RACGP

Royal Australian College *of* General Practitioners

Privacy and managing health information in general practice

racgp.org.au

Healthy Profession.
Healthy Australia.

Privacy and managing health information in general practice

Disclaimer

The information set out in this publication is current at the date of first publication and is intended for use as a guide of a general nature only and may or may not be relevant to particular patients or circumstances. Nor is this publication exhaustive of the subject matter. Persons implementing any recommendations contained in this publication must exercise their own independent skill or judgement or seek appropriate professional advice relevant to their own particular circumstances when so doing. Compliance with any recommendations cannot of itself guarantee discharge of the duty of care owed to patients and others coming into contact with the health professional and the premises from which the health professional operates.

Accordingly, The Royal Australian College of General Practitioners (RACGP) and its employees and agents shall have no liability (including without limitation liability by reason of negligence) to any users of the information contained in this publication for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of any person using or relying on the information contained in this publication and whether caused by reason of any error, negligent act, omission or misrepresentation in the information.

Recommended citation

The Royal Australian College of General Practitioners. Privacy and managing health information in general practice. East Melbourne, Vic: RACGP, 2017.

The Royal Australian College of General Practitioners
100 Wellington Parade
East Melbourne, Victoria 3002

Tel 03 8699 0414
Fax 03 8699 0400

www.racgp.org.au

ABN 34 000 223 807
ISBN 978-0-86906-468-9 (web)

Published May 2017

We recognise the traditional custodians of the land and sea on which we work and live.

RACGP

Royal Australian College *of* General Practitioners

Privacy and managing health information in general practice

Foreword

General practice has a fundamental role in ensuring the privacy of patient health information. It is important general practices have up-to-date information on the current legislative framework for the management of health information.

Addressing this need, and as part of its ongoing member focus, The Royal Australian College of General Practitioners (RACGP) has published *Privacy and managing health information in general practice*.

This resource aligns with current best practice and examines the *Privacy Act 1988* incorporating 13 Australian Privacy Principles (APPs), and the relevant health records legislation.

Privacy and managing health information in general practice provides guidance and examples for compliance with each APP within the general practice setting.

However, privacy reflects only one aspect of the management of health information. Complementing this are important and complex notions of general patient consent, the existence of medical records, patient rights and information used in medical research.

All RACGP privacy resources are available at www.racgp.org.au/ehealth/privacy

Contents

1. Key concepts

1.1 Glossary

Australian Privacy Commissioner

The Australian Privacy Commissioner is the national regulator of privacy, conferred by the *Privacy Act 1988* (Privacy Act) and other laws. The Australian Privacy Commissioner holds position within the Office of the Australian Information Commissioner (OAIC).

Australian Privacy Principles

The Australian Privacy Principles (APPs) provide a consolidated and universal set of principle-based laws, focusing on transparency in the following five areas:

- Consideration of personal information (APPs 1 and 2)
- Collection of personal information (APPs 3, 4 and 5)
- Dealing with personal information (APPs 6, 7, 8 and 9)
- Integrity of personal information (APPs 10 and 11)
- Access to and correction of personal information (APPs 12 and 13)

Confidentiality

The National Health and Medical Research Council (NHMRC) defines 'confidentiality' as 'the obligation of people not to use private information – whether private because of its content or the context of its communication – for any purpose other than that for which it was given to them.'[1]

Generally, confidentiality refers to a set of obligations imposed through law or ethics. A patient discloses confidential information to their general practitioner (GP) on the understanding the information will only be used within the practitioner–patient relationship.

Consent

Refer to Section 1.3. Patient consent.

De-identified health information

Health information is de-identified if it is 'no longer about an identifiable individual or an individual who is reasonably identifiable'.[2] Care should be taken to ensure no re-identification can occur. If health information is de-identified it falls outside of the privacy legislation.

Health information

Health information includes information or opinions about the health or disability of an individual and a patient's wishes about future healthcare. It also includes information collected in connection with the provision of a health service (and therefore includes personal details such as names and addresses).[2]

Health information is regarded as one of the most sensitive types of personal information. For this reason, the Privacy Act provides extra protections for the way health information is handled.

Held

A GP or general practice 'holds' health information if they have possession or control of the relevant medical record.

