

Privacy and Confidentiality Policy

Navigate Health

Navigate Health is dedicated to protecting our client's privacy and maintaining strict confidentiality of all personal, sensitive, and health information. This Privacy and Confidentiality Policy outlines how we collect, use, store, and protect client information, as well as the expectations and responsibilities we uphold regarding confidentiality in the delivery of our allied health, injury management, and rehabilitation services throughout Australia.

Scope of Services

Our services include client-centered rehabilitation for individuals with injury, illness, or disability to help them achieve health, social, and vocational goals; allied health assessments and treatments (such as psychology, counselling, and social work); workplace rehabilitation; injury prevention; and work health and safety assessments, training, and consulting (collectively, "Services").

Compliance with Privacy Laws

Navigate Health provides its Services in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and other applicable Australian health privacy laws.

In addition to our obligations under federal privacy law, Navigate Health is also committed to meeting the requirements of New South Wales state legislation where we primarily operate, including the Health Records and Information Privacy Act 2002 (HRIP Act) and the Privacy and Personal Information Protection Act 1998 (PPIP Act). We ensure that all personal and health information is managed in accordance with these Acts, which set out specific standards for the collection, use, storage, and disclosure of personal and health information within NSW. Our practices are designed to uphold client's rights under both Commonwealth and state legislation, providing them with additional assurances regarding the protection of their information.

Purpose of this Policy

This Privacy and Confidentiality Policy explains how Navigate Health collects, stores, uses, discloses, and protects personal, sensitive, and health information. It applies to all personal information gathered during the provision of our Services and via our website.

This Policy includes information about:

- Types of personal information collected
- How personal information is collected
- How we use personal information
- How we share or disclose personal information

- Our confidentiality obligations and how we protect confidential information
- How personal information is held and protected
- Use of cookies and website tracking
- How clients can access and correct your information
- How to provide feedback or make a privacy or confidentiality complaint

Confidentiality at Navigate Health

Navigate Health is committed to maintaining strict confidentiality in all aspects of service delivery. Confidentiality means that:

- Any information shared with us is treated with the highest level of discretion
- Only authorised personnel involved in your care can access your information
- Information is used solely for the purpose for which it was collected unless legally permitted or required

We uphold confidentiality through:

Staff Obligations

All staff, contractors, and students must:

- Complete mandatory privacy and confidentiality training
- Limit access to client information to what is essential for their role
- Maintain confidentiality during and after their involvement with Navigate Health
- Avoid discussing client information in public or non-secure settings

Breach of confidentiality is taken extremely seriously and may result in disciplinary action, termination of engagement, or legal consequences.

Data Breach Reporting and Response

Navigate Health manages data breaches under the organisation's **Data Breach Procedure**, which sets out the required steps for identifying, reporting, containing, assessing, and notifying relevant parties of any actual or suspected breach of personal or health information.

Staff must immediately report any potential breach to the Delegated Director (Privacy Officer) in accordance with that procedure. The Data Breach Procedure supports this policy by ensuring compliance with the Privacy Act 1988 (Cth), the Notifiable Data Breaches Scheme, NSW privacy legislation and the Workplace Rehabilitation Provider Approval Framework.

Situations Where Confidentiality May Be Broken

Confidentiality may only be lawfully breached when:

- Required by law (e.g., subpoena, court order)
- There is a serious or imminent threat to someone's life, health, or safety

- Mandatory reporting laws apply
- Disclosure is required to prevent significant harm

Where possible, we will attempt to discuss any required disclosure with our clients before it occurs.

Confidentiality in Digital Communication

Navigate Health ensures confidentiality in all digital communications by:

- Using secure case management software (Vinci)
- Encrypting data in transit and at rest
- Verifying identity before sharing information
- Restricting access to authorised personnel only

We do not transmit sensitive information via unsecured channels unless unavoidable, and only with explicit risk consideration.

What is Personal Information?

“Personal information” is information or an opinion that can reasonably identify our client, whether or not the information is accurate or recorded. This includes your name, age, gender, contact details, and sensitive information.

“Sensitive information” includes:

- Health information (e.g., medical history, diagnosis, treatment details)
- Genetic and biometric information
- Information about racial or ethnic origin, sexual orientation, membership of professional or trade associations/unions, and religious beliefs

Types of Information Collected

Navigate Health collects only the information necessary to deliver our Services. This may include:

- Name, address, phone number, and date of birth
- Employment status and salary
- Diagnosis and treatment history
- Contact details of treatment providers
- Injury, illness, and/or disability history
- Government-related identifiers (e.g., insurer claim numbers, NDIS Plan number)
- Employment history and educational qualifications
- Claim and referral information
- Correspondence (letters, emails, faxes, phone records)
- Photos (such as workplace assessment images)

- Medical records, certificates, reports, and assessments
- Job applicant referee details

How We Collect Personal Information

We may collect personal and sensitive information through various means, including:

- Face-to-face and phone interactions, or virtual meetings
- Completion of forms on our website or online portals
- Enquiries submitted through our website
- Emails or other direct communications

We may also collect information from other authorised sources if you have provided consent or if collection is required or permitted by law. This can include your employer, care agencies, insurers, or treating professionals.

