H&H Care SA Pty Ltd	**Form03.** Consent Privacy and Information Sharing **Australian Government Support at Home Program**	
Doc No: Form03	**Version No: 01**	**Version Date: 24/10/2026**

Policy and procedure 3
H&H Care SA Pty Ltd | Support at Home services

This policy sets out how H&H Care SA obtains and records consent, protects personal and health information, and shares information lawfully for care, oversight and other authorised purposes. It gives workers practical instructions for daily visits, records, requests and privacy incidents.

Document control	Details
Policy number	HH SAH PRIV 003
Version and status	1.0 — Draft for Director approval
Prepared	24 October 2026
Policy owner	Director and designated Privacy Officer
Approved by	Huy Le, Director — signature: _____
Effective date	24 October 2026
Next review	12 months after approval, or earlier following relevant change
Applies to	Directors, managers, nurses, workers, administration and approved contractors handling client information

1 Purpose and scope

H&H Care will handle information fairly, securely and transparently, using only what is reasonably necessary for its lawful functions. This policy applies to paper and electronic records, verbal discussions, photographs, messages and information held by service systems and approved suppliers. It covers Support at Home services delivered on behalf of The Fig Trees and other separately approved registered provider arrangements.

As a business providing health services and holding health information, H&H Care must not assume the small-business exemption removes its Privacy Act obligations. The Director confirms applicable privacy, aged care, professional and contractual requirements. The registered provider's oversight does not remove H&H Care's own privacy duties.

2 Core requirements

- Distinguish consent to care from consent to collect, use or disclose information. A service agreement does not authorise every task or disclosure.
- Explain what is collected, why, who may receive it and how clients can ask questions, seek access or complain.
- Use consent or another valid legal basis; do not claim that consent is always required or that a contract alone authorises disclosure.
- Restrict access to authorised people, verify recipients, and report suspected privacy breaches immediately.

This is an internal operating policy. Before implementation, publish a separate, accessible APP privacy notice/policy with H&H Care's verified contact details and actual information handling and overseas disclosure practices.

Responsibilities and informed consent

3 Responsibilities

The Director appoints a Privacy Officer and backup in writing, provides resources and approves systems and suppliers. Until a separate appointment is made, the Director performs the Privacy Officer function. Record current names and business contact details in the controlled contact list and client privacy information.

The Privacy Officer manages information requests, disclosures requiring review, privacy complaints, breach assessments, retention controls and staff training. The Coordinator checks intake notices, consent and supporter authority and communicates relevant restrictions. The Clinical Lead RN advises on clinical consent and urgent health information. Every worker checks consent, uses secure records and immediately reports errors or concerns.

4 Obtaining informed consent

Before seeking consent, identify the specific care or information activity and explain its purpose, relevant options, benefits, material risks, proposed recipients and consequences of declining. Use plain language, an interpreter or communication aids as needed. Allow time and check understanding without pressure.

Consent must be voluntary, informed, current and sufficiently specific, given by a person able to make that decision or a person with applicable lawful authority. It may be express or, where legally appropriate and supported by the circumstances, implied. Use express documented consent for optional disclosures, clinical photographs, recordings, publicity and sensitive situations. Silence, attendance or a signature on an unrelated form is not blanket consent.

Record what was explained, the activity and information covered, permitted recipients, limits, duration or review trigger, method of consent, date and person obtaining it. Verbal consent may be recorded in the client record; obtain written consent where required by law, professional standards or the particular activity. Do not delay urgent lawful care solely to obtain a form.

5 Supporters and legal authority

Support the client to decide before relying on another person. A family member, next of kin or emergency contact does not automatically have authority to consent to care or all information disclosures. Registered supporter status assists decision-making but does not itself confer substitute decision-making power.

Verify the identity and relevant legal authority of any appointed decision-maker, including scope, activation and limits. Check registered supporter arrangements and the information access rights applicable to the request rather than treating them as unrestricted. Continue to involve the client and follow their will and preferences as required. Refer uncertainty to the Privacy Officer and Clinical Lead RN, with legal advice where needed.

