



Brighton Family & Women's Clinic Privacy Policy

Current as of: 11.11.2025

The objective of this privacy notice is to provide you, our patient, with clear information on how your personal information is collected and used within the practice. Occasionally we also need to share your personal information to involve others in your healthcare and this policy outlines when, how, and why we share your information.

1. Who can I contact about this policy?

For enquiries concerning this policy, you can contact the managers via phone or email admin@brightonfwc.com.au

2. When and why is your consent necessary?

When you register as a patient of a practice, you provide consent for the GPs and staff to access and use your personal information to facilitate the delivery of healthcare. Access to your personal information is restricted to practice members who require it for your care. If we ever use your personal information for purposes other than healthcare provision, we will obtain additional consent from you.

It is important to us that you understand why we collect and use your personal information.

By acknowledging this Privacy Policy you consent to us collecting, holding, using, retaining and disclosing your personal information in the manners described below.

3. Why do we collect, use, store, and share your personal information?

The practice collects, uses, stores, and shares your personal information primarily to manage your health safely and effectively. This includes providing healthcare services, managing medical records, and ensuring accurate billing and payments. Additionally, we may utilise your information for internal quality and safety improvement processes such as practice audits, accreditation purposes, and staff training to maintain high-quality service standards.

4. What personal information is collected?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details
- medical information including medical history, medicines, allergies, and adverse reactions
immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifier numbers
- health fund details.

Your Patient Health Record is covered under our Privacy Policy. It includes information, held about a patient, in electronic form, which may include:

- contact and demographic information
- medical history

- clinical notes and observations
- images and photographs
- correspondence
- investigations
- test results
- prescription records
- medication charts
- insurance information
- legal information and reports
- work health and safety reports

5. Can you deal with us anonymously?

You can deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals. Examples of when it is impractical for us to deal with you anonymously include when processing Medicare claims, booking appointments, issuing prescriptions or referrals, ordering diagnostic tests, accessing My Health Record, transferring medical records, complying with mandatory reporting obligations, or providing clinical care that requires accurate identification to ensure your safety.

6. How is personal information collected?

Our practice will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, using, holding, and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (e.g., staff training).

When you make your first appointment, the practice team will collect your personal and demographic information via your registration. During the course of providing medical services, we may collect further personal information. Information can also be collected through electronic transfer of prescriptions (e-scripts), My Health Record, e.g., via Shared Health Summary, Event Summary. We do participate in these eHealth services.

We use document automation technologies so that only relevant information is included in referral letters.

We may also collect your personal information when you visit our website, send us an email or SMS, telephone us, make an online appointment, or communicate with us using social media.

In some circumstances, personal information may also be collected from other sources, including:

- Your guardian or responsible person.
- Other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services, and pathology and diagnostic imaging services.
- Your health fund, Medicare, or the Department of Veterans' Affairs (if relevant).
- While providing medical services, further personal information may be collected via:
 - electronic prescribing

- My Health Record
- online appointments

Various types of images may be collected and used, including:

- **CCTV footage:** Collected from our premises for security and safety purpose
- **Photos and medical images:** While the clinic provides dedicated devices for taking photos and medical images, these may also be taken using personal devices for medical purposes, following the guidelines outlined in our guide on using personal devices for medical images. The guidelines on using personal devices for medical images align with Australian privacy obligations, particularly the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth).

We will always comply with privacy obligations when collecting personal information from third-party sources. This includes ensuring transparency with patients, obtaining necessary consents, maintaining data accuracy, securing the information, and using it only for specified purposes.

7. When, why and with whom do we share your personal information?

We sometimes share your personal information:

- with third parties for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- with other healthcare providers (e.g. In referral letters)
- when it is required or authorised by law (e.g. court subpoenas)
- when it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of confidential dispute resolution process
- When it is a statutory requirement to share certain personal information (e.g. some diseases require mandatory notification)
- When it is provision of medical services, through electronic prescribing, My Health Record (e.g. via Shared Health Summary, Event Summary).

