PRIORITY HEALTH GROUP - PRIVACY POLICY

INTRODUCTION

We are committed to protecting the privacy of patient information and to handling your personal information in a responsible manner in accordance with the Privacy Act 1988 (Cth), the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Australian Privacy Principles and relevant State and Territory privacy legislation (referred to as privacy legislation).

This Privacy Policy explains how we collect, use and disclose your personal information, how you may access that information and how you may seek the correction of any information. It also explains how you may make a complaint about a breach of privacy legislation.

This Privacy Policy is current as of 15/01/2026 and is reviewed annually. From time to time, we may make changes to our policy, processes and systems in relation to how we handle your personal information. We will update this Privacy Policy to reflect any changes. Those changes will be available on our website and in practice.

A patient Health record is a record where health data and other information related to the care of a patient is maintained.

COLLECTION

We collect information that is necessary and relevant to provide you with medical care and treatment and manage our medical practice. This information may include your name, address, date of birth, gender, health information, family history and contact details. This information may be stored on our computer medical records system.

Wherever practicable we will only collect information from you personally. We may also need to collect information from other sources such as treating specialists, radiologists, pathologists, hospitals, other health care providers, and the MyHealth record system.

We collect information in various ways, such as over the phone, or in writing, in person in our clinics or over the internet if you transact with us online. This information may be collected by medical and non-medical staff. In emergency situations we may also need to collect information from your relatives or friends. We may be required by law to retain medical records for certain periods of time depending on your age at the time we provide services.

DOCUMENT AUTOMATION TECHNOLOGIES

The practice uses document automation technologies within Best Practice to support the preparation of clinical documents, including referral letters and correspondence.

Templates and auto-populated fields are configured to extract relevant patient information directly from the clinical record, such as medical history, medications, allergies, investigation results, and consultation notes. Treating clinicians review and edit all generated documents prior to sending to ensure the information included is clinically relevant, accurate, and appropriate for the intended recipient.

The practice also limits unnecessary disclosure of information by:

- using referral templates tailored to the purpose of the referral;
- including only information relevant to the patient's ongoing care and treatment;
- requiring clinician oversight before documents are finalised

These processes assist the practice in maintaining patient confidentiality, supporting accurate communication, and complying with privacy and professional obligations.

PATIENT CONSENT FOR TELEHEALTH AND USE OF TRANSCRIBING TOOLS

The practice is committed to protecting patient privacy, confidentiality, and the security of personal health information during all Telehealth consultations, including telephone and video consultations. Prior to commencing any Telehealth consultation, the treating doctor will:

- obtain the patient's consent to proceed with the Telehealth consultation;
- verify the patient's identity through a three-point identity check; and
- discuss the limitations of Telehealth consultations, including the inability to conduct a physical examination where applicable and any potential clinical limitations associated with remote consultations.

The practice ensures that:

- all Telehealth consultations are conducted using secure and appropriate communication methods;
- patient information is handled in accordance with applicable privacy legislation and professional obligations;
- any clinical notes, recordings, or transcriptions are securely stored within the patient's clinical record; and
- access to patient information is restricted to authorised personnel only.

Where a treating doctor uses AI-assisted transcription, or any real-time audio or visual recording of a consultation (including Telehealth and consultations conducted remotely), the patient's informed consent is obtained before recording or transcription commences. Any recording, duplication, and storage of a consultation is undertaken only with that consent and is managed securely within the patient's clinical record. The practice ensures that:

- Only clinically relevant information is incorporated into the patient record or correspondence;
- recordings or transcriptions are handled in accordance with privacy and confidentiality obligations;
- secure systems and access controls are maintained; and
- clinicians review all generated documentation for accuracy and appropriateness before finalisation.

Written consent is obtained from the patient on an initial one-time basis prior to the use of any audio/visual recording or transcription technology. At subsequent visits, the patient's ongoing consent is verbally confirmed and documented within the clinical record for each consultation.

USE AND DISCLOSURE

We will treat your personal information as strictly private and confidential. Personal information will only be used for the purpose of providing medical services and for claims and payments, unless otherwise consented to. Some disclosure may occur to third parties engaged by or for the Practice for business purposes, such as Accreditation or for the provision of Information Technology. These third parties are required to comply with this Policy undersigned, written agreements.

The Practice will inform the patient where there is a statutory requirement to disclose certain personal information (for example, some diseases require mandatory notification).