6 Refusal withdrawal and review

Clients may limit or withdraw consent prospectively. Record the change promptly, update alerts and notify authorised recipients where necessary. Explain any effect on safe service delivery and offer alternatives. Withdrawal does not undo prior lawful handling or require destruction of records that must be retained. Consent is reviewed when tasks, recipients, purposes, authority or client preferences change; check consent for care at each visit under Policy 2.

Collection transparency and information sharing

7 Collection and privacy notification

Collect only reasonably necessary information using lawful, fair methods. Usually collect directly from the client, with consent for health and other sensitive information unless a valid exception applies. When obtaining referral information from The Fig Trees, hospitals, family or clinicians, check the purpose and lawful basis and verify important facts with the client where practicable.

At or before collection, or as soon as practicable afterwards, explain H&H Care's identity and contacts; what is collected and why; any legal collection requirement; consequences of non-collection; usual recipients; access and correction processes; complaint options; and likely overseas disclosures, including countries where practicable. Record when accessible privacy information was provided. An acknowledgement shows receipt, not blanket consent.

If unsolicited or excessive information arrives, refer it to the Privacy Officer to assess whether H&H Care could lawfully have collected it and whether it should be retained, securely destroyed or de-identified, subject to legal requirements. Do not copy irrelevant information into the client file.

8 Disclosure decision procedure

- Confirm the requester's identity, role, purpose and authority using trusted contact details. Do not rely solely on an incoming email, claimed family relationship or caller ID.
- Identify the specific information needed and check consent, restrictions and any other applicable legal basis. Disclose only what is relevant and necessary.
- For the primary care purpose, use or disclose information within that lawful purpose. For a secondary purpose, check consent or an applicable exception, such as a directly related purpose reasonably expected by the client, or a legal requirement. Escalate uncertainty.
- Check recipient details and attachments; remove unrelated client information and hidden content. Use the approved secure channel.
- Record non-routine disclosures, authority or legal basis, recipient, information, date and decision-maker. Routine sharing must remain traceable through approved systems.

9 Working with The Fig Trees

Share relevant care plans, visit evidence, clinical changes, incidents and other records needed for authorised delivery and oversight, using an established lawful basis. Explain routine sharing to clients. Agree access roles, secure channels, authorised contacts, breach coordination, audit arrangements and record transfer in writing. The contract does not override privacy law or authorise unrestricted access to unrelated H&H Care clients, staff or business records.

Supply invoices with the client details required by the contract through approved channels. Keep clinical detail out of invoices unless necessary and authorised. For audits, verify scope and authority, use secure access and limit unrelated information. Refer disputed or unusually broad requests to the Privacy Officer without obstructing lawful oversight.

Special disclosures and secure daily practice

10 Family clinicians emergencies and legal requests

Ask clients which family members or carers may receive updates and what may be shared. Consent to contact a person in an emergency does not authorise routine disclosure of the full record. Where a person cannot give or communicate consent, any disclosure to a responsible person must satisfy the relevant legal conditions; refer to the Privacy Officer or RN and consider known client wishes.

Share relevant information with treating clinicians on a lawful care basis and verify the receiving service. In an emergency, provide information needed by emergency responders. Where relying on a serious-threat exception, record the applicable basis, why obtaining consent was unreasonable or impracticable where required, and why the disclosure was necessary. Emergency circumstances do not authorise unlimited later disclosure.

Refer police, court, insurer, solicitor, regulator and government requests to the Privacy Officer for verification of legal authority and scope. Cooperate with mandatory reporting and lawful notices. Do not assume every police request is compulsory or seek consent where law requires disclosure regardless. Record reasons and seek advice where needed. Do not alert a person if doing so would be unlawful or compromise safety.

11 Photographs recordings publicity and technology

Clinical photographs require a defined care purpose, appropriate consent or other lawful basis, an approved device and secure transfer to the clinical record. Record who may access them. Marketing photographs, testimonials and recordings require separate, specific opt-in consent explaining use, audience, duration and withdrawal limitations. Declining publicity must not affect care.