We also store contact details of clients, contractors, insurers, suppliers, and other business contacts as needed for our operations.

We do not collect personal information from our social media pages.

How We Use Personal Information

Personal and sensitive information is used only as necessary to provide our Services, including:

- Assessing your needs for rehabilitation or intervention services
- Contacting you regarding your enquiry or services used or of interest
- Fulfilling contractual and legal obligations
- Managing health, safety, and wellness risks
- Assessing the suitability of job applicants and consultants

Sharing and Disclosure of Personal Information

We only share personal and sensitive information with third parties as permitted by law, including:

- With client consent
- Where related to the purpose for which it was collected
- If sourced from a public record
- In health situations where disclosure is permitted under privacy law
- To prevent or lessen a serious threat to health or safety
- For legal proceedings or law enforcement
- As required by government authorities or regulators

Where disclosure is required for service delivery, we will seek client consent wherever possible. In exceptional circumstances (e.g., risk of harm), we may disclose information without consent as required by law.

Information may be shared with:

- Authorised health practitioners and representatives
- Industry partners such as employers and insurers
- Our related entities and professional advisors
- Government agencies and service partners (such as iCare, Comcare, and SIRA)

Personal and sensitive information is not routinely disclosed outside Australia. If necessary, we will ensure that the recipient upholds privacy standards comparable to those in Australian law.

How Personal Information is Held and Protected

Navigate Health maintains high standards of technology and operational security to protect information from misuse, loss, unauthorised access, modification, or disclosure.

Personal and sensitive information is stored in Vinci, our secure case management software, which features password access controls and robust data protection measures. All health-related data stored within Vinci is encrypted at rest and during transmission, and access is restricted based on staff roles and responsibilities. Only personnel with appropriate authorisation can access files relevant to their duties.

Paper records are securely destroyed once digitised and uploaded to Vinci. Our organisation uses locks, secure storage, password-protected devices, and other IT security safeguards to maintain confidentiality during client appointments.

We take reasonable steps to destroy or de-identify information that is no longer required, subject to any legal record-keeping obligations. For instance, health information may need to be retained for a minimum of seven years from the date of the last service, as required under Australian privacy law.

All Navigate Health staff and contractors are trained in privacy obligations and procedures. Information is not transferred to third parties without proper authorisation and identity verification.

Use of Cookies and Website Tracking

We may collect non-identifying information about client's use of our website, including the pages they visit, the device type, IP address, and the referring website. This helps us analyse and improve our website and services.

Our website uses cookies to enhance client experience and remember preferences. Cookies can be turned off in browser settings, but some website features may not function as intended.

Accessing and Correcting Your Information

We take reasonable steps to ensure information is accurate, complete, and up-to-date. Clients have the right to request access to or correction of personal and sensitive information.

Requests will be addressed within a reasonable timeframe. In some cases, we may decline access or correction as permitted by law (e.g., if the information is a professional opinion). If we refuse a request, we will provide written

reasons and instructions on how to lodge a complaint. If requested, we will add a statement to the client's record regarding the requested correction.

Notification Obligations to SIRA

Navigate Health will inform SIRA as soon as reasonably practicable, and within a maximum of 30 calendar days of any Breach of Privacy

Regulatory Reporting to SIRA

As part of reporting requirements under the Workplace Rehabilitation Provider Framework, Navigate Health will provide any privacy breach to SIRA as soon as possible and no later than thirty days after discovery of the breach. A summary report of all Privacy Breaches forms part of Annual reporting requirements to SIRA. This will include a copy of Privacy Breach register, actions taken and assessment/investigation outcomes.

Feedback and Complaints

Feedback or concerns about this Privacy Policy or our handling of information are managed by our designated Privacy Officer (Delegated Director):

Email: info@navhealth.com.au

Our Privacy Officer will review the complaint and aim to resolve it promptly. Complaints will be addressed within 10 working days. For more complex matters, we will keep clients informed of progress and expected timeframes.

If clients are not satisfied with our response, they may contact the Office of the Australian Information Commissioner (OAIC):

Phone: 1300 363 992

Website: oaic.gov.au

Changes to this Policy

Navigate Health may update this Privacy Policy from time to time. Any changes will be published on our website. Where changes are material, we will provide reasonable notice before their implementation.

Contact Us

Privacy Officer

Navigate Health

Email: info@navhealth.com.au