Practice Patient Privacy Policies & Forms 2025

Based on RACGP Privacy and managing health information in general practice
May 2023

Practice Patient Privacy Policy

South Coast Medical (Practice) takes your privacy seriously. This privacy policy is to provide information to you, the patient, with clear information on how your personal information (which includes your health information) is collected and used within the practice and the circumstances in which we may share it with third parties when it is necessary to involve others in your healthcare. The Practice Manager can assist you with further queries on this policy.

Privacy protection and confidentiality of health information is essential for quality health care and we are committed to protecting the privacy and confidentiality of the information we handle about you.

This policy explains:

- how we collect, store, use and disclose your personal information
- how you may access your personal information
- how we protect the quality and security of your personal information
- how you may seek correction of any personal information we hold
- how we will respond if we suspect that there has been a breach of our electronic data security
- how you may make a complaint about our handling of your personal information

In addition to our professional and ethical obligations, at a minimum, the Practice handles your personal information in accordance with federal and state privacy law. This includes complying with the federal Australian Privacy Principles (APPs) forming part of the Privacy Act 1998 (Cth) and the Victorian Health Privacy Principles (HPPs) forming part of the Health Records Act 2001 (Vic).

More information about the APPs and HPPs can be found on the Australian Information Commissioner's website www.oaic.gov.au or in hard copy on request from our Practice.

Why and When Your Consent is Necessary

When you register as a patient of South Coast Medical, you provide consent for the GP's and practice staff to access and use your personal information in order to provide you with the best healthcare possible. Only staff or independent medical practitioners that need access to your personal information to provide you care will have access to view it. If your information is required for any other purpose, we will request additional consent from you to do this. It is important that you understand why we collect and use your personal information.

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

Why do we collect, use, hold and share your personal information?

South Coast Medical needs to collect your personal information in order to provide healthcare services to you. We collect, use, hold and share your personal information to manage your health. This includes providing healthcare services, managing medical records, and ensuring accurate billing and payments. We also use it for directly relating business activities, such as financial claims and payments, practice audits and accreditation and business processes (eg. staff training)

Practice Patient Privacy Policy

Collection of Information

The Practice collects and holds personal information about you so that we may properly assess, diagnose, treat and be proactive in your health care needs. The type of personal information we collect may include:

- personal details (name, address, date of birth, Medicare number, health identifier numbers)
- your medical history (including medical history, medications, allergies, immunisations, social history, family history and risk factors)
- notes made during the course of a medical consultation
- referral to other health services providers
- results and reports received from other health service providers

How is personal information collected?

Wherever practicable we will collect this information from you personally - either at the Practice, online via patient registration or consent forms, over the phone, via written or email correspondence or via internet (including social media) if you transact with us online.

In some instances, we may need to collect information about you from other sources when it is not practical or reasonable to collect it from you directly. This may include information from:

- Your guardian, POA or responsible person
- Other involved healthcare providers; such as referring doctors, treating specialists, pathology, radiology, allied health professionals, hospitals or other health care providers.
- My Health Record, eg. via Shared Health Summary, Event or Discharge Summary
- Your health fund, Medicare or the Department of Veteran's Affairs (as necessary)

In an emergency, we may collect information from your immediate family, friends or carers.

Various types of images may be collected and used when attending a clinic, including:

- CCTV footage: collected from the premises for security and safety purposes only
- Photos and Medical images: These can be taken using personal devices for medical purposes, following the guidelines outlined in the guide on using personal devices for medical images.

Dealing with South Coast Medical anonymously

You have the right to deal anonymously or under a pseudonym in some circumstances. However, it is impractical in a healthcare setting, particularly for prescribing (APP2)

Practice Patient Privacy Policy

Use and Disclosure to other Parties

Your personal information will only be used or disclosed for purposes directly related to providing you with quality health care, or in ways you would reasonably expect us to use it in order to provide you with this service.