Do not place identifiable client information in personal email, messaging groups, social media, unapproved AI tools or public transcription services. The Director must approve any digital recording, AI or transcription workflow only after privacy, security, consent, supplier and retention requirements are assessed. A client's consent alone does not make an insecure tool acceptable.

12 Daily security controls

- Use individual logins, strong passwords, multi-factor authentication where available, least-privilege access and screen locks. Never share credentials or browse files without a work purpose.
- Use approved business systems and devices. Personal devices require explicit approval, secure configuration, access controls and a managed removal process; do not retain local client copies.
- Verify email addresses and attachments before sending. Prefer secure portals or controlled links for sensitive records; send any access code separately. Use BCC for unrelated recipients where appropriate.
- Keep paper records locked and transport only necessary records securely. Do not leave files in vehicles or visible at home. Discuss care privately and confirm who is present before a phone or video discussion.
- Immediately report lost devices, misdirected messages, suspicious logins and unauthorised viewing. Remove access promptly when roles change or engagement ends.

Access correction retention and suppliers

13 Requests for access or correction

Clients may request access to personal information held about them and correction of inaccurate, out-of-date, incomplete, irrelevant or misleading information. Accept requests in accessible ways, including verbally, and refer them promptly to the Privacy Officer. Verify identity proportionately and verify authority for requests made by another person.

Log the request, scope, date, identity checks and response. As an internal service target, acknowledge within five business days and aim to respond within 30 calendar days; the applicable legal standard for a private organisation is a reasonable period. Explain any justified delay and keep the client informed. Do not charge for making a request or correction; any lawful access charge must be reasonable, explained beforehand and not excessive.

Provide access in the requested manner where reasonable and practicable. Protect other people's information and assess any lawful refusal ground rather than applying a blanket restriction. If refusing access or correction, give required written reasons, complaint options and alternatives where appropriate. If a requested correction is refused, explain how the client may request an associated statement. Correct by dated amendment or addendum, preserving the audit trail; do not silently overwrite clinical history.

Coordinate with The Fig Trees where relevant, but do not assume only the registered provider may respond to information H&H Care holds. Decide each entity's obligations and communicate clearly to the client. Correct information previously shared where required or appropriate and lawful.

14 Retention and secure disposal

Maintain an approved retention schedule based on applicable law, clinical and professional requirements, insurance needs and the contract. The Fig Trees agreement requires records during the term and for seven years afterwards unless otherwise notified, and also contains return or destruction provisions. The Privacy Officer must resolve conflicting instructions before disposal; no contract instruction overrides a legal retention duty.

Do not retain information indefinitely without a valid reason. When information is no longer needed and retention is not required, securely destroy or de-identify it under the applicable privacy requirements. Suspend disposal for complaints, investigations, claims or legal holds. Record approval, records affected, method, date and disposal confirmation. Address backups and supplier-held copies through controlled lifecycle arrangements.

15 Cloud services and overseas handling

Before using ShiftCare, cloud storage, email or another supplier for client information, the Director verifies access controls, storage locations, support access, subcontractors, breach response, backups, recovery, export and deletion arrangements. Do not assert that data stays in Australia without evidence.

Assess whether an overseas disclosure occurs and apply APP 8 and other relevant requirements where applicable. Seek specialist advice where needed, document safeguards and reflect actual likely disclosures in client privacy information. Do not assume a client's ordinary service consent waives overseas disclosure obligations. Review suppliers at least annually and when terms, locations or risks change as an H&H Care internal control.

Privacy breach response and complaints

16 Immediate breach response

Any suspected loss, misuse, unauthorised access or disclosure must be reported to the manager and Privacy Officer immediately, even if the information appears to have been recovered. This includes wrong-recipient emails, misplaced paper records, stolen phones, ransomware and improper staff access.

