Approved by:	CEO
Approval date:	6 May 2025
Date for review:	6 May 2027
Review frequency:	Biennially
Version:	2.1.

Privacy Policy

Policy Number 3.14.

IT, KNOWLEDGE AND INFORMATION MANAGEMENT

1. Background

The Privacy Act 1988 (Privacy Act):

- Was introduced to promote and protect the privacy of individuals and to regulate how personal information is handled. It also regulates the privacy component of the consumer credit reporting system, tax file numbers, and health and medical research.
- **Defines personal information** as information or opinions "about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not".
- Outlines 13 Australian Privacy Principles (APPs) which govern how organisations should collect, handle and use personal information as well as organisational accountability. A breach of an APP is deemed an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.

Personal information can be publicly available and/or sensitive and/or confidential.

Wentworth Healthcare collect a broad range of personal and sensitive information from those we interact with.

2. Purpose

The purpose of this policy is to set out how Wentworth Healthcare manages personal information including: why Wentworth Healthcare needs to collect personal information, how it is collected, what we do with it, how it is stored, who we might share it with as well as individual rights to access and correct personal information.

3. Scope/Application

This policy applies to all staff and individuals who interact with Wentworth Healthcare.

It applies across all activities undertaken by Wentworth Healthcare.

Wentworth Healthcare Board, Staff, Service Providers and other stakeholders are expected (and supported) to understand and act in accordance with this Privacy Policy and any relevant supporting documents (including the Privacy Impact Assessment (PIA) Policy, related procedures, forms and guidelines).

4. Privacy Framework

Wentworth Healthcare has developed a four-step framework to support implementation of privacy across the organisation:

STEP 1: EMBEDDING A CULTURE OF PRIVACY THAT ENABLES COMPLIANCE

Wentworth Healthcare's leadership and governance supports a culture of privacy compliance, demonstrated in:

- Data security and privacy protection being a key data governance concept supporting Wentworth Healthcare's Data Governance Framework and approach to risk.
- Wentworth Healthcare's Risk Appetite Statement, where privacy risk is assessed as:
  - 'Controlled' for Regulatory compliance.
  - 'Cautious' for Governance.

*This means Wentworth Healthcare has a **zero to low** tolerance for privacy risk.*

STEP 2: ESTABLISH: ROBUST AND EFFECTIVE PRIVACY PRACTICES, PROCEDURES AND SYSTEMS

Wentworth Healthcare has effective practices, procedures and systems to support good privacy management.

STEP 3: CONTINUOUS IMPROVEMENT

Wentworth Healthcare regularly evaluates privacy practices, procedures and systems to ensure continued effectiveness.

STEP 4: ENHANCING WENTWORTH HEALTHCARE'S RESPONSE TO PRIVACY ISSUES

Wentworth Healthcare is committed to ensuring responsiveness to new privacy issues.

5. Policy Statement

Wentworth Healthcare Limited (WHL) is the provider of the Primary Health Network for the Nepean Blue Mountains region which includes the Blue Mountains, Hawkesbury, Lithgow and Penrith.

Wentworth Healthcare is committed to protecting personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs) and other applicable privacy laws and regulations, such as the Health Records and Information Privacy Act 2002 (NSW).

This Privacy Policy describes how Wentworth Healthcare will collect, hold, use and disclose personal information, and how we maintain the quality and security of personal information.

Wentworth Healthcare will update this Privacy Policy when there is a change to how we handle personal information (including when applicable laws change). An update will be effective as at the date that it is published on our website.

Data Collection

- ***Who we collect information from***

  Wentworth Healthcare collects personal information from individuals we interact with, including but not limited to:

  - consumers, carers and community members, including those with lived experience.
  - healthcare professionals and practice staff (including general practice and allied health)

- commissioned service providers, consultants, visitors and contractors
- employees, board members, committee members, non-government organisations (NGOs) or other health and non-health agencies

➢ ***What information do we collect***

The information we collect will vary depending on the interaction, but it may include personal information that could be used, to directly or indirectly, identify an individual. It may also include sensitive information.

Personal and/or sensitive information that we may collect includes but is not limited to:

- Name
- Date of birth
- Gender
- Racial origin
- Sexual orientation
- Contact details such as email, address and phone number
- Signature
- Criminal record
- Financial information
- Health information
- Photographs or video
- Internet protocol (IP) address information

➢ ***How we collect information***

Where possible, Wentworth Healthcare collects personal information directly from individuals through an informed consent process however we may also collect information from other sources, such as:

- Government and non-government agencies.
- Publicly available information sources.
- Healthcare organisations.