This includes use or disclosure:

- to the professional team directly involved in your health care, including treating doctors, pathology services, radiology services and other specialists outside this medical practice. For example, this may occur through referral to other doctors when requesting medical tests or in the report or result returned to us following the referrals;
- to the Practice's administrative staff for billing and other administrative tasks necessary to run our practice. Our staff are trained in the handling of personal information in accordance with the Practice Privacy Policy;
- to your health insurance fund, Medicare or other organisations responsible for the financial aspects of your care;
- where required by law, for example, pursuant to a subpoena;
- to insurers or lawyers for the defence of a medical claim; and/or
- to assist with training and education of other health care professionals
- when it is necessary to lessen or prevent a serious injury or 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
- when there is a statutory requirement to share certain information (eg. some diseases require mandatory notification)
- during the course of providing medical services, through eTP, My Health Record (via shared health summary)
- with third parties who work with South Coast Medical for business purposes, such as accreditation agencies or information technology providers (these third parties are required to comply with APP and this policy)

If you do not wish for your information to be used for training of health professionals please tick here: ☐

Our practice does not intend to disclose your personal information to anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

South Coast Medical will not use your personal information for marketing any of our services directly to you without your consent (by supplying your email address to accept our newsletter). If you do initially consent, you may opt out of South Coast Medical marketing at any time by notifying our practice in writing or by clicking unsubscribe on the newsletter.

Practice Patient Privacy Policy

How is your information used to improve service?

The practice may use your 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.

The practice may provide de-identified data to other organisations to improve population health outcomes. If we provide this information to other organisations patients cannot be identified from the information that is shared, the information is secure and is stored only within Australia. You can let reception know if you do not want your de-identified data included.

How are document automation technologies used?

Document automation is where systems use existing data to generate electronic documents relation to medical conditions and healthcare. The practice may use 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, Best Practice.
All users of Best Practice have their own unique user credentials are password and they can only access information that is relevant to their role in the practice team.

The practice complies with the Australian privacy legislation and APP's 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.

How are Artificial Intelligence (AI) Scribes used?

The practice uses an AI scribe tool to support GPs take notes during their consultations with you. The AI scribe uses an audio recording on your consultation to generate a clinical note for your health record. The practice AI scribe service is Lyrebird (Registrars may choose to use Heidi).

South Coast Medical will only use data from the digital scribe service to provide healthcare you.
Patients are provided with the opportunity to consent or to opt out of the use of AI scribe for their consultation.
With strict compliance to Australian regulation, Lyrebird Health is designed to prevent unauthorised access, uphold patient anonymity and securely dispose of sensitive data.

- Transcription is performed exclusively within Australia
- Audio file is immediately destroyed post-transcription
- Transcription is redacted of sensitive, personal identifying information received
- Post-redaction, the transcript is encrypted. It is not stored in original form
- Data is stored on an Australian server for 4 days prior to deletion
- Learn more about how Lyrebird Health is ensuring your privacy at https://www.lyrebirdhealth.com/patient

Practitioners and the facility will only use data from the digital scribe service to provide healthcare to you.

Information Quality

We aim to ensure the information we hold about you is accurate, complete, up to date and relevant. To this end our staff may ask you to confirm that your personal details are correct when you attend a consultation. Please let us know if any of the information we hold about you is incorrect or not up to date.

How do we store and protect your personal information?

The Practice takes all reasonable steps to protect the security of the personal information we hold, by:

- securing our premises;
- using passwords on all electronic systems and databases and varying access levels to protect electronic information from unauthorised interference, access, modification or disclosure; and
- storing hard copy records in secure filing cabinets or rooms that are accessible only to Practice staff.

Reasonable Steps to Secure Data

South Coast Medical takes all reasonable steps (as defined under the Privacy and Other Legislation Amendment Act 2024) to protect personal information. These include:

- Technical Measures: encryption, access controls, secure remote logins and vulnerability patching
- Organisational Measures: regular staff training on data protection, signed confidentiality agreements, clear internal data handling protocols, and third-party compliance audits

There is a strong culture of cybersecurity, including proactive assessments and a standing commitment to exceed industry best practice.

