ROKEBY GP
A Better Experience

Privacy Policy 2018

Policy for the Management of Health Information

Nature and scope of this practice policy
This policy primarily addresses the management of 'personal health information' in the practice.

The policy covers the following areas:

1. Privacy
2. Informing new patients
3. Patient access to their personal health information
4. Alteration of patient records
5. Access to personal health information by practice staff for the purposes of research, professional development and quality assurance/improvement
6. Confidentiality agreements
7. Disclosure to third parties
8. Requests for personal health information and medical records by other medical practices
9. Security
10. Complaints about privacy related matters
11. Retention of medical records
12. Staff training

This policy:

In March 2014, privacy law reforms introduced the Australian Privacy Principles (APPs) into the Privacy Act 1988. The APPs regulate the handling of personal information by both Australian government agencies and some private sector organisations. The reforms compliment the culture of confidentiality that exists in general practice.

Practices should familiarise with the APPs, including the Australian Privacy Principle Guidelines published by the Office of the Australian Information Commissioner. The Guidelines are available at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines

ROKEBY GP
A Better Experience

This practice complies with both laws and the Australian and Health Privacy Principles (APPs & HPPs) adopted therein. See summary headings of Principles in this section. Both Acts give individuals the right to know what information a private sector organisation holds about them, the right to access this information and to also make corrections if they consider data is incorrect.

Australian Privacy Principles

APP 1: Open and transparent management of personal information.
APP 2: Anonymity and pseudonymity.
APP 3: Collection of solicited personal information.
APP 4: Dealing with unsolicited personal information.
APP 5: Notification of the collection of personal information.
APP 6: Use or disclosure of personal information.
APP 7: Direct marketing.
APP 8: Cross-border disclosure of personal information.
APP 9: Adoption, use or disclosure of government related identifiers.
APP10: Quality of personal information.
APP11: Security of personal information.
APP12: Access to personal information.
APP13: Correction of personal information.

As adopted within *Commonwealth Privacy Amendment (Private Sector) Act* (2000):

We have a privacy policy in place that sets out how to manage health information and the steps an individual must take to obtain access to their health information. This includes the different forms of access and the applicable time frames and fees.

While the policy focuses on the management of the patient's health record, it also relates to other recorded information, for example Medicare data, billing and accounting records, pathology and radiology results, medical certificates and letters to and from hospitals and other doctors.

ROKEBY GP

A Better Experience

1. Privacy

Personal health information is defined as information concerning a patient's health, medical history, or past or present medical care; and which is in a form that enables or could enable the patient to be identified. It includes information about an individual's express wishes concerning current and future health services.

All GP's and practice staff will ensure that patients can discuss issues relating to their health, and that the GP can record relevant personal health information, in a setting that provides visual privacy and protects against any conversation being overheard by a third party.

Staff will not enter a consultation room during a consultation without knocking or otherwise communicating with the GP.

Staff and students will not be present during the consultation without the prior permission of the patient.

2. Informing new patients

GPs will discuss the practice's privacy policy with patients who are new to the practice at their first visit or when it is clear that the patient is continuing with the practice.

New patients will be offered the practice's leaflet about personal information, privacy and their GP, and will be offered access to the practice information policy.

This practice tries to make sure that the information on privacy available to patients is appropriate for the range of people who come here. Feedback about the information is welcome.

Information provided to patients, both by GPs and staff verbally will advise that, for the purpose of patient care and teaching, this practice normally allows access to patient records by:

- other GPs in the practice
- GP locums, and
- general practice registrars attached to the practice for training.

The GP will provide the patient with opportunity to limited access to their record and will note any requirements in the 'alert' section of the computerised record.

GPs will make a contemporaneous note in the patient's record outlining the patient's consent to the collection and use of information that is particularly sensitive.

The practice will inform the patient through practice leaflets the option of not being identified when a health service at the practice is accessed, as long as it is lawful and practical to do so. Patients will be encouraged to use a consistent alias or code to enable records to be kept for continuity of care. Patients will be made aware that normal fee arrangements will apply, and a Medicare rebate may not be able to be claimed.

The practice staff, including its GPs will endeavour to ensure that continuing patients of the practice are informed about the impact of changes to privacy legislation, by bringing relevant materials to the attention of continuing patients.