Personal information we collect may be obtained:

- Verbally, over the phone, in person or via digital meetings; or in writing, including via forms, emails, surveys or data submitted via our systems, social media or website.
- Through enquiries we perform, including online verification such as police checks for employees and other stakeholders where a police check is required;
- Anonymously, where it is lawful and practical to do so, such as where an individual requests information, submits feedback, complaints, or surveys.

  At times, it may be impractical to interact with individuals anonymously, or through use of a pseudonym, as limits our ability to:
  - make appropriate enquiries.
  - respond to feedback.
  - provide care and/or support, however we will provide this to the extent that we can.
- Without it being requested by Wentworth Healthcare (unsolicited information).

  If we receive unsolicited personal information about a third party from other individuals or entities, it will be handled in accordance with this Privacy Policy however the information will be destroyed as soon as practicable, and the sender notified.
- We may maintain records of our interaction with individuals and may take photographs or video of individuals at events we sponsor or run.

Individuals should be aware that there are risks in transmitting data across the internet and that, while reasonable efforts are made, Wentworth Healthcare cannot guarantee the security of information transmitted online.

How We Use Personal Information

Wentworth Healthcare will collect personal information only where it is necessary to do so and only uses personal information for its intended purpose, additional purposes for which consent was obtained or a related purpose that would reasonably be expected.

The main purposes for which we collect, use and hold information are:

- To communicate, and maintain contact with, consumers, healthcare professionals and practice staff.
- To provide support to consumers, healthcare professionals and practice staff, including:
  - Initial mental health assessments.
  - Referral information or support engaging with regional services.
  - Training and education services offered or facilitated by Wentworth Healthcare.
- Commissioning, contracting or co-design activities funded and/or delivered by Wentworth Healthcare.
- To consider applications made to us and respond to requests for information or feedback (including compliments or complaints) and to provide referrals.
- Where required to do so by law, regulation, rule or professional standard.
- For marketing or promotional purposes including notification of upcoming events or services.
- Recruitment and employment activities.
- Other purposes relating to the operation of the Primary Health Network (including invoicing, account management and evaluation activities) and the fulfilment of any contractual and/or legal obligations.

How We Store Information (Data Security and Storage)

Wentworth Healthcare may keep information in electronic and physical records.

We will take reasonable steps to protect the security and integrity of personal information to ensure that it is:

- Necessary, accurate and up to date.
- Kept confidential and stored securely with appropriate access controls.
- Protected from **misuse, interference and loss,** as well as **unauthorised access, modification or disclosure.**
- Destroyed or de-identified when it is no longer needed.

Wentworth Healthcare will hold information for the relevant statutory period, dependent on its initial purpose.

How To Access and Correct Personal Information

Individuals have a right to request access to their personal information at any time. Individuals also have the right to request incorrect or inaccurate information be amended.

Wentworth Healthcare require verification of an individual's identity prior to providing access to any personal information however we will not unreasonably withhold access to, or correction of, personal information.

To request access to your information, please contact us (details below).

Marketing Communications

Wentworth Healthcare may use personal information for marketing or promotional purposes including notification of upcoming events or services. Any direct marketing is consent based, and in accordance with the *Spam Act 2003*.

Individuals and organisations who receive marketing communications are provided with opportunity to unsubscribe in each marketing communication and may also contact Wentworth Healthcare at any time to notify a change in their communication preference.

Wentworth Healthcare does not sell personal information for marketing purposes.

Disclosure

Wentworth Healthcare may need to share information, including personal or sensitive information, with third parties including government departments and health organisations. Wentworth Healthcare does not routinely disclose information unless:

- An individual gives consent for us to do so.
- Required to do so by law, regulation, rule or professional standard (e.g. obligations in respect of child protection or compliance with a funding arrangement with the Department of Health and Aged Care).
- There is a public duty to do so.
- An individual is at risk.
- Necessary, in connection with a service we provide (e.g. where we provide a supported referral to another service or where verification, such as police check for new employees, is required or for use in community service directories).

Wentworth Healthcare may use third party providers to support some services we offer. This means parties external to Wentworth Healthcare may have access to some personal information collected and held by us. This may include, but is not limited to, independent contractors and consultants, translation services, off-site storage providers, information technology providers, event managers, credit managers or debt collecting agencies.

