Privacy and Information Storage Policy | Bloom Healthcare

Canonical: https://bloom-healthcare.com.au/privacy-policy/

Details:

This is Bloom Healthcare's privacy policy. It is the authoritative statement of how Bloom Healthcare collects, stores, uses and discloses personal information. The sections that follow set out the policy itself; the final part of the page explains the general legal setting it sits in and how to escalate a complaint.

1. Introduction to Our Privacy Policy

Bloom Healthcare is committed to protecting the privacy and personal information of its employees, clients, and stakeholders.

This Privacy and Information Storage Policy ensures that personal information is collected, stored, and used in accordance with the Privacy Act 1988 (Australia) and the Australian Privacy Principles.

Bloom Healthcare is governed by the guiding principles of the Privacy Act 1988. Our commitment to privacy is taken seriously, and we have systems and processes in place to ensure privacy is maintained at all times.

To provide high-quality healthcare services, personal information is required to be maintained and stored. Personal information is obtained so that we can:

Best tailor services to your needs

Evaluate and monitor program outcomes

Facilitate resolution of complaints with stakeholders

2. What This Privacy Policy Covers

This policy applies to all employees and contractors of Bloom Healthcare who have access to personal information as part of their work.

It covers all personal information collected, stored, or used by Bloom Healthcare while delivering healthcare and support services.

3. Purpose of Collecting Personal Information

The intent of this policy is to reaffirm our commitment to providing a safe, secure, and private healthcare service that complies both legally and ethically.

The purpose of this policy is to:

Ensure personal information is collected, stored, and used lawfully and ethically

Protect the privacy of individuals

Comply with the Privacy Act 1988 and Australian Privacy Principles

Promote a culture of privacy and data security

4. Roles and Responsibilities for Data Privacy

The Director/s and management team are responsible for ensuring this policy is implemented effectively.

Employees and contractors must:

Comply with this policy and relevant privacy laws

Report any privacy breaches or incidents

Participate in privacy and data security training

5. Collection, Use and Disclosure of Personal Information

5.1 How We Collect Personal Information

Bloom Healthcare collects personal information only for purposes relevant to our healthcare services and with your consent.

Consent may be provided verbally or in writing. However, written consent is required before sharing information with third parties (unless required by law). We limit collection to information that is necessary and ensure it is accurate, complete, and up to date.

5.2 Why We Use Your Information

We use personal information to:

Inform treatment and care decisions

Identify and protect the individual

Deliver safe and effective healthcare services

5.3 When We Share Personal Information

Personal information may be disclosed to:

Other treating healthcare professionals

Family or authorised representatives

Persons at direct or immediate risk

Law enforcement authorities

Referring organisations

Legal practitioners

Community service providers

Unless required by law, disclosure only occurs with written consent. Bloom Healthcare does not sell, trade, or rent personal information.

6. Information Storage, Security and Data Protection

Bloom Healthcare securely stores personal information to prevent unauthorised access, use, or disclosure.

We use a secure case management system where:

Only authorised personnel can access information

All activity and communication are managed within the system

Personal information from assessments and appointments is stored electronically, and hard copies are securely destroyed.

We use physical, technical, and administrative safeguards and regularly review our systems to maintain security.

7. Accessing and Correcting Your Personal Information

Bloom Healthcare recognises your right to access and correct your personal information.

You may:

Request access to your personal records

Request corrections to inaccurate or incomplete information

Please contact our team to make a request.

8. Data Access Controls and Confidentiality

Access to personal information is granted on a strict need-to-know basis.

Employees and contractors must not share or disclose information without authorisation.

All staff are required to:

Use strong passwords

Follow secure data handling practices

All data is backed up regularly and securely stored.

Personal information is deleted or destroyed when no longer required in accordance with the Privacy Act 1988.

9. Staff Training and Privacy Compliance

Bloom Healthcare provides ongoing training on privacy and confidentiality.