Criminalisation of Doxxing

We are committed to protecting your identity and personal information. Under new federal law, **doxxing**—the intentional publication of personal data to cause harm—is now a criminal offence. South Coast Medical enforces a zero-tolerance policy for any such misuse of information.

Data Breach Response Plan

We maintain a formal **Data Breach Response Plan** to ensure immediate and effective action in the event of a breach. The plan includes:

- Containment and investigation
- Notification to affected individuals and regulators (if required)
- A full review and improvement cycle

Staff receive regular training and simulations to remain prepared.

Your Rights Under Updated Privacy Law

As a patient, you have enhanced rights under the 2024 amendments to Australian privacy law:

- The right to **access** the personal information we hold about you
- The right to **request correction** of any inaccurate or outdated information
- The right to **transparency** in how your data is collected, used, and stored
- The right to pursue legal action for **serious invasion of privacy**, including misuse or unauthorised access

We are committed to upholding these rights in line with both the Privacy Act and the amended legislation.

How can you access and correct your personal information?

Under law you have a right to access personal information we hold about you. South Coast Medical acknowledges that patients may request access to their medical records. Please contact our Administration Team for more information on our Access to Medical Records Policy.

We ask that you put your request in writing. A fee for the retrieval and copying of your medical record will apply, charged in accordance with the schedule of fees specified in the Health Records Regulations 2008 (Vic), plus GST. This fee is not redeemable through Medicare. The practice will take all reasonable steps to provide information within 5 business days.

Our practice will take all reasonable steps to correct your information where the personal information is not accurate or up to date. From time to time, we will ask you to verify that your personal information held by South Coast Medical is current and accurate. You may request that the practice correct or update your information. To do this please contact jane@scmc.com.au

You can choose not to provide your information to us.

You are not obliged to give us your personal information. However, if you choose not to provide the Practice with the personal details requested, it may limit our ability to provide you with full service. We encourage you to discuss your concerns with our reception staff prior to your first consultation or with your doctor.

Dealing with unauthorised access or disclosure of your personal information

We take every care to ensure that our data security systems protect your electronic data. If we have reason to suspect that there may have been unauthorised access to or unauthorised disclosure of your health information which we are unable to rectify we will comply with the requirements of the Privacy Act to notify you and the Office of the Australian Information Commissioner.

Practice Patient Privacy Policy

How can you lodge a privacy related complaint and how will the complaint be handled?

We take your complaints and concerns regarding privacy seriously. If you have a complaint regarding the way your personal information has been handled by our Practice, please put it in writing and address it to the Administration Manager or the Practice Manager. We will acknowledge receipt of your complaint within 14 days, and endeavour to provide a full response within 30 days of receipt.

Should you be dissatisfied with our response, you may also contact the Office or 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.

If you have a query regarding our Practice's privacy policy, please contact the practice manager who will be happy to discuss the matter with you.

How is privacy on the website maintained?

At South Coast Medical, any personal information that you share with the practice through website, email and social media, is handled securely and confidentially. The practice uses analytics and cookies.

Policy Review

The South Coast Medical Practice Patient Privacy Policy is reviewed regularly to ensure it is in accordance with any changes that may occur to ensure compliance with current obligations. New versions of the policy will be available on the website and in clinic as they are updated.

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

PRIVACY CONSENT FORM

(to be read in conjunction with the Practice Privacy Policy)

I, _____ have read and understand the information (insert patient name)

Contained in the South Coast Medical Practice Privacy Policy, including:

- the types of personal information collected by the Practice, the reasons why it is necessary to collect it and the circumstances in which my personal information may be used or disclosed;
- that I may request access to my personal information, which may be granted in accordance with the Practice's Access to Personal Information Policy. I will be provided with a written reason if access is denied;
- that I may request an amendment to my personal information if it is incorrect. I will be provided with a written reason if a request for amendment is denied;
- that my personal information will not be used for direct marketing or disclosed to overseas recipients;
- that I am not obliged to provide the Practice with my personal information, but withholding information may limit the Practice's ability to provide me with full service.
- that I have the right to lodge a compliant about the handling of my personal information if I am dissatisfied, which will be dealt with in accordance with the Practice's complaint handling procedure.