Any agreement made by Wentworth Healthcare with such a third-party provider will consider your right to privacy.

- ***Overseas disclosures***

  Wentworth Healthcare prefers to retain all personal information within Australia.

  If personal information is collected, and Wentworth Healthcare is aware that it may be disclosed to overseas recipients (such as use of a survey platform where the host server is

located overseas) our commitment to protecting your privacy will not change. Wentworth Healthcare will only transfer personal information where confident the information will be managed by the recipient in a manner that is aligned with the *Privacy Act 1988 (Cth)*.

Our websites

Wentworth Healthcare websites use cookies and web beacons.

- A cookie is a piece of code placed on a device, to recognise when that device has visited our website before. It distinguishes one user from another and can improve user experience.
- A web beacon is a piece of code placed on a webpage. When used with cookies, this can tell us what content is being accessed by users of our website.

We do not use cookies and web-beacons to identify you, however where an individual uses a login to access website functionality, this is personally identifiable.

For all website users, we may collect information such as pages visited, server address, type of browser used, operating system, top-level domain name and when access occurred. This information is solely used for the purpose of website management and development.

We use Google Analytics to monitor our website activity. Website users can prevent their data being used by Google Analytics through opt-out applications, such as the Google Analytics Opt-Out Browser Add-On.

- ***Other websites***

  Wentworth Healthcare seek to enhance user experience by providing links from our website to third-party websites and resources however we are not responsible for the content of these websites or resources. Providing a link does not endorse nor guarantee the accuracy of the information contained on that website or resource.

  We recommend that you review each third-party website's privacy policy, especially if you intend to disclose personal information via that site.

Questions or Complaints

If you have any questions or complaints regarding privacy, please contact us to discuss.

Webform:	Have your say | Nepean Blue Mountains PHN
Email:	privacy@nbmphn.com.au
Post:	Privacy Officer Wentworth Healthcare, Blg BR, Level 1, Suite 1, Locked Bag 1797, Penrith NSW 2751
Phone:	(02) 4708 8100

We will respond to your complaint within 30 days. Your complaint should provide sufficient detail to allow us to investigate and respond. You can find more information on our complaints process and your rights when using our services on our website.

If you are not satisfied with the way we handle your complaint, you may contact the Office of the Australian Information Commissioner.

6. Roles and Responsibilities

While the Board has ultimate accountability and responsibility, all staff have a role to play in ensuring our privacy obligations are satisfied.

Key appointments to support and monitor organisational privacy compliance are:

- **All Staff** are responsible for day-to-day implementation of the Wentworth Healthcare privacy policy.
- **The CEO** who is appointed by the Board to provide immediate oversight.
- **The CEO and Executive** who must ensure mechanisms are in place to provide assurance that ensure personal information is protected. Action and decisions regarding privacy may be informed and supported by Wentworth Healthcare Committees including the Board Finance and Audit Risk Management Committee, Board Clinical Governance Committee and Management's Data Governance Committee.
- **The Privacy Officer**, performed by the position of Executive Manager Corporate and Strategic Performance, must:
    - Be the first point of contact for all privacy matters for Wentworth Healthcare staff.
    - Promote strong privacy governance and capability within Wentworth Healthcare to support compliance.
    - Maintain an in-depth understanding of the Privacy Act, the Australian Government Agencies Privacy Code and other legislation that governs the way Wentworth Healthcare handles personal information with the ability to translate these requirements into practice.
    - Understand Wentworth Healthcare's strategic priorities and key projects involving the use of personal information.
    - Understand the systems and processes Wentworth Healthcare uses to handle personal information.
    - Understand privacy dispute resolution and complaint-handling methods and processes.
    - Perform the following functions (which may be delegated to the Performance and Planning Team who support the Privacy Officer role):
        - Provide advice on:
            - new initiatives that have a potential privacy impact.
            - general application of privacy law to Wentworth Healthcare activities.
            - whether or not to carry out a PIA or Dataset PIA.
            - safeguards to apply to mitigate risks to the privacy of individuals.
        - Liaise with the Office of the Australian Information Commissioner (OAIC).
        - Co-ordinate the handling of internal and external privacy enquiries, privacy of complaints, and requests for access to, and correction of, personal information.
        - Maintain a record of Wentworth Healthcare's personal information holdings.