All employees and contractors:

Understand privacy obligations

Follow internal procedures

Management conducts annual reviews and self-assessments to ensure compliance and continuous improvement.

10. Privacy Complaints and Enquiries

Bloom Healthcare takes privacy concerns seriously and has procedures to respond promptly.

To raise a concern:

Speak with your clinician or manager

Email hello@bloom-healthcare.com.au

11. Data Breach Response and Incident Management

Bloom Healthcare has an Incident Response Procedure for suspected or confirmed data breaches.

This includes:

Immediate response and investigation

Notification of affected individuals where required

Reporting to relevant authorities

Implementing corrective actions

See also the Incident Management Policy .

12. Monitoring and Continuous Improvement

We regularly monitor and evaluate this policy using:

Feedback from clients and staff

Privacy incident reporting

Management tracks implementation and performance.

Employees and contractors are encouraged to provide feedback for improvement.

13. Policy Review and Updates

This policy is reviewed annually to ensure it remains compliant, effective, and up to date.

All updates are recorded in the Policy and Procedure Register.

Contacting Bloom Healthcare

Registration no: 4-JR6F5KX Provider no: 4050148863

Phone: 1300 771 465

Email: hello@bloom-healthcare.com.au

Hours: Monday to Thursday 7:30am–6pm, Friday 7:30am–5pm, Saturday by appointment

If you need this information in an accessible format, ask when you make contact. See the Accessibility Statement .

How this policy sits within Australian privacy law

This part of the page is general context. It does not change or add to the policy set out in the sections numbered 1 to 13, which is the text to rely on.

What an APP entity is

Australian privacy law is set by the Privacy Act 1988 and the 13 Australian Privacy Principles, usually shortened to the APPs. An organisation that the Privacy Act covers is often called an APP entity.

The APPs are principles-based and technology neutral, so they apply across different business models and change with technology rather than being tied to particular systems. They set standards for how personal information is collected, used and disclosed, how an organisation governs and accounts for its handling of that information, how it keeps information accurate and corrects it, and what access individuals have to information held about them.

Health service providers are covered. That includes doctors, private hospitals, pharmacists and allied health professionals such as physiotherapists, occupational therapists, speech pathologists, exercise physiologists and dietitians. The Office of the Australian Information Commissioner, the OAIC, publishes a Guide to Health Privacy for providers in this group.

The rights Australian privacy law gives you

These are general rights under the APPs. They are not a description of any one organisation's arrangements.

Transparency. An organisation covered by the Act has to manage personal information openly, and to have a clear and current policy about how it handles that information.

Anonymity and pseudonymity. Where it is practicable, you can deal with an organisation anonymously or under a pseudonym.

Access. You can ask to see the personal information an organisation holds about you.

Correction. You can ask for information about you to be corrected if it is wrong, out of date or incomplete.

Notification of serious breaches. Where a data breach is likely to cause serious harm, the law requires affected people and the OAIC to be told.

Complaint. You can complain if you believe an Australian Privacy Principle has been breached. A breach of an APP is treated as an interference with your privacy and can lead to regulatory action and penalties.

Escalating to the Office of the Australian Information Commissioner

The OAIC is the independent regulator that administers the Privacy Act and the Australian Privacy Principles.

The OAIC generally expects you to raise the matter with the organisation first and to allow around 30 days for a response. If you do not get a response in that time, or you are not satisfied with the response you get, you can take the complaint to the OAIC.

Complaints can be made through the privacy complaint form on the OAIC website, by email to enquiries@oaic.gov.au, or by post to GPO Box 5218, Sydney NSW 2001.

Common questions about privacy at Bloom Healthcare

Can I ask to see my own records?

Yes. Bloom Healthcare recognises your right to access and correct your personal information, and you can request access to your personal records or ask for corrections to information that is inaccurate or incomplete. Contact the team to make a request.

Will my information be shared without my consent?