Personal information

The Privacy Act defines personal information as 'information or opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable'.[2] Personal information includes an individual's name and address, signature, contact details, birth date, medical records and bank account details.

It does not matter whether the information is true. Personal information can be held in any media. General practice may record personal information on paper and in electronic records, X-rays, CT scans, videos, photos and audio recordings. Personal information may be collected by a GP directly from the patient or from a third party in the course of providing a healthcare service.

Practice

In this resource, the term 'practice' refers only to general practices that operate as a single functional unit for the purposes of patient care, practice management and accreditation, and not to groupings of individual GPs.

Use and disclosure

Neither 'use' nor 'disclosure' are defined terms. Generally, the distinction between use and disclosure refers to whether third parties are involved.

For example, a practice will 'use' health information when it holds and manages that information internally, such as for clinical or business practices. A GP will also use health information during a consultation.

A practice 'discloses' health information if it makes it accessible to persons, agencies or companies 'outside the entity and releases the subsequent handling of the personal information from its effective control'.[3] A GP may disclose health information if they discuss a patient's conditions with other practitioners.

1.2 Privacy legislation

Most aspects of information management in general practice will have privacy implications. This section aims to provide an awareness of the sources of privacy laws that GPs are most likely to be exposed to.

1.2.1 The Privacy Act

The Privacy Act regulates how most personal information is managed. It includes 13 APPs.

The Privacy Act applies to private sector organisations, as well as most government agencies, unless an exception applies. General practice is subject to stringent privacy obligations by virtue of handling health information.

Individuals found liable of privacy infringements can face penalties of up to $340,000 and corporations up to $1,700,000.

1.2.2 Health records legislation

Victoria, New South Wales and the Australian Capital Territory have their own health records legislation[4–6] regulating the handling of health information, as detailed in sets of principles.

Such principles operate concurrently to the Privacy Act but are broadly consistent with the APPs. Their respective definitions of personal information and health information are also broadly similar.

However, the state and territory health records legislation may impose additional requirements in certain situations (for example, refer to Section 3.2. Sale or closure of a practice), and care should be taken to ensure compliance with both sets of laws where necessary.

1.2.3 Doctor–patient confidentiality

The Medical Board of Australia in its *Good medical practice: A code of conduct for doctors in Australia* states 'a good doctor–patient partnership requires high standards of professional conduct'.[7] Among other principles, this involves 'protecting patients' privacy and right to confidentiality, unless release of information is required by law or by public-interest considerations'.[7]

According to this code of conduct, 'patients have a right to expect that doctors and their staff will hold information about them in confidence, unless release of information is required by law or public interest considerations'.[7]

1.2.4 Professional advice

This resource provides a high-level understanding of the regulatory and best practice framework for the management of information (personal information, sensitive information and health information) in a general practice setting.

It is not tailored to any particular practice environment and the material is not exhaustive. The RACGP strongly recommends appropriate legal or professional advice is sought prior to reliance on its contents, or when integrating the content into practice procedures.

1.3 Patient consent

Patients have the ethical and legal right to make informed decisions about their health. Informed consent forms the basis for many Privacy Act exceptions, permitting collection, use and disclosure.

Obtaining a patient's informed consent should be the key guiding principle for GPs. Many medico-legal proceedings result from a failure to obtain such consent.

The requirement to obtain informed consent also applies to research undertaken by a practice.[1]

1.3.1 Informed consent

To provide informed consent, patients must have sufficient information about their own healthcare, and the ability to then make appropriate decisions.

The information required is context dependent. In relation to health information, it may include details of the scope of use and disclosure (if any), any benefits and risks, or referral or treatment needs. Patients should also be informed if it is likely their information will be sent outside of Australia and if so, to where.

GPs should be cognisant of local competency when determining whether patients are capable of giving informed consent (refer to Section 1.3.4. Competence, capacity and maturity to provide consent).

1.3.2 Inferred or express consent

A verbal or written consent may be:

- express – when a patient signs or clearly articulates their agreement
- inferred (or 'implied') – where the circumstances are such to reasonably infer the patient has consented.

Express consent should be sought wherever practical and/or where significant clinical risk is likely, for example, for a procedure or surgery. A signed form is an example (and is easier to demonstrate), but an informative and well-documented discussion with a patient may equally satisfy this requirement.