ROKEBY GP
A Better Experience

3. Patient access to their personal health information

Under privacy legislation provisions, all patients have the right to access their health information stored at the practice. The treating GP will provide an up to date and accurate summary of their health information on request or whenever appropriate.

The treating GP will consider all requests made by a patient for access to their medical record. In doing so the GP will need to consider the risk of any physical or mental harm resulting from the disclosure of health information.

If the GP is satisfied that the patient may safely obtain the record then he/she will either show the patient the record, or arrange for provision of a photocopy, and explain the contents to the patient.

Any information that is provided by others (such as information provided by a referring medical practitioner or another medical specialist) is part of the health record and can be accessed by the patient.

Appropriate administration costs may be charged to the patient.

The practice will comply with all relevant State and Commonwealth legislation with regard to a patient's request for access to their personal health records.

4. Alteration of patient records

This practice will alter personal health information at the request of the patient when the request for alteration is straightforward (eg. amending an address or telephone number).

With most requests to alter or correct information, the General Practitioner will annotate the patient's record to indicate the nature of the request and whether the GP agrees with it. For legal reasons, the doctor will not alter or erase the original entry.

5. Access to personal health information by practice staff for the purposes of research, professional development and quality assurance/improvement.

New patients will also be informed that the practice undertakes research, professional development, and quality assurance/improvement (QA) activities from time to time, to improve individual and community health care and practice management.

Patients will be advised of the ways in which the practice undertakes 'recall' and 'follow-up' activities, eg. when the practice would write to a patient or phone them.

When a patient agrees to participate in a recall or reminder system, the doctor will make a note of this in their record.

Should this general practice decide to stop a recall or reminder system, it will write to each person on the system at their last known address, and advise them that the system will be ceasing.

Patients will be informed when quality improvement, professional development and research activities are being conducted and given the opportunity to 'opt out' of any involvement in these activities. The GP responsible for the activity will ensure that appropriate information is available to patients from the reception staff.

When research projects are conducted in the practice under the approval of an institutional ethics committee, staff will be made aware of the requirements to obtain consent specified in the research protocol and ensure that consent is properly obtained.

Where possible identifying information will be removed from personal health information being used for research and QA activities. Where this is not possible, internal staff accessing personal health information are aware that they are under an obligation of confidentiality not to disclose the information. Breaches of that obligation may result in instant dismissal. The GP from the practice who is responsible will ensure that any external researchers are also under an explicit written obligation of confidentiality with appropriate penalties for disclosure.

6. Confidentiality agreements

In order to protect personal privacy, this practice has staff, including temporary or casual staff; sub-contractors (eg. software providers etc.) and medical students sign a confidentiality agreement.

7. Disclosure to third parties

GP's and staff will ensure that personal health information is disclosed to third parties only where consent of the patient has been obtained. Exceptions to this rule occur when the disclosure is necessary to manage a serious and imminent threat to the patient's health or welfare, or is required by law.

The GP will refer to relevant legislation and the maturity of the patient before deciding whether the patient (in this case a minor) can make decisions about the use and disclosure of information independently (ie. without the consent of a parent or guardian). For example, for the patient to consent to treatment, the GP must be satisfied that the patient (a minor) is aware and able to understand the nature, consequences and risks of the proposed treatment. This patient is then also able to make decisions on the use and disclosure of his or her health information.

GP's will explain the nature of any information about the patient to be provided to other people, for example, in letters of referral to hospitals or specialists. The patient consents to the provision of this information by agreeing to take the letter to the hospital or specialist, or by agreeing for the practice to send it.

NOTE: Increasingly there is an expectation by patients that they will see and be advised of the contents of referral letters. They are able to access such letters in their records.

GP's and staff will disclose to third parties only that information which is required to fulfil the needs of the patient.

These principles apply to the personal information provided to a treating team (for example, a physiotherapist or consultant physician also involved in a person's care). The principles also apply where the information is transferred by other means, for example, via an intranet.

Information classified by a patient as restricted will not be disclosed to third parties without the explicit consent of the patient. GP's will make a contemporaneous note when such permission is given.

Information disclosed to Medicare or other health insurers will be limited to the minimum required to obtain insurance rebates.

Should an outstanding debt be referred to a collection agency, this practice will provide only the contact details of the debtor and the amount of the debt. No other personal information will be provided.

