of providers. The current internal systems register records the exact use, information category, access owner, country information and review status.

Current system	Current purpose and information boundary
Tally	New-client enquiry and intake collection. Tally acts as PHOENIX SANCTUM's form processor; form data is stored in Europe and submissions are processed through Google Cloud infrastructure in Belgium. Tally's self-email notification sends the submitted non-empty answers to info@phoenixsanctum.com through SendGrid in the United States so authorised personnel do not miss a new enquiry. Respondent emails, PDF attachments, integrations, analytics, webhooks, uploads, payments, Tally AI and paid features remain disabled for this form.
Google Workspace Gmail, Drive, Calendar	Email, files, calendar and administration. The restricted PHOENIX SANCTUM mailbox receives Tally's new-enquiry notification and submitted non-empty answers for timely review. Sensitive content is access-restricted; public links, automatic forwarding and unnecessary copies are prohibited. The former Google Forms intake is retained only as controlled rollback evidence and is not the public intake destination.
Vercel	Public website hosting, content delivery, domain/DNS and platform security/log functions. The static public website is not the detailed health-intake system; it links new-client enquiries to Tally.
Square	Booking, customer, transaction, invoice, receipt and payment execution. PHOENIX SANCTUM does not use Square as the clinical/session-note system.
Control Centre and Supabase	Protected operational records, including client, appointment, service, session and audit information. Supabase is the database provider; access is restricted to authorised operations.
Approved AI or document tools	Limited drafting, summarisation, analysis or administration under the controls below. A tool is not approved merely because it is available.

Overseas handling

Cloud and payment providers may process, store or make information accessible outside Australia. Tally stores form data in Europe and uses Google Cloud infrastructure in Belgium to process submissions. When the self-email notification is enabled, Tally uses SendGrid in the United States to deliver the submitted non-empty answers to PHOENIX SANCTUM's restricted Google Workspace mailbox. Other relevant provider locations may include Australia, the United States, Canada, Japan, Singapore, Ireland, France, Spain, the United Kingdom and other countries where a provider or its subprocessors operate. The exact location can depend on account settings, service routing and provider infrastructure.

Before a new or changed overseas arrangement is approved, we assess the information involved, necessity, contractual and security controls, access, deletion, subprocessors and whether the arrangement is a use or disclosure for APP 8 purposes. We minimise the information shared and keep the provider review in our internal register.

AI, automation and human review

- Identifiable or sensitive client information must not be entered into a publicly available or unapproved general-purpose AI tool.
- An AI-assisted use involving personal information requires an approved purpose, provider review, lawful basis, data minimisation, access control and human checking.
- AI output may be wrong. A practitioner or authorised person verifies material facts, client attribution, safety content and external communications before use.
- We do not intentionally use client information to train a public AI model.

> **Current decision position**
> Software may organise, compare or surface information for review. As at this version, PHOENIX SANCTUM does not arrange for a program to independently approve or refuse access to services, diagnose a condition, determine treatment, or make another material safety decision about a client. A person remains responsible for material decisions. We will reassess each relevant workflow before the automated-decision privacy-policy obligations commence on 10 December 2026 and update this policy if required.

4. How we protect and retain information

Security

We take reasonable steps appropriate to the sensitivity, volume, location and likely harm to protect information from misuse, interference, loss, unauthorised access, modification and disclosure. Controls may include:

- multi-factor authentication;
- unique accounts and strong credential controls;
- least-privilege access;
- restricted sharing and no public client-data links;
- device locking, updates and supported encryption;
- provider and permission review;
- secure transmission where supported;
- backups and restoration checks;
- confidentiality requirements;
- retention, disposal and incident procedures.

No internet or storage system can be guaranteed completely secure. Our controls reduce risk and support a prompt response; they do not remove every possible risk.

Retention and disposal

We keep information for the longest applicable legal, safety, insurance, dispute or operational period, then securely destroy or de-identify it where permitted.

Record	Current rule
Adult NSW health information	At least 7 years from the last occasion on which a health service was provided.
Information collected while under 18	At least until the person turns 25. A longer applicable period controls if services continue or another obligation applies.
Tax and core transaction records	Generally at least 5 years from the relevant preparation, obtaining or completed transaction, subject to longer special rules.
Unconverted Tally enquiries	Reviewed manually and ordinarily deleted from Tally within 24 months unless a lawful, safety, complaint, insurance or dispute reason requires longer retention. Tally's deleted-submission trash is also reviewed and emptied manually when appropriate. The duplicate notification email is kept only as long as needed to identify, triage and safely transfer or manage the enquiry, then deleted subject to the same lawful holds and record-integrity checks.
Converted client enquiries	The information needed for the client record is transferred to the approved record system and kept for the applicable health-record period. Duplicate or temporary Tally copies are removed after transfer and record-integrity checks.
Recordings and temporary working material	Only while needed for the agreed purpose, verification or a longer legal, safety, complaint, insurance or record-integrity reason.
Other information	According to the active Data Retention and Secure Disposal Schedule and any legal hold.