Only people who need to access your personal information will be able to do so. Other than providing medical services or as otherwise described in this policy, the practice will not share personal information with any third party without your consent.

We do not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

8. Will your information be used for marketing purposes?

The practice will not use your personal information for marketing any goods or services directly to you without your expressed consent. If you do consent, you may opt out of direct marketing at any time by notifying the practice in writing.

9. How is your information used to improve services?

The practice may use your personal information to improve the quality of the services offered to patients through research, analysis of patient data for quality improvement and for training activities with the practice team

We may provide de-identified data to other organisations to improve population health outcomes. The information is secure, patients cannot be identified, and the information is stored within Australia. You can let reception staff know if you do not want your information included.

10. How are document automation technologies used?

Document automation is where systems use existing data to generate electronic documents relating to medical conditions and healthcare.

The practice uses document automation technologies to create documents such as referrals, which are sent to other healthcare providers. These documents contain only your relevant medical information.

These document automation technologies are used through secure medical software Zedmed.

All users of the medical software have their own unique user credentials and password and can only access information that is relevant to their role in the practice team.

The practice complies with the Australian privacy legislation and APPs to protect your information.

All data, both electronic and paper are stored and managed in accordance with the Royal Australian College of General Practitioners [Privacy and managing health information guidance](#).

11. How is your personal information stored and protected?

Your personal information may be stored electronically and visually (e.g. photos, imaging). All information is stored on our secure servers which are protected by firewalls and encryption.

The practice stores all personal information securely. We do not record audio or visual information regarding telehealth consultations.

12. How can you access and correct your personal information at the practice?

You have the right to request access to, and correction of, your personal information.

The practice acknowledges patients may request access to their medical records.

Practice policy is for the patient to sign Transfer of Records form (available on the website or at reception). Once received your record will be forwarded within 28 days.

The practice will respond to any requests to access or correct your personal information within 7 business days.

The practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. Sometimes, we will ask you to verify your personal information held by the practice is correct and current. You may request we correct or update your information. To do this please contact via phone on 9516 5100 or email admin@brightonfwc.com.au

13. How can you lodge a privacy-related complaint, and how will the complaint be handled?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have. We will then attempt to resolve it in accordance with the resolution procedure.

If you do not feel we have resolved your issue You may also contact the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner will require you to give them time to respond before they investigate. For further information visit www.oaic.gov.au or call the OAIC (Office of the Australian Information Commissioner) on 1300 363 992.

14. How is privacy on the website maintained?

At Brighton Family & Women's Clinic any personal information you share with us through website, email, and social media, is handled securely and confidentially. This practice uses analytics and cookies.

15. How we use AI in the clinic

AI scribe may be used by the doctor in your consultation. This will never be used without your express verbal consent at each instance. We also ensure that the AI scribes used in the clinic are not stored on servers overseas, and that your data is deleted.

- Patients must be **informed** of the use of AI scribe software during their consultation.
- A **verbal or written consent** process must be documented, in accordance with guidelines from the Office of the Australian Information Commissioner (OAIC).
- Patients must be allowed to **opt out** of AI-assisted documentation at any time without affecting their care.

16. Privacy during telehealth and remote access

Doctors at BFWC will never access your information using their remote access in an inappropriate area. This means they won't access it in public, in areas of their residence that can be viewed by others, or on unsure networks.

Telehealth video is conducted via HealthDirect, which is a government approved encrypted platform. Use of this platform by the doctors ensures they do not access it in public, in areas of their residence that can be viewed by others, or on unsure networks. The same is true for phone consultations.

17. Policy review statement

Our privacy policy is regularly reviewed to ensure compliance with current obligations.

If any changes are made:

- They will be reflected on the website
- Significant changes may be communicated directly to patients via email or other means

Please check the policy periodically for updates. If you have any questions, feel free to contact us.