Inferred consent should be relied on only when express consent cannot be reasonably obtained. If so, care must be taken not to overestimate the scope of that consent.

For example, it is reasonable to infer that patients consent to their health records being collected and used during repeat consultations. However, this consent would not necessarily extend to the disclosure of that information to third parties, such as including health summaries within referral letters. GPs should be wary of taking silence or a lack of objection as an indicator of consent; if there is any doubt, GPs should obtain express consent.

It is recommended that consent conversations are thoroughly documented. Problems may arise if a patient does not understand the potential uses of their health information. In circumstances where GPs must establish implied consent, comprehensive and concurrent consultation notes are extremely valuable. Notes should refer to the information provided, the nature of the discussion and the patient's response.

1.3.3 Withheld consent

GPs should be careful when treating patients who refuse to provide certain health information or withhold consent for particular healthcare.

This is particularly problematic where the possibility of detrimental outcomes exists if certain information is not collected or used. This should be clearly explained to the patient.

In such circumstances, it is recommended GPs make detailed notes to document the discussion, the patient's decision and the ultimate outcome. In certain circumstances this outcome may conflict with the GP's underlying duty of care, and comprehensive consultation notes will be valuable.

1.3.4 Competence, capacity and maturity to provide consent

Some patients may not be competent to provide adequate consent.

Various state and territory guardianship legislation documents provide a framework for obtaining substitute consent on behalf of patients who are incompetent because of age, illness or disability. GPs are advised to seek appropriate advice if these situations arise.

Age-related consent is dealt with at the state and territory level. As a general rule, if a child is sufficiently mature to understand what will happen to their information they will have capacity to consent.

New South Wales, South Australia and the Australian Capital Territory have legislation stipulating the age at which a child can provide valid consent. In SA, the age is 16 years or over; in NSW, the age is 14 years or over. The ACT requires a parent or guardian to consent for a child under the age of 18 years, unless the health practitioner assesses the child to have sufficient maturity and adequate understanding.

In Victoria, consideration should be given to the *Medical Treatment Planning and Decisions Act 2016* and specifically to the concept of decision-making capacity.

The Privacy Act does not stipulate age; its guidelines assume people over the age of 15 have the 'capacity' to give informed consent.[2] GPs must therefore assess the capacity and maturity of each child to understand and make informed decisions on a case-by-case basis.

In unclear cases, GPs are entitled to request the patient presents corroborating consent from their parent or guardian.

2. Information management relating to patients

2.1 Collection of health information

Key points

- Your practice should not collect health information unless the patient consents and the information is reasonably necessary for delivery of healthcare services.
- Your practice must collect personal information only by lawful and fair means (without being unreasonably intrusive or using methods of intimidation).
- Consent is not required where:
  - the health information is collected in accordance with the law or rules established by 'competent health or medical bodies'[8]
  - it is unreasonable to seek it and the collection is necessary to 'lessen or prevent a serious threat to life, health or safety' of an individual or the public.[8]

  Other exceptions also apply.
- Unsolicited information (received without asking) must be destroyed unless your practice would ordinarily have lawfully collected that information.

Prior to making an informed decision about whether to provide health information, your practice's patients should be notified about how their information may be used or disclosed, and what rights of access will apply.

In the context of a general practice, it may be reasonable to consider an attending and willing patient as consenting unless their consent is expressly revoked. If there is any doubt, it is best to obtain the patient's express consent (by a signed admittance form, for example).

When a patient first attends their consulting GP, it is suitable to take a full patient medical history where clinically appropriate.

2.1.1 Health information from third parties

While GPs obtain most health information directly from the patient (and should do so wherever practical), they will receive some health information from third parties, such as guardians or other health professionals involved in the patient's care.

Where personal information is received without the GP soliciting it, GPs should determine whether or not they could have ordinarily collected the information. If not, the information should be destroyed or de-identified.

In many situations, such as where GPs collect a family medical history from a patient, it may not be possible to obtain each family member's consent. GPs can collect a patient's family, social or medical health information when necessary to provide them with healthcare services, however will need to be careful during any disclosure of that material (refer to Section 2.6.4. Refusing access).[2]

2.2 Notification

2.2.1 Notification obligations

Key points

- Upon collecting health information, or as soon as possible afterwards, GPs must take reasonable steps to notify the patient of such collection.
- Notified information must include the practice's details, the purpose for which the information is collected, to whom the health information may be disclosed, and whether it will be disclosed to an overseas recipient (and if so, where).