Signed: _____

Patient or parent/guardian of patient

Date: _____

PERSONAL INFORMATION POLICY

Under the Privacy Act 1988 (Cth) and the Health Records Act 2001 (Vic), you have a legal right to access the personal information South Coast Medical (Practice) holds about you (such as your medical record), subject to some exceptions.

ACCESS FEES

The Practice is entitled to charge an appropriate fee, determined in accordance with the Health Records Regulations 2002 (Vic), plus GST, to cover the administrative costs of this service. Our reception will advise you of the applicable fee, which is not redeemable under Medicare or private health insurance.

HOW DO I REQUEST ACCESS TO PERSONAL INFORMATION?

Patients who wish to access or obtain a copy of their personal information should put their request in writing using the attached Request to Access Personal Information Form, and submit the form to our Practice reception. All requests will be acknowledged in writing within 14 days of receipt of the request.

Ordinarily, access to the requested information will be provided within 30 days.

HOW WILL ACCESS BE PROVIDED?

Access may be provided by:

- inspecting your medical record (or a print out of your record) at the Practice.; and/or
- providing a copy of the requested information in person or via secure email or post (additional fees for postage may apply); or
- providing an accurate summary of the information, instead of a copy, if you and the doctor agree that a summary is appropriate.

We recommend that you make an appointment with your doctor to view your medical record together, so the doctor can assist you to understand and interpret the material contained within it. A consultation fee will apply in addition to the administration fee, plus GST. The fee is not redeemable via Medicare or private health insurance.

CAN I AMEND MY MEDICAL RECORD?

You will not be permitted to remove any contents of your medical record from the Practice. Should you wish to amend or delete any personal information, you will need to fill out a separate written request using the Request to Amend Medical Record Form available from reception.

WHEN WILL ACCESS TO MY MEDICAL RECORD BE REFUSED?

Access to your personal information may be legitimately withheld in certain situations, including (among others):

- where access would pose a serious threat to the life, health or safety of any individual or the public;
- where access would cause unreasonable impact on the privacy of other individuals;
- where the request is frivolous or vexatious; or
- where the information is privileged as a result of actual or anticipated legal proceedings.

If access to your personal information is refused, the Practice will provide you with written reasons for the refusal. You will not be charged an access fee in this instance. If access is refused, you are welcome to contact the Practice to discuss means by which access may be facilitated.

If you have any queries regarding the above policy, please contact the Practice Manager who will be happy to discuss these with you.

Medical Record Access Information for Applicants

Under the Health Records Act 2001 (Vic) an individual may request access to medical records held by South Coast Medical. Medical records held by South Coast Medical may be requested using the attached request form.

Types of access

Access to a medical record can be requested for:

- A print out of the medical record (whole or partial)
- A digital copy of the medical record (whole or partial) via email

How to make a request

Complete the attached request form in full. The request must include the patient's full name and date of birth, along with copies of the proof of identification documents specified below.

Proof of identification required

Under the Health Records Act 2001 (Vic) we may require evidence of the identity of an applicant, and if the request is for another person's medical record, evidence of the applicant's authority to make the request. A completed request must include certified copies of the documents listed below.

Where requesting your own medical record

1. A copy of your Australian Drivers Licence or Australian Passport, OR two forms of identification (at least one of which is photographic identification).

Where requesting the medical record of another person

1. A copy of the applicant's Australian Drivers Licence or Australian Passport, OR two forms of identification (at least one of which is photographic identification), and
2. A copy of evidence that the applicant is the authorised representative of the patient (eg Guardianship Order, Medical Enduring Power of Attorney, child's Birth Certificate).

Where requesting the medical record of a deceased person

1. A certified photocopy of the applicant's Australian Drivers Licence or Australian Passport, OR two forms of identification (at least one of which is photographic identification), and
2. A certified photocopy of evidence that the applicant is the legal representative of the deceased in the form of the Grant of Probate or Letters of Administration.