Information supplied in response to a court order will be limited to the matter under consideration by the court.

From time to time General Practitioners will provide their medical defence organisation or insurer with information, in order to meet their insurance obligations.

This practice participates in practice accreditation, which assists it to improve the quality of its services. Practice accreditation may involve the 'surveyors' who visit the practice reviewing patient records to ensure that appropriate standards are being met. This practice will advise patients when practice accreditation is occurring by placing a notice in the foyer prior to the survey visit occurring. Patient will be given the opportunity of refusing accreditation surveyors access to their (the patient's) health information.

8. Requests for personal health information and medical records by other medical practices

Access to accurate and up to date information about the patient by a new treating GP is integral to the GP providing high quality health care.

This practice engages an after-hours service to provide care, and will allow this service to have access to a patient's personal health information in order to assist the after-hours service to provide high quality care. Our after-hours care provider is WADMS and they have access to patient information via telephone, fax and email.

If a patient transfers away from the practice to another GP, and the patient requests that the medical record be transferred, the existing GP will provide a summary to the new treating GP or to the patient. This practice will retain original documents and records.

This practice will seek written permission from the patient for the provision of personal health information to another medical practice.

The practice will provide summaries of patient's records to other doctors without charge as a matter of good clinical practice. Requests for more detailed information may be submitted to the practice for review by the patient's doctor or a practice partner. The practice reserves the right to charge reasonable administration costs. The practice will comply with all relevant State and Commonwealth legislation with regard to access to patient records.

9. Security

Medical practitioners, practice staff and contractors will protect personal health information against unauthorised access, modification or disclosure and misuse and loss while it is being stored or actively used for continued management of the patient's health care.

Staff will ensure that patients, visitors and other health care providers to the practice do not have unauthorised access to the medical record storage area or computers.

Staff will ensure that records, pathology test results, and any other papers or electronic devices containing personal health information are not left where they may be accessed by unauthorised persons.

Non clinical staff will limit their access to personal health information to the minimum necessary for the performance of their duties.

Fax, email and telephone messages will be treated with security equal to that applying to medical records.

Computer screens will be positioned to prevent unauthorised viewing of personal health information. Through the use of, for example, password-protected screen-savers, staff will ensure that computers left unattended cannot be accessed by unauthorised persons.

Medical practitioners and staff will ensure that personal health information held in the practice is secured against loss or alteration of data. This includes adherence to national encryption protocols.

Manual medical records and other papers containing personal health information will be filed promptly after each patient contact as appropriate.

Staff will ensure that manual and electronic records, computers, other electronic devices and filing areas are secured at the end of each day and that the building is locked when leaving.

The data on the computer system will be backed up daily and a duplicate backup drive given to the nominated staff member for storage off site. Backups should be routinely tested to ensure daily duplication processes are valid and retrievable.

10. Complaints about privacy-related matters

Complaints about privacy-related matters will be addressed in the same way as other complaints. This procedure is outlined elsewhere in this practice's procedures manual.

11. Retention of medical records

It is the policy of the practice that individual patient medical records be retained until the patient has reached the age of 25 or for a minimum of 7 years from the time of last contact, whichever is the longer. No record will be destroyed at any time without the permission of the treating GP or of the authorised GP in the practice.

In the event of a GP dying or transferring out of the practice, the practice may post a notice in the practice waiting room, or a GP who is leaving the practice may write individually to each patient, asking them to nominate a practitioner to whom the record should be transferred.

If the practice closes, patients will be contacted individually or, if this is not practical, a public notice will be placed in the local newspaper indicating how patients may arrange for their record to be transferred to another GP. In the event of the practice closing, it has been arranged that any medical records not transferred will be stored securely under the supervision of the Managing Partner.

12. Staff training

Practice training and induction procedures for medical practitioners and staff should ensure that medical practitioners and staff demonstrate understanding of this policy.
Ongoing education and training processes in the practice will ensure that skills and competence in the implementation of the privacy policy and related issues are maintained and updated

ROKEBY GP
A Better Experience

.

13. Contact details

Rokeby GP can be contacted via:

Phone:	08 9381 4880
Post:	PO Box 2122 Subiaco WA 6904
Address:	1/142 Rokeby Road Subiaco WA 6008
Email:	info@rokebygp.com.au