

Nundah Village Family Practice

Privacy Policy

Purpose

To ensure patients who receive care from the Practice are comfortable in entrusting their health information to the Practice. This policy provides information to patients as to how their personal information (which includes their health information) is collected and used within the Practice, and the circumstances in which we may disclose it to third parties.

Related standards

RACGP Compliance indicators for the Australian Privacy Principles: an addendum to the computer and information security standards (Second edition).

Background and Rationale

The APPs provide a privacy protection framework that supports the rights and obligations of collecting, holding, using, accessing and correcting personal information. The APPs consist of 13 principle-based laws and apply equally to paper-based and digital environments. The APPs complement the long-standing general practice obligation to manage personal information in a regulated, open and transparent manner.

This policy will guide Practice staff in meeting these legal obligations. It also details to patients how the Practice uses their personal information. The policy must be made available to patients upon request.

Practice Procedure

The Practice will:

- provide a copy of this policy upon request
- ensure staff comply with the APPs and deal appropriately with inquiries or concerns
- take such steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance with the APPs and deal with inquiries or complaints
- collect personal information for the primary purpose of managing a patient's healthcare and for financial claims and payments
- take reasonable steps to ensure the secure handling and storage of personal information, including electronic security, password protection, restricted access, and secure disposal
- comply with the Notifiable Data Breaches (NDB) scheme where required

Staff Responsibility

The Practice's staff will take reasonable steps to ensure patients understand:

- what information has been and is being collected
- why the information is being collected, and whether this is due to a legal requirement
- how the information will be used or disclosed
- why and when their consent is necessary
- the Practice's procedures for access and correction of information, and responding to complaints of information breaches, including by providing this policy
- that the Practice acknowledges, records and implements the affirmed **names, gender identity and pronouns** used by each patient

Patient Consent

The Practice will only interpret and apply a patient's consent for the primary purpose for which it was provided. The Practice staff must seek additional consent from the patient if the personal information collected may be used for any other purpose.

Collection of Information

The Practice will need to collect personal information as a provision of clinical services to a patient at the Practice. Collected personal information will include patients':

- names, addresses and contact details
- affirmed name, gender identity and pronouns (where provided)
- Medicare number (where available) (for identification and claiming purposes)
- healthcare identifiers
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors.

A patient's personal information may be held at the Practice in various forms:

- as paper records
- as electronic records
- as visual – x-rays, CT scans, videos and photos
- as audio recordings.

The Practice's procedure for collecting personal information is set out below.

1. Practice staff collect patients' personal and demographic information via registration when patients present to the Practice for the first time. Patients are encouraged to pay attention to the collection statement attached to/within the form and information about the management of collected information and patient privacy.

2. During the course of providing medical services, the Practice's healthcare practitioners will consequently collect further personal information.
3. Personal information may also be collected from the patient's guardian or responsible person (where practicable and necessary), or from any other involved healthcare specialists.

The Practice holds all personal information securely, whether in electronic format, in protected information systems or in hard copy format in a secured environment.

Electronic Communication

The Practice may use SMS, email or secure online platforms (such as HotDoc) to communicate appointment reminders, recalls and relevant administrative information. Patients may opt out of electronic communication at any time. Sensitive clinical information is transmitted using secure methods wherever possible.

Use and Disclosure of Information

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.

The Practice may access or upload information to a patient's My Health Record where appropriate and in accordance with national eHealth regulations.

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:

- required by law
- 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 a confidential dispute resolution process.

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

The Practice may use **de-identified** data for quality improvement, teaching or reporting activities. No identifiable information will be used without patient consent.

Access, Corrections and Privacy Concerns

The Practice acknowledges patients may request access to their medical records. Patients are encouraged to make this request in writing, and the Practice will respond within a reasonable time.

The Practice will take reasonable steps to correct personal information where it is satisfied that the information is not accurate or up to date. From time to time, the Practice will ask patients to verify the personal information held by the Practice is correct and up to date. Patients may also request the Practice correct or update their information, and patients should make such requests in writing.

The Practice retains personal health information for the minimum time required by law (generally seven years from last contact, or until a child turns 25).

The Practice takes complaints and concerns about the privacy of patients' personal information seriously. Patients should express any privacy concerns in writing. The Practice will then attempt to resolve it in accordance with its complaint resolution procedure.

If a data breach occurs that is likely to result in serious harm, the Practice will comply with the **Notifiable Data Breaches** scheme and notify affected individuals and the Office of the Australian Information Commissioner (OAIC) where required.