Patients need to be made aware of the potential use and disclosure of their health information. Extensive prescribed notification requirements apply to the collection of health information.

It is not necessary to notify your practice's patients if their health information is being collected during recurring consultations, as it is clearly apparent. It is not necessary to notify patients if their health information will need to be disclosed when referring to a specialist.

However, there are various aspects of collection that are not so straightforward. For example, the organisation ultimately collecting and holding the information may not be obvious, particularly in incorporated practices with sophisticated administration and complex corporate structures.

For those items that are prescribed but not obvious or covered during a consultation, more formal notification requirements will be needed.

The notification requirements have administrative implications for incorporated practices, practices with operating services trusts and practices using cloud computing (refer to Section 2.3.8. Information transferred overseas).

It is recommended practices ensure their patient information/consent forms are updated to account for this prescribed notification. Where necessary, your practice should secure renewed consent from its patients.

2.2.2 Privacy notices

Your practice should consider whether a privacy notice (also known as a 'collection notice' or 'APP 5 Notice') addressing the prescribed notification matters in a predetermined format and medium would be an appropriate medium for notifying your patients.

Such notices may include information about:

- disclosure within a multidisciplinary medical team
- disclosure to colleagues as part of case management
- use and disclosure in medical research
- disclosure for practitioner continuing professional development purposes or for quality improvement activities
- the process for disclosure to other specialists.

The practice can always choose whether to provide additional information about how a patient's health information may be used. This will assist in managing the patient's expectations, promoting trust as well as increasing the likelihood that further uses of that patient's health information will constitute secondary use (refer to Section 2.3. Use and disclosure of health information).

It is recommended to use practice information notices for this purpose. This information may also be considered for inclusion in your general practice's collection notice (refer to Section 2.2. Notification), and incorporated into your practice's privacy policy (for more information on privacy policies, refer to Section 2.4. Privacy policies).

When used appropriately, these notices will assist patients to understand how their health information is used and disclosed.

Your practice can customise the RACGP *Patient privacy pamphlet* which is available to download here: http://www.racgp.org.au/ehealth/privacy

2.3 Use and disclosure of health information

2.3.1 Use for primary and secondary purposes

Key points

- A GP's primary purpose for collecting health information is to provide healthcare services.
- Your practice may use and disclose health information for that 'primary' purpose.
- Health information may be used or disclosed for another 'secondary' purpose where:
  - the patient consents
  - the patient would reasonably expect a use or disclosure related to their healthcare
  - it is unreasonable to seek consent and the collection is necessary to lessen or prevent a serious threat to life, health or safety of an individual or the public
  - a reasonable belief exists that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual
  - the patient is physically or legally incapable of giving consent, and the health information is disclosed to a responsible person (which may include parents, adult siblings, spouses, adult relatives, guardians or attorneys granted power concerning health decisions), for compassionate reasons or to enable appropriate care or treatment of the patient.
- A practice may use or disclose health information as required or authorised by or under law.
- Practices are responsible for information disclosed overseas.

When dealing with health information, your practice must determine whether the intended use or disclosure is for a primary purpose (the purpose for collection) or a secondary purpose (which must be directly related).

Health information is usually collected for providing particular healthcare services (this is the primary purpose). Your practice can use or disclose health information for the primary purpose.

In certain circumstances, your practice can choose to use health information for another 'secondary' purpose if the patient consents, or the patient would reasonably expect that use or disclosure, which is directly related to their healthcare.

Where there is doubt as to patient expectations, consent should be sought. It is often much simpler to gain a patient's consent than to balance their belief of reasonable expectations, or justify it if investigated.

A practice relying on 'reasonable expectations' must consider these expectations from the perspective of an average patient with no particular medical knowledge. The patient's age, cultural background and medical history should be considered. Whether the intended use or disclosure was ever notified to the patient is also relevant.

2.3.2 Use or disclosure in the practice setting

In the practice setting, patients will generally expect their health information to be used for a wide variety of activities that are directly related to the healthcare services they have received.