For destroyed NSW health information, we keep the required disposal record identifying the person, the period covered and the disposal date. For a transfer to another health provider, we record the client, transfer date and recipient provider details.

Data breaches

We use a documented response plan to contain, assess, notify and review actual or suspected breaches. If there are reasonable grounds to suspect an eligible data breach, we conduct a reasonable and expeditious assessment and take all reasonable steps to complete it within 30 calendar days. If an eligible breach is established, we promptly notify affected individuals and the OAIC as required.

> **Report a concern immediately**
> If you receive information intended for someone else, see an unexpected client record, lose a PHOENIX SANCTUM device or document, or suspect unauthorised access, stop using or sharing the information and contact info@phoenixsanctum.com.

5. Access, correction and complaints

Access and correction

You may ask for access to personal information we hold about you or ask us to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. Email info@phoenixsanctum.com. We verify identity and authority before releasing or changing information.

We aim to respond within 30 days. A valid legal exception may limit access or the exact correction requested. If so, we will explain the decision where required and tell you about available complaint options. We do not charge merely for making a request, although a lawful and reasonable access charge may apply in limited circumstances after notice.

Deletion requests

You may ask us to delete information. Deletion is not absolute. We may need to keep information for health-record retention, tax, fraud prevention, legal, insurance, dispute, safety or record-integrity reasons. Where deletion is not available, we consider access restriction, correction or de-identification where appropriate.

Anonymity and pseudonyms

You may use anonymity or a pseudonym for a general enquiry where lawful and practicable. It is usually not practicable for a booking, payment, service, report, sample assignment, safety assessment, records request or ongoing client record.

Children and authorised representatives

For a minor or a person who cannot manage their own affairs, we assess capacity, authority and the person's interests. We may deal with a parent, guardian or other authorised representative where lawful and reasonably necessary, while involving the person directly where appropriate.

Cookies and third-party links

Our website may use necessary, security, analytics and campaign cookies. Browser settings can limit cookies, although site functions may be affected. Links to another website or app are governed by that provider's privacy practices.

Privacy complaints

1. Email info@phoenixsanctum.com with the issue, relevant dates and the outcome you seek.
2. We record the complaint, protect it from unnecessary access, investigate fairly and aim to respond within 30 days.
3. If you are not satisfied, you may contact the Office of the Australian Information Commissioner and, for NSW health information, the Information and Privacy Commission NSW.

> **Questions are welcome**
> You do not need legal language to raise a concern. Tell us what happened, which information is involved and what you would like us to do.

6. Policy authority and changes

This version preserves the substantive coverage of the 22 July 2026 policy and records the approved Tally intake, explicit sensitive-information purpose and consent, APP 5 collection notice, the operational self-email notification through SendGrid, overseas processing and manual retention/deletion controls. It is supported by separate internal plans, schedules and registers.

Primary authority sources

- Privacy Act 1988 (Cth), current compilation as at 4 June 2026: legislation.gov.au/Latest/C2021C00024.
- OAIC, Australian Privacy Principles Guidelines, updated 13 May 2026: oaic.gov.au/privacy/australian-privacy-principles/....
- OAIC, health service provider coverage: oaic.gov.au/.../what-is-a-health-service-provider.
- Information and Privacy Commission NSW, retention and storage of health information, October 2025: ipc.nsw.gov.au/resources/....
- OAIC, Notifiable Data Breach Scheme, updated February 2025: oaic.gov.au/privacy/notifiable-data-breaches/....
- OAIC, commercial AI products guidance, updated 17 January 2025: oaic.gov.au/privacy/.../commercially-available-ai-products.
- OAIC, APP 1 automated-decision transparency obligations commencing 10 December 2026: oaic.gov.au/privacy/.../chapter-1-app-1.
- ATO, Taxation Ruling TR 96/7, general business record keeping: ato.gov.au/law/view/document?LocID=TR967.

Provider sources checked

- Tally GDPR, Data Processing Addendum, subprocessors and submissions-retention documentation, checked 24 August 2026.
- Square Australian seller and buyer privacy notices, including overseas processing information.
- Supabase official platform-region documentation.
- Google Workspace official data-region documentation.
- Vercel Privacy Notice, Data Processing Addendum and Security & Compliance documentation.
- Live PHOENIX SANCTUM website and Control Centre operating documentation.

Research cut-off: 24 August 2026. Provider services, subprocessors and account settings can change. The internal systems register is reviewed when a provider or workflow changes and at least every six months.

Changes to this policy

We may update this policy for changes in law, provider terms, systems or business practices. The current version is published with its date. A material change that affects an existing collection or use is assessed separately; merely updating this policy does not create consent for a new use.

Owner approval
Steven / PHOENIX SANCTUM
Date: 24 August 2026

Activation record
Canonical Drive version activated
Date: 24 August 2026