Fees for accessing medical records

You do not need to send payment with your request form. You will be notified of the fees for accessing medical records by invoice when your request is processed. The following fees are in accordance with the regulations under the Health Records Regulations 2001 (Vic), and attract GST
Under the Health Records Regulations Act (Vic), medical records must be kept for 7 years for an adult and until the age of 25 years if the patient attended as a child

Where a copy is requested:

Black and white A4 $0.20 per page*
Email $0.20 per page*
*An additional administration/collation fee will be applied
Registered Post: Actual Postage Cost

How long will it take?

Under the Health Records Act 2001 (Vic) we have a maximum of 45 days to respond to your request. We will do our best to do it as soon as possible.

How do I pay my invoice?

Your invoice will include payment instructions. Payment methods available are credit card and bank deposit.

Further questions If you have any questions about accessing medical records, please contact the Practice Manager on:

Phone: 03 5985 7776

This completed request form may be returned to the Practice Manager by:

Mail:
South Coast Medical
PO Box 465, Rosebud Vic 3939

Email:
jane@scmc.com.au

Fax:
(03) 59857819

APPLICATION CHECKLIST

- Fully completed request form
- Attached a copy of the applicant's photo ID
- Attached a certified copy of proof of your capacity to make this request on the patient's behalf (if applicable)

DO NOT SEND PAYMENT WITH THIS FORM. AN INVOICE WILL BE MAILED TO YOU.

Medical Record Access
Request Form

1. *Patient details*

Surname

Previous surname (if applicable)

Given name(s)

Date of birth

Year of Last Attendance at South Coast Medical

2. *Are you applying to access your own medical record?*

☐ No, go to next question Yes,

☐ go to 4

3. *Applicant details (if not the patient)*

Surname

Given name(s)

What is your relationship to the patient?

You must attach a copy of the specified proof of your capacity to make this request on the patient's behalf.

☐ Executor : *Attach Grant of Probate or Letters of Administration*

☐ Guardian or Administrator: *Attach Order*

☐ Medical Enduring Power of Attorney: *Attach Power of Attorney*

☐ Parent: *Attach child's Birth Certificate*

☐ Other capacity (please specify)

* Please be aware that if your child is over 18 years of age or deemed mature minded, they will be required to make their own request.

4. *Applicant photographic identification*

You must attach a certified copy of one category of identification below for your application to be processed.

- Current Australian Drivers Licence or
- Current Australian Passport or
- Two forms of identification
  including at least one form of photographic identification

Office Use Only - to be completed by the practice

I confirm I have sited original or certified identification from the requester (please tick)

☐ • Current Australian Drivers Licence/Passport or

☐ • Two forms of identification (including at least one form of photographic identification)

Name:_____ Signature:_____

Date: _____

6. *Applicant contact details*

Postal address (for delivery of medical record)

Home phone number

Mobile phone number

Email address

7. *Document access requested*

- Complete medical record Go to 8
- Partial access

Describe clearly the dates, admissions and/or documents required:

Medical Record Access
Request Form

8. Type of access required
Tick all that apply

☐ Hard copy of the medical record (entire)

☐ Digital copy via email

9. Reason for request

10. Acknowledgement of fee

I acknowledge that there is a fee involved in providing the requested information and that payment is required on or prior to collection. An invoice for access to the medical record will be forwarded and I agree to be responsible for payment of the associated fee. I understand I will not be permitted to make changes to my medical record.

Applicant signature

Print full name

Date

Collection of files (to be signed on collection)

I acknowledge that I have collected the requested information and that I take responsibility for ongoing privacy and access to the information provided.

Applicant signature

Print full name

Date

Office Use Only - to be completed by practitioner

Signature of practitioner authorising access to patient's medical record

Practitioner signature

Practitioner full name

Date

Office Use Only - to be completed by practice staff

Signature of practice staff authorised to prepare and collate patient's medical record

Practice staff signature

Practice staff full name

Date

AMEND MEDICAL RECORDS FORM

I, _____

insert patient name

of _____

address

request to amend my medical record held by South Coast Medical (Practice) as described in Table A, below.

