

Doctors' Health NSW – Privacy, Information Management and IT Security Policy

Document owner	Medical Director
Approved by	Board
Version date	4 August 2026
Next scheduled review	2028
Status	Approved

1. Purpose

This policy sets out how Doctors' Health NSW manages personal, health and organisational information to protect privacy, maintain confidentiality and support secure service delivery.

2. Scope

This policy applies to Board members, employees, contractors, call panel doctors and any person who collects, accesses, uses or manages information on behalf of Doctors' Health NSW.

3. Policy Statement

Trust is fundamental to the services provided by Doctors' Health NSW. Protecting the privacy, confidentiality and security of information is essential to maintaining that trust. Doctors' Health NSW manages information responsibly, lawfully and in accordance with best practice while recognising the unique importance of confidentiality to doctors and medical students seeking support.

4. Key Principles

- Only collect information necessary to provide services or meet legal obligations.
- Be open about why information is collected and how it will be used.
- Protect information from unauthorised access, loss or misuse.
- Use information only for the purpose for which it was collected unless otherwise permitted by law.
- Support individuals to access or correct their personal information where appropriate.
- Use de-identified information wherever possible for reporting, evaluation and quality improvement.

5. Confidentiality

The Doctors' Health NSW phone service is founded on confidentiality. Callers may remain anonymous. Identifying information is collected only where necessary, with the caller's agreement, and retained only for the shortest period necessary to support an agreed follow-up, referral or other authorised purpose.

- Calls are not recorded.
- Personally identifying information is retained only for as long as required for the agreed purpose.
- Clinical and activity reporting uses de-identified information.
- Information will only be disclosed with consent, where required or authorised by law, or where necessary to lessen or prevent a serious threat to life, health or safety.

6. Information Management

- Information is collected fairly and lawfully.
- Records are stored securely using approved systems.
- Access is limited to authorised people with a legitimate need to know.
- Records are retained only for as long as required by law or organisational need and are then securely destroyed or permanently de-identified.
- Personal information is only shared with third parties with the individual's consent, where required or authorised by law, or where necessary to lessen or prevent a serious threat to life, health or safety.

7. Information Security

Doctors' Health NSW engages an external IT provider to manage technical security controls. Overall responsibility for information governance remains with Doctors' Health NSW.

- Strong passwords and multi-factor authentication are used where available.
- Encryption, secure cloud storage and backups are maintained.
- Access to information systems is reviewed periodically to ensure access remains appropriate.
- Software and security controls are regularly reviewed.
- Suspected cyber security incidents must be reported immediately.

8. Data Breaches and IT Security Incidents

Any suspected privacy breach or cyber security incident must be reported immediately to the Medical Director. Incidents will be managed in accordance with the IT Incident Response Procedure, including assessment, containment, notification (where required) and review.

9. Responsibilities

Role	Responsibilities
Board	Oversee privacy, confidentiality and information governance.
Medical Director	Implement this policy, manage privacy risks, respond to breaches and ensure appropriate education.
Staff, contractors and call panel doctors	Protect confidential information, comply with this policy and report suspected breaches promptly.

External IT provider	Maintain technical security controls, support cyber security monitoring and assist with incident response.
----------------------	--

10. Related Documents

- Governance and Legal Compliance Policy
- Statement of Services
- Risk Management Policy
- Incident Management Procedure
- IT Incident Response Procedure
- Call Panel Privacy Statement

11. Relevant Legislation and Standards

- Privacy Act 1988 (Cth)
- Australian Privacy Principles
- Health Records and Information Privacy Act 2002 (NSW)
- Privacy and Personal Information Protection Act 1998 (NSW)
- National Standards for Doctors' Health Services

12. Document History

Date	Description of changes	Approved by
4 August 2026	Merged the former Privacy Policy and Data Management, Record-Keeping and IT Security Policy. Updated in plain English, strengthened confidentiality, clarified information governance responsibilities and aligned with current legislation and the National Standards.	Approved