- assist with the preparation of PIAs and Dataset PIAs.
- Measure and document Wentworth Healthcare's performance against its privacy management plan.
- Coordinate privacy training for staff.
- Proactively monitor compliance and manage Wentworth Healthcare's response to data breaches.

- **The Chief Data Officer**, performed by the position of Executive Manager Corporate and Strategic Performance who has ultimate accountability for the data within the PHN, and for decisions related to data including the privacy protection of the same data.
- **Nominated Data Sponsors**, Data Custodians and all Data Users who are responsible for taking reasonable steps to protect the privacy of personal information from inappropriate or unauthorised use, access or disclosure.

External parties can impact (or be impacted by) Wentworth Healthcare privacy compliance, accordingly Wentworth Healthcare must ensure that all **commissioned or contracted service providers** abide by Wentworth Healthcare's Privacy Policy by clearly articulating obligations in communications, notices and service agreements (contracts) where applicable.

7. Definitions

Australian Government Agencies Privacy Code:	The Australian Government Agencies Privacy Code (the Code) commenced on 1 July 2018. It applies to all Australian Government agencies subject to the Privacy Act 1988 (the Act) (except for Ministers) and is a binding legislative instrument under the Act. The Code sets out specific requirements and key practical steps that agencies must take as part of complying with APP 1.2. The Code: • Requires a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian Government agencies. • Enhances existing privacy capability within agencies, builds greater transparency in information handling practices, and fosters a culture of respect for privacy and the value of personal information. • Symbolises the commitment to protection of privacy, helps build public trust and confidence in personal information handling practices and new uses of data proposed by agencies.
Consent:	Consent means express consent or implied consent (s 6(1)). The four key elements of consent are: • The individual is adequately informed before giving consent.

- The individual gives consent voluntarily.
- The consent is current and specific, and
- The individual has the capacity to understand and communicate their consent.

Express consent is explicit, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement. **Implied consent** arises where consent may reasonably be inferred in the circumstances from the conduct of the individual.

Health Information: Information or an opinion, that also constitutes personal information, about:

- The health or disability (at any time) of an individual; or
- An individual's expressed wishes about the future provision of health services to him or her; or
- A health service provided, or to be provided, to an individual; that is also personal information; or
- Other personal information collected to provide, or in providing, a health service; or
- Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- Genetic information about an individual in a form that is, or could be, predictive of the health of the individual or genetic relative of the individual or a genetic relative of the individual.

8. References and Other Documents

Document Number	Document Name	Access point
3.06.01	Privacy Impact Assessment Procedure	Intranet
3.06.01.05	PIA Threshold Assessment Form	Intranet
	WHL Privacy Impact Assessment Report	Data team
NA	PIA Process Flowchart	Intranet
	WHL Privacy Impact Assessment Register	Data team
3.06.01.04	PIA Action Plan	Intranet
	WHL Dataset PIA Tool	Data team
3.06.01.02	Dataset PIA Guidelines	Intranet
	WHL Dataset PIAs Register	Data team
3.05	Data Breach Response Policy	Intranet
3.05.01	Data Breach Response Procedure	Intranet

3.05.01.01	Data Breach Response Guidelines	Intranet
3.02.05	Data Quality Policy	Intranet
3.02.06	Data Quality Procedure	Intranet
3.03	Data Access, Collection, Retention, Archive & Disposal Policy	Intranet
	WHL Data Asset Register	Data Team
	Wentworth Healthcare Data Sharing Agreements Register	Health Data Officer
1.11	Wentworth Healthcare Risk Management Policy	Intranet
3.14.01	Inbound (identified) Third Party Personal Information – Individuals (Procedure)	Intranet

9. Further Assistance

If you would like further information on our privacy policy, or if you have any concerns over the protection of your personal information, please contact our Privacy Officer.

10. Revisions Made to This Policy

Date	Major, Minor or Editorial Revision	Description of Revision	Author
30.11.2020	Revision		Elisa Manley
1/3/21	Editorial	Proofing and Formatting	Project Support Officer Business Improvement
15/4/21	Editorial	Corrected proofing errors	Project Support Officer Business Improvement
14/02/2024	Editorial	Updating and proofing	Elisa Manley Carolyn Townsend
17/02/25	Major	Plain English review to refine (but not amend intention of) policy. Required to ensure compliance with digital mental health accreditation for the IAR phone service which did not appear to be well addressed within existing policy.	