I understand the Practice has the right to request me to attend a consultation with my doctor to discuss my medical record. I have been advised of the applicable fees for this service and that the fee will not be redeemable via Medicare.

I understand that the Practice has the right to refuse my request if the Practice is satisfied that the information contained in my medical record is not incomplete, incorrect, irrelevant, out of date or misleading, or if the requested amendment contains information that is incorrect or misleading. The reasons for any refusal will be provided to me by the Practice in writing.

If I am dissatisfied with the way my personal information has been handled, I may lodge a complaint addressed to the Practice Manager which will be dealt with according to the Practice's compliant handling process.

Signed: _____

Patient or parent/guardian of patient

Date: _____

LETTER ACKNOWLEDGING RECEIPT OF REQUEST FOR ACCESS TO MEDICAL RECORDS

South Coast Medical

Po Box 465, Rosebud VIC 3939

Ph: (03) 5985 7776

[DATE]

Dear [INSERT NAME OF PATIENT],

Thank you for submitting your request to access personal information held by South Coast Medical, dated [INSERT DATE OF REQUEST].

We received your request on [INSERT DATE REQUEST RECIEVED]. We will contact you shortly to discuss how access may be provided and to inform you of the applicable fee, which will be charged in accordance the Health Records Regulations 2002 (Vic). Normally, access will be provided within 30 days of receipt of request.

If we are not able to provide you with access to your record, we will provide you with the reasons for refusal in writing. No fee will apply in this circumstance.

If you have any queries, please contact the Practice Manager who will be happy to discuss these with you.

Yours sincerely,

Simone Clark

South Coast Medical

SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES (APPS)

APP 1 OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

The practice must have an up to date and available privacy policy that covers specified information. The privacy policy must be made available to patients free of charge.

APP 2 ANONYMITY AND PSEUDONYMITY

Individuals must have the option of not identifying themselves, or using a pseudonym, unless impracticable or unlawful.

APP 3 COLLECTION OF SOLICITED INFORMATION

Sensitive information (including health information) must only be collected:

- with consent from the individual (or authorised guardian); and
- where reasonably necessary for the functions and activities of the practice (that is, the provision of health services).

Information should only be collected from the patient unless it is impracticable to do so.

Example: Information about a patient's family member is collected while taking a history. This is acceptable if the information is reasonably necessary to treat the patient.

APP 4 DEALING WITH UNSOLICITED INFORMATION

Where an entity receives personal information it did not solicit, it must determine whether the information could have been collected under APP 3. If not, the information must be de-identified or destroyed.

APP 5 NOTIFICATION OF COLLECTION OF PERSONAL INFORMATION

Individuals must be made aware of the nature of the personal information the practice collects.

This includes information on:

- accessing and amending medical records
- how to make a complaint
- whether information will be used for direct marketing or disclosed to overseas recipients.

The practice's privacy and patient consent documents should cover these points.

SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES (APPS)

APP 6 USE AND DISCLOSURE OF PERSONAL INFORMATION

Information collected by the practice must only be used for a primary purpose or a secondary purpose directly related to the primary purpose, and only where the patient has provided consent to the use or disclosure.

A ‘primary purpose’ is the reason the information was collected (for example, for the provision of health care)

A ‘secondary purpose’ is a purpose ancillary but closely related to the primary purpose. For example, using patient details for billing purposes, or disclosing patient details to a specialist for referral.

Disclosure may also be required by law, including where there is a:

- warrant from Police to access medical records
- subpoena to produce document or give evidence
- obligation of mandatory notification of child abuse or notifiable disease.