Unless disclosure is required by law, information is only shared with your written consent. Bloom Healthcare does not sell, trade, or rent personal information.

Who might my information be shared with?

With your written consent, personal information may be disclosed to other treating healthcare professionals, family or authorised representatives, referring organisations, legal practitioners, community service providers, and — where there is direct or immediate risk — to persons at risk or to law enforcement authorities.

What happens if there is a data breach?

Bloom Healthcare has an Incident Response Procedure covering immediate response and investigation, notification of affected individuals where required, reporting to relevant authorities, and corrective action. Separately, Australian law requires that where a data breach is likely to cause serious harm, affected people and the OAIC are notified.

How long is my information kept?

Personal information is deleted or destroyed when it is no longer required, in accordance with the Privacy Act 1988.

How do I make a privacy complaint?

Start with Bloom Healthcare — speak with your clinician or manager, or email hello@bloom-healthcare.com.au. If you do not receive a response within about 30 days, or you are not satisfied with the response, you can take the complaint to the OAIC.

Is my health information treated differently from other personal information?

Health information is sensitive information under the Privacy Act, and health service providers are covered by the Act. The OAIC publishes a Guide to Health Privacy specifically for providers in this group.

How often is this policy reviewed?

Annually. All updates are recorded in the Policy and Procedure Register.

What is Bloom Healthcare's Privacy Policy based on?

Bloom Healthcare's Privacy Policy follows the Privacy Act 1988 (Australia) and the Australian Privacy Principles (APPs) to ensure full security in how personal information is collected, stored, and used.

Why does Bloom Healthcare collect personal information?

Bloom Healthcare collects personal information to tailor services to individual needs, evaluate and monitor program outcomes, and facilitate resolution of complaints, all for purposes relevant to healthcare services and with the individual's consent.

Does Bloom Healthcare need consent before sharing personal information with third parties?

Yes, written consent is required before sharing personal information with third parties, unless disclosure is required by law.

How does Bloom Healthcare use the personal information it collects?

Personal information is used to inform treatment and care decisions, identify and protect the individual, and deliver safe and effective healthcare services.

How does Bloom Healthcare store personal information securely?

Bloom Healthcare stores personal information in a secure case management system where only authorized personnel can access it, as part of multiple safeguards designed to prevent unauthorized access, use, or disclosure.

What are Bloom Healthcare's key commitments in its privacy approach?

Bloom Healthcare's privacy approach commits to legal compliance with the Privacy Act 1988, personalized service delivery based on collected personal information, and providing safe, secure, and private healthcare services that meet legal and ethical standards.

Does Bloom Healthcare limit the amount of personal information it collects?

Yes, Bloom Healthcare limits collection to information that is necessary and ensures it is accurate, complete, and up to date.

What is Bloom Healthcare and what services does it provide?

Bloom Healthcare is a boutique disability and aged care allied health provider that believes all people have the right to access quality healthcare, delivering evidence-based, client-centric services through highly qualified health practitioners across Australia.

Can I ask to see my own records?

Yes. Bloom Healthcare recognises your right to access and correct your personal information, and you can request access to your personal records or ask for corrections to information that is inaccurate or incomplete. Contact the team to make a request.

Will my information be shared without my consent?

Unless disclosure is required by law, information is only shared with your written consent. Bloom Healthcare does not sell, trade, or rent personal information.

Who might my information be shared with?

With your written consent, personal information may be disclosed to other treating healthcare professionals, family or authorised representatives, referring organisations, legal practitioners, community service providers, and — where there is direct or immediate risk — to persons at risk or to law enforcement authorities.

What happens if there is a data breach?

Bloom Healthcare has an Incident Response Procedure covering immediate response and investigation, notification of affected individuals where required, reporting to relevant authorities, and

corrective action. Separately, Australian law requires that where a data breach is likely to cause serious harm, affected people and the OAIC are notified.