These may include:

- providing information about treatments
- being treated by a person other than their treating GP, such as a specialist or during admission to hospital
- internal assessment practices, such as to assess the feasibility of particular treatments
- management, funding, complaint-handling, planning, evaluation and accreditation activities
- disclosure to experts or lawyers (for legal opinions), insurers or medical defence organisations to report adverse incidents or for the defence of legal proceedings
- disclosure to clinical supervisors.[9]

Some practices may use or disclose health information for medical research or for quality assessment or clinical audit activities. As these are not uniformly expected by patients, practices should limit their use or disclosure except where consent is obtained. In any event, consent is often a key component to human clinical trial ethical approval (for more information, refer to Section 3.8. Health research).

Case study 1: Primary and directly-related purposes

Laura has been seeing her treating GP for many years. Recently she suffered a stroke, and now suffers from stroke complications, some of which are likely to be permanent.

Laura's healthcare will need a coordinated effort between her treating healthcare professionals, including her neurologist, rehabilitation team and practice nurse.

In her currently distressed state, Laura may not expect her GP to organise this multidisciplinary team. Accordingly, her GP organises a consultation with Laura to discuss the benefits of multidisciplinary care, so that she can make an informed decision to allow disclosure of her health information to other health practitioners. Laura's treating GP carefully notes the conversation and Laura's express consent.

Laura's GP has recognised that the primary purpose for using Laura's health information is for the GP to treat and manage her stroke symptoms. Laura would expect this use as part of her regular healthcare.

However, it is unclear whether Laura would expect her health information to be disclosed to other health practitioners. This disclosure by Laura's GP may be considered a secondary purpose. Under the Privacy Act, the disclosure of the information necessary to treat and manage Laura's stroke recovery is ordinarily prohibited, unless an exception applies; in this case the two most applicable exceptions are consent and reasonable expectations.

It was therefore prudent for Laura's GP to seek Laura's consent. Additionally, by discussing the care plan and the scope of involvement of the multidisciplinary team, Laura's GP has managed her reasonable expectations regarding the use of her health information by the members of her team. This will allow greater flexibility in treating Laura and it is probably reasonable to not require Laura's consent to each exchange.

2.3.3 Use for business practices

It is reasonably expected for your practice to use health information for a secondary purpose relating to the general practice business.

For more information, refer to Chapter 3. Information management relating to general practice, and specifically Section 3.1. The business of general practice.

2.3.4 Use for training and education purposes

Patients are often not aware that their health information may be used for GPs' training and education purposes.

Without consent, it may be unreasonable for GPs to expect patients to permit their health information to be used in such circumstances. However, this expectation may be influenced by the nature of the training activity. For example, filming a family therapy session is highly likely to require express consent. In contrast, GPs are more likely to rely on implied consent for activities more closely linked to the provision of healthcare services, such as reflective discussion with peers or for training registrars.

In the absence of consent, health information should be de-identified before it is used for training or educational purposes, or quality assurance or audit exercises.

GPs should consider whether to include consent for training and education purposes on their patient registration forms to avoid this becoming an issue.

Your practice is encouraged to include information about these activities and clinical audits in your practice policy on managing health information. If a practice intends to use de-identified information, it is still worth notifying patients of this in your privacy notice.

2.3.5 Limiting disclosure

Where health information must be disclosed to a third party, your practice must consider what information is relevant for the proposed purpose. Patients will reasonably expect the disclosure of only the necessary subset of their health information, along with third-party access restrictions.

For example, a referring GP may not be justified in forwarding a copy of a patient's complete medical record or other health information to another medical practitioner if that health information does not relate to the condition for which the referral is being made.

Prior to disclosing any health information, your practice should carefully examine its authority for disclosure and seek advice where necessary (refer to Section 2.3.6. Subpoenas and disclosure required by law).

For further information, refer to the RACGP's resources on managing the use of your practice data, available at www.racgp.org.au/your-practice/ehealth/data

Case study 2: Limiting disclosure

Laura has commenced her stroke rehabilitation. Her treatment is being led by her GP, who is coordinating a multidisciplinary healthcare team consisting of a neurologist, rehabilitation team and practice nurse.

Laura visits her neurologist on a regular basis. The consultation recommendations are provided to Laura's GP, who then passes them onto the other healthcare professionals.

Laura discloses to her neurologist that she has been having difficulty controlling her emotions, including suffering from depression. Her GP is advised and discusses Laura's depression with her, and prescribes medication as appropriate.