Use or disclosure for a secondary purpose is also lawful in ‘permitted general situations’, without consent of the patient. These most relevant of these include:

- where necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public and it is unreasonable/impracticable to obtain the patient’s consent. The threat need not be ‘imminent’ but it must be ‘serious’.
- in instances of suspected or actual unlawful activity or serious misconduct that relates to the practice’s functions and use or disclosure is necessary to take appropriate action.
- to locate a missing person – if the practice has a reasonable belief that the use or disclosure of personal information is reasonably necessary to locate a missing person. Example: medical records indicate a 17 yr old male who has been reported missing was proposing to travel interstate to meet a girl he met on facebook.
- to defend or establish a legal or equitable claim.
- to lawyers or insurers in response to complaints or claims.
- for confidential mediation/ADR processes – practices have the right to use or disclose patient information during a confidential alternative dispute resolution process such as mediation.

SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES (APPS)

There are 3 ‘permitted health situations’ where a practice can use or disclose health or genetic information for a ‘secondary purpose’. These are:

- Research- if relevant to public health or safety and it is impracticable to obtain a patient’s consent. The research must be conducted in accordance with research guidelines and the practice must reasonably believe that the information will not be further disclosed by the recipient.
- Prevention of a serious threat to the life, safety or health of a genetic relative. Example: a female daughter may request access to her mother and grandmother’s medical records to determine the nature of their disease.
- Responsible person/Guardian – where a patient is either physically or mentally incapable of giving consent, a practice may disclose information to a responsible person or guardian where the disclosure is necessary to provide appropriate care or treatment to the patient or for ‘compassionate reasons’. The disclosure must not be contrary to the wishes of the patient and limited to the extent necessary for care or compassion.

APP 7 DIRECT MARKETING

The practice must not use personal information for direct marketing unless the individual has given specific consent for this to occur.

Direct marketing involves the use of personal information to communicate with an individual to promote goods and services.

Example: sending patients an SMS offering discounted services at the practice is direct marketing and not permitted. Direct marketing is permitted where an individual would have a reasonable expectation that this would occur and they can easily ‘opt out’.

APP 8 CROSS BORDER DISCLOSURE OF PERSONAL INFORMATION

If the practice is going to send personal information overseas, it must take reasonable steps to ensure the overseas recipient will not breach the APPs. There are exceptions where the overseas recipient has a similar enforceable law in place or the patient has consented after being expressly informed that information will be sent overseas.

Example: having a contract with an overseas cloud service provider that requires compliance with APPs.

SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES (APPS)

APP 9 USE OF GOVERNMENT IDENTIFIERS

- The practice must not adopt, use of disclose a government related identifier unless:
- the adoption, use or disclosure is required or authorised by law
- it is reasonably necessary to verify the identify of the individual.
- It is reasonably necessary to fulfil the obligations to a Commonwealth agency or state or territory authority;
- The practice believes it is reasonably necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public;
- The practice reasonably believes use or disclosure is necessary to take action in relation to suspected unlawful activity or misconduct of a serious nature
- The practice reasonably believes use or disclosure is necessary for enforcement related activities of an enforcement body.

A government related identifier includes a Medicare number, Centerlink reference number, driver's licence or passport number.

Example: the practice is not permitted to use Medicare numbers as the basis for patient identification. However, a practice can view and record Medicare numbers to verify the identification of a patient and for billing purposes.

APP 10 QUALITY OF PERSONAL INFORMATION

Practices must take reasonable steps to ensure the personal information it collects uses or discloses is accurate, up to date complete and relevant.

APP 11 SECURITY OF PERSONAL INFORMATION

Practices must take reasonable steps to protect the personal information it holds from misuse, interference, loss, unauthorised access, modification or disclosure.

Example: Practices should issue staff with passwords to access patient databases that are changed on a regular basis, and store hard copy files in lockable filing cabinets or rooms, accessible only to authorised practice staff.

SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES (APPS)

APP 12 ACCESS TO PERSONAL INFORMATION

The practice must, on request, provide a patient with access to their personal information within a reasonable time, unless an exception applies (see APP 6 above).

The practice is entitled to charge a 'reasonable' fee for access under the Privacy Act 1988 (Cth). The Victorian Health Records Act 2001 (Vic) sets specified fees for access to medical records. Further information on these fees can be obtained from AMA Victoria.