- Contain: stop further disclosure, revoke links or access and secure affected devices with competent technical help. Ask unintended recipients to secure or delete information where appropriate. Preserve evidence; do not wipe logs or investigate beyond authority.
- Assess: record the awareness time, information and people affected, likely access, possible harm and containment steps. Obtain technical, legal and clinical advice. Determine whether the event is a suspected eligible data breach under the NDB scheme.
- Coordinate: promptly alert The Fig Trees when its client information or services are affected under the agreed pathway. Agree a lead and communication plan, while confirming H&H Care's own legal duties rather than assuming another entity's report discharges them.
- Notify: if an eligible data breach is established, prepare the required statement and notify the OAIC and affected or at-risk individuals as applicable, as soon as practicable. Explain the event, information types, contact point and protective steps without exposing others.
- Review: document decisions, advice, notices, remediation and effectiveness checks. Update access, training and systems and report significant issues to the Director.

17 NDB assessment and notification controls

An eligible data breach generally involves unauthorised access or disclosure, or relevant loss of information, likely to cause serious harm, where effective remedial action has not prevented that likelihood. The Privacy Officer assesses the statutory test, including sensitivity, recipients, security and potential physical, financial, psychological or other serious harm.

Where there are reasonable grounds to suspect an eligible breach, undertake a reasonable and expeditious assessment and take all reasonable steps to complete it within 30 calendar days of becoming aware of those grounds. This is an assessment period, not permission to wait 30 days before acting. Where reasonable grounds to believe an eligible breach already exist, proceed to notification as soon as practicable. Record and obtain advice on any exception or delay; do not treat every minor breach as automatically notifiable or every recovered email as harmless.

18 Privacy complaints

Accept complaints verbally or in writing and provide interpreter, supporter or advocacy assistance. Use the verified business privacy contact; clients may also raise concerns with The Fig Trees, the OAIC or the aged care complaints regulator as relevant. Do not require them to obtain permission to complain.

As internal targets, acknowledge within five business days and aim to provide a reasoned response within 30 calendar days, or explain the delay. Investigate fairly, protect against retaliation, communicate the outcome and available escalation options, and record improvement actions. Mandatory breach notifications must not wait for complaint resolution.

Supporting records implementation and references

19 Supporting forms and registers

Record	Minimum content
Consent and preferences	Specific care or disclosure; purpose, recipients and limits; explanation and support; decision, method, date and review trigger.
Authority verification	Identity; supporter status or appointment; relevant powers, activation and limits; verification and review date.
Disclosure and request log	Requester; verified authority and legal basis; information; recipient; channel; dates, decisions and outcome.
Privacy breach register	Discovery and awareness times; affected information; containment; assessment; notification decision and reasons; follow-up.
System and retention register	Approved systems, supplier and location checks; access owners; retention basis; legal holds; disposal approvals.
Separate media consent	Image or recording purpose; approved audience and channels; optional consent; duration and withdrawal explanation.

20 Implementation and review

Before approval, appoint the Privacy Officer and backup; publish verified contact details; complete an accurate public privacy policy and collection notice; confirm supplier and overseas handling; agree The Fig Trees' sharing and breach contacts; and train staff. Keep consent forms distinct from privacy notices. Do not leave client-facing contacts blank when the policy takes effect.

As internal controls, review privacy incidents and requests monthly, audit a risk-based sample of access and disclosure practices quarterly, and review the policy and supplier controls annually. Reassess after incidents, legislative or system changes. Record corrective actions, owners, due dates and verified outcomes.

21 References

Use current versions. Official OAIC guidance checked on 24 October 2026. This policy supports privacy practice and does not replace advice about a particular disclosure, consent dispute or breach.

- Privacy Act 1988, Australian Privacy Principles and Part IIIC Notifiable Data Breaches scheme.
- OAIC — Guide to health privacy. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/guide-to-health-privacy
- OAIC — Guide to securing personal information. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information
- OAIC — Notifiable Data Breaches scheme. https://www.oaic.gov.au/privacy/notifiable-data-breaches
- Aged Care Act 2024 and Aged Care Rules 2025; relevant South Australian consent, advance care directive and guardianship laws; applicable nursing and professional standards.
- H&H Care Policies 1 and 2; records, safeguarding, complaints and incident procedures; The Fig Trees brokerage agreement dated 10 March 2026 and current approved variations.

Approval signature: _____ Effective date: _____

Version 1.0 — Initial draft prepared 24 October 2026. Approval and implementation remain to be completed.