The Practice will not disclose personal information to any third party other than in the course of providing medical services, without full disclosure to the patient or the recipient, the reason for the information transfer and full consent from the patient. The Practice will not disclose personal information to anyone outside Australia without need and without patient consent.

Exceptions to disclose without patient consent are where the information is:

- For medical defence purposes;
- As required by law in instances of mandatory reporting of communicable diseases;
- Necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health safety, or it is impracticable to obtain patient's consent;
- To assist in locating a missing person
- For the purpose the patient was advised during consult with the treating Doctor;
- As required during the normal operation of services provided. i.e. for referral to a medical specialist or other health service provider;
- To establish, exercise or defend an equitable claim
- For the purpose of a confidential dispute resolution process
- Some disclosure may occur to third parties engaged by or for the practice for the Practice for business purposes such as accreditation or for the provision of information technology. These third parties are required to comply with this policy.

The Practice may use a patient's contact information as supplied to the Practice (mailing address, telephone numbers (including mobile phones and email addresses) in order to contact patients for appointment reminders, recall reminders and to request a patient to attend to discuss, for example, test results. At no time will a patient's actual medical information be sent to them in this way (as we have no way to guarantee who sees it) without the patient's express permission. For the above reasons, the practice does not undertake to give medical advice to patients via email requests.

If a patient wishes to forward copies of their confidential medical information to us via email they may do so to myGP@priorityhealthgroup.com.au, they are considered to be doing so at their own risk.

The Practice will not use any personal information in relation to direct marketing to a patient without that patient's express consent. Patients may opt-out of direct marketing at any time by notifying the Practice in a letter or email. The Practice will comply with Australian Privacy Principle 8 — cross-border disclosure of personal information when health information is likely to be disclosed oversees.

The Practice evaluates all unsolicited information it receives to decide if it should be kept, acted on or destroyed.

DATA QUALITY AND SECURITY

We will take reasonable steps to ensure that your personal information is accurate, complete, up to date and relevant. For this purpose, our staff may ask you to confirm that your contact details are correct when you attend a consultation. We request that you let us know if any of the information we hold about you is incorrect or out of date.

Only the relevant information is included in referral letters. The practice software (Best Practice) has automated referral templates pre-programed in the system that all practitioners use in our clinic.
Personal information that we hold is protected by:

- securing our premises
- placing passwords and varying access levels on databases to limit access and protect electronic information from unauthorised interference, access, modification, and disclosure; and
- providing locked cabinets and rooms for the storage of physical records.

STORAGE OF OFFICIAL DOCUMENTS

The practice securely stores all official documents to prevent unauthorised access, use, alteration, loss or removal. Official documents include prescription forms, administrative records, document templates and practice letterhead, as well as patient health records. Electronic information and documents are stored within our clinical software (Best Practice), our Microsoft 365 environment, and the practice's servers.
These systems are protected by measures including individual user accounts and passwords, role-based access levels that restrict access to authorised personnel, regular data backups, and current security controls maintained on our servers and Microsoft 365 environment. Physical official documents, such as blank prescription forms and letterhead, are kept on secured premises in locked cabinets or rooms, with access limited to authorised staff. Pre-printed prescription forms, letterhead and templates are stored securely to prevent misuse or unauthorised reproduction, and obsolete or superseded official documents are disposed of securely.

NOTIFIABLE DATA BREACHES

The practice complies with the Notifiable Data Breaches (NDB) scheme established under Part IIIC of the Privacy Act 1988 (Cth). A data breach occurs when personal information held by the practice is lost, or is accessed, disclosed or modified without authorisation.
Where the practice becomes aware of an actual or suspected data breach, we will promptly assess the circumstances and take reasonable steps to contain the breach and limit any resulting harm. An eligible data breach is one that is likely to result in serious harm to one or more individuals and that the practice has not been able to prevent.
If the practice determines that an eligible data breach has occurred, we will notify the affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable, in accordance with our obligations under the Privacy Act 1988 (Cth). The practice maintains a data breach response process to guide staff in identifying, escalating, managing and recording any actual or suspected breach.

GOVERNMENT-RELATED IDENTIFIERS

In the course of providing care and managing claims and payments, the practice collects government-related identifiers, such as Medicare numbers, Department of Veterans' Affairs numbers, Individual Healthcare Identifiers (IHIs) and Pensioner Concession Card numbers. We do not adopt a government-related identifier as our own means of identifying a patient. We use and disclose these identifiers only where reasonably necessary to verify a patient's identity, to fulfil our obligations to an agency (for example, for Medicare billing and claiming), or where otherwise required or authorised by law, consistent with Australian Privacy Principle 9.