Any refusal must be accompanied by written reasons and information on how the patient may lodge a complaint.

APP 13 CORRECTION OF PERSONAL INFORMATION

A practice must take reasonable steps to ensure the personal information it holds is up to date, accurate, complete, relevant and not misleading. There is a positive obligation on practices to correct information where it is wrong.

The practice must acknowledge a request for an amendment to their medical records, within a reasonable time. No charge can be made for the practice making the requested changes.

Example: Reception staff should confirm the contact details of the patient are up to date when they present for an appointment.

HEALTH RECORDS ACT 2008 (VIC) OBLIGATIONS

In addition to the obligations imposed by the APPs under the Privacy Act 1988 (Cth), the Health Records Act 2008 (Vic) imposes 11 Health Privacy Principles (HPPs) which apply specifically to the collection, use, disclosure and handling of health information in Victoria.

The HPPs are substantially the same as the APPs and so it is not required to set them out separately. There are, however, two added obligations imposed by the HPPs that are not included in the APPs. These are:

HPP 10 – a practice must provide a patient with information about their medical record if the practice is transferred, sold or closed.

HPP 11 – a practice is required to transfer a patient's health information to another health service provider upon request from the patient.

MANDATORY DATA BREACH NOTIFICATION REQUIREMENTS

Part IIIC of the Privacy Act 1988 (Cth) (the Act) requires health service providers including medical practices to notify the Office of the Australian Information Commissioner (the OAIC) and affected individuals when an eligible data breach occurs, ie, when you suspect that a data breach has occurred and there is a real risk of serious harm to individuals as a result of the breach.

ELIGIBLE DATA BREACH

An eligible data breach occurs when:

- there is unauthorised access to, or unauthorised disclosure of, information in circumstances where a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
- information is lost and unauthorised access to, or unauthorised disclosure of, information is likely to occur, and assuming unauthorised access or disclosure of the information will occur, the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates.

Breaches may occur through data theft, hacking or by accidental loss or disclosure of information through internal errors or failure to follow policies.

SERIOUS HARM

If a reasonable person would conclude that the data breach is likely to result in serious harm, it is an eligible breach. “Serious harm” is not defined, but the Explanatory Memorandum indicates that it could include serious physical, psychological, emotional, economic and financial harm, or serious harm to reputation.

Serious harm will be “likely” if such harm is more probable that not, having regard to a number of factors set out in the Act, including the kinds of information accessed / disclosed / lost, the sensitivity of the information, whether the information is protected by security measures, the person(s) or kinds of persons who obtained or could obtain the information and the nature of the harm that may result.

SUSPECTED ELIGIBLE DATA BREACH

If a provider has reasonable grounds to suspect an eligible data breach may have occurred but cannot confirm this is so at the time, the provider has 30 days to carry out a reasonable and expeditious assessment as to whether there are reasonable grounds to believe that the circumstances amount to an eligible data breach.

MANDATORY DATA BREACH NOTIFICATION REQUIREMENTS

NOTIFICATION

If a provider has reasonable grounds to believe there has been an eligible data breach, the provider must prepare a statement setting out:

- the identity and contact details of the provider;
- a description of the data breach that the provider has reasonable grounds to believe has occurred;
- the kinds of information concerned; and
- recommendations about the steps which individuals should take in response to the data breach.

The statement must be provided to the OAIC and, if practicable, the provider must also notify the individuals to whom the information relates, or each of the individuals who are at risk as a consequence of the data breach, of the contents of the statement.

If it is not practicable to contact the individuals, the provider must take reasonable steps to publicise the contents of the statement and must publish a copy on its website (if it has one).

EXCEPTIONS

A mandatory notification is not required to be made if the breach is required to be, and is, reported pursuant to the My Health Records Act 2012.

A mandatory notification is not required to be made if effective remedial action is taken before any serious harm is caused by the breach.

Policies Approved 22 April 2025

Simone Clark

Practice Manager

Neil Stitt

Director

Page left blank.