MY HEALTH RECORD

The practice participates in the My Health Record system. Where a patient has a My Health Record, authorised members of the practice team may access and upload clinical information (such as shared health summaries, event summaries and prescription information) to support safe and continuous care.
Access to the My Health Record system is limited to authorised personnel, is governed by the My Health

Records Act 2012 (Cth) and its associated rules, and is managed in accordance with the practice's My Health Record Security and Access Policy. Patients may ask the practice not to access or upload to their My Health Record, and may set their own access controls directly through the My Health Record system.

CORRECTIONS

If you believe that the information we have about you is not accurate, complete, or up to date, we ask that you contact us in writing (see details below).

ACCESS

You are entitled to request access to your medical records. We request that you put your request in writing and we will respond to it within a reasonable time.
There may be a fee for the administrative costs of retrieving and providing you with copies of your medical records.

We may deny access to your medical records in certain circumstances permitted by law, for example, if disclosure may cause a serious threat to your health or safety. We will always tell you why access is denied and the options you must respond to our decision.

TRANSFER OF PATIENT HEALTH INFORMATION

The practice transfers patient health information — for example, when a patient moves to another practice, is referred to another provider, or requests that a copy of their records be sent to a third party — only in response to a valid request and in accordance with privacy legislation and the Australian Privacy Principles.
Before transferring health information, the practice determines that the request is valid by:

- verifying the identity of the patient and, where the request is made by a third party, confirming their authority to receive the information;
- obtaining the patient's consent (or confirming another lawful basis) for the transfer, unless the disclosure is otherwise required or authorised by law;
- confirming the scope of the request and that only the information relevant to that request is transferred.

Once a request is verified, the practice transfers the information within a reasonable timeframe so as not to disadvantage the patient's ongoing care. Information is transferred using secure mechanisms — such as secure clinical messaging, encrypted electronic transfer, the My Health Record system where appropriate, or sealed and clearly addressed mail — and the practice does not transfer health information by unsecured means. Where information is sent electronically, staff confirm the recipient's correct and secure delivery details before sending. A record of the request and the transfer is documented in the patient's clinical record. These procedures are supported by the practice's related policies and staff training, and reasonable administrative costs of providing copies may apply as set out in the Access section above.

OVERSEAS TRANSFER OF DATA

We will not transfer your personal information to an overseas recipient unless we have your consent, or we are required to do so by law.

HOW CAN YOU LODGE A PRIVACY RELATED COMPLAINT, AND HOW WILL THE COMPLAINT BE HANDLED AT OUR PRACTICE?

We take complaints and concerns about the privacy of patients' personal information seriously. Patients should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with its complaint resolution procedure.

PLEASE ADDRESS ALL COMPLAINTS TO:
Managing Director
C/O: Priority Health Group & Emerald Surgery
53 Ruby Street Emerald | 46 Ruby Street,
Emerald QLD 4720,
or email: schifadza@priorityhealthgroup.com.au

DEALING WITH US ANONYMOUSLY
You have the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorized by law to only deal with identified individuals. We will endeavor to respond to all complaints within a reasonable time, which will not be longer than 21 working days.

POLICY REVIEW STATEMENT
This policy will be reviewed and updated / amended annually.
Contact us regarding any privacy concerns on:
Phone: 07 4910 7800
Fax: 07 3040 4434
Email: myGP@priorityhealthgroup.com.au

POST
C/O – Managing Director
Priority Health Group - 53 Ruby Street
Emerald, QLD 4720

For more information, visit the website of the Office of the Health Ombudsman. You will be able to access a range of general and health related privacy information here http://www.oaic.gov.au. If the complaint has not been resolved to your level of satisfaction all complaints should be directed to:

Office of the Health Ombudsman
Email: complaints@oho.qld.gov.au
Phone: 133 OHO (131 646)

Mail: Office of the Health Ombudsman
PO Box 13281
BRISBANE QLD 4003

Website: http://www.oho.qld.gov.au

SUPPORTING DOCUMENTATION
National Privacy Principles
Freedom of Information Act 2001

DOCUMENT REVIEW DETAILS

Review Date:	January 2026
Next Review:	January 2027
Approving officer:	Saru Chifadza
Position:	Managing Director - Priority Health Group & Emerald Surgery