When Laura visits her treating physiotherapist, he talks to Laura about her depression. Laura is surprised and embarrassed by this. She did not expect her physiotherapist to receive information disclosed to her neurologist.

It is reasonable to expect that Laura consented to her GP disclosing those aspects of her health relevant to each treating team member. However, Laura's GP did not contemplate that she was unlikely to consent to unrelated disclosures, in this instance, her physiotherapist becoming aware of her depression. This may be an unauthorised disclosure under the Privacy Act, irrespective of whether the physiotherapist acquired the information from her medical record or whether it was disclosed by another team member.

In assessing what aspects of Laura's medical record should be disclosed, Laura's GP should have:

- managed the information provided to each team member and maintained strict confidentiality in discussing Laura's condition
- managed what information was collected in her general file, and what was stored separately
- discussed with Laura how (and with whom) her information would be shared.

2.3.6 Subpoenas and disclosure required by law

GPs are obliged to disclose health information in certain circumstances, including for mandatory reporting purposes – such as to colleagues, or regarding communicable diseases or child abuse.

GPs may also receive demands for medical files as part of legal proceedings. These requests may arise where a patient is suing the GP or another organisation (such as an insurer) and the medical records are relevant.

In such circumstances, a subpoena or discovery order is an exception permitting disclosure. Practices should closely examine the scope of any subpoena or discovery order. These orders may request all or only part of a patient's medical record although, generally, court rules require only those records that are reasonably necessary and relevant to the proceeding. Appropriate legal advice should be sought where necessary.

What is reasonably necessary is assessed on a case-by-case basis. If a GP deems it inappropriate to provide a patient's complete health information despite a subpoena, they may have to justify this decision to the court.

GPs may charge reasonable administration charges for the production of these documents. The Australian Medical Association establishes a schedule of professional fees for this.[10]

2.3.7 Transfers of medical records

Privacy legislation does not expressly cover the transfer of medical files between practices, such as during the sale of a practice. However, the Australian Privacy Commissioner has indicated this may require patient consent obtained by both the vendor and purchaser. Professional advice should be sought to ensure transferring patients' records is done in accordance with the relevant laws (for more information, refer to Section 3.2. Sale or closure of a practice).

2.3.8 Information transferred overseas

It is particularly important to consider privacy implications in transferring health information outside Australia, as some countries have little or no privacy standards. Once personal information is disclosed in an unregulated manner, it is very difficult to regain control over it.

The need for protection extends to the use of overseas data storage as well as processing of patient information overseas, such as through the use of transcription and reporting services.

It is recommended to seek patient consent before transferring health information outside Australia (note that alerting patients to this possibility is a requirement of privacy policies. Refer to Section 2.4. Privacy policies). However, consent is not strictly necessary in circumstances where reasonable steps have been taken to ensure the overseas recipient does not breach the privacy of that individual, or where the practice believes the overseas recipient is subject to a privacy scheme or law protecting the information in a manner similar to Australia.

2.4 Privacy policies

Key points

- Your practice must have an up-to-date and patient-focused privacy policy (which includes describing how health information is managed in your practice).
- Your practice's privacy policy must be available free of charge and easily accessible to your patients in an appropriate form.
- Privacy policies must accurately reflect your practice's actual procedures and address certain prescribed requirements.
- A privacy policy must explain:
  - how personal information is collected, used and disclosed within the practice
  - how a patient may access and correct their information
  - how privacy complaints can be made and how the complaint will be dealt with
  - whether information is likely to be disclosed overseas and, if so, where.

2.4.1 External privacy policies

Your practice should maintain a clearly expressed privacy policy that is freely available in printed or electronic form. For example, display a printed copy at the practice reception desk or in waiting areas, or publish an electronic copy on the practice website.

The privacy policy's content will depend on each practice's processes and structure and the record-keeping system used.

Your practice's privacy policy will enable the practice to better manage patient enquiries or complaints concerning their health information.

The RACGP has developed a privacy policy template. It is important to adapt this template to ensure its relevance to your practice. The template is available at www.racgp.org.au/ehealth/privacy

2.4.2 Internal privacy procedures

It is strongly recommended your practice has documented internal privacy procedures. Such procedures should include information about:

- the collection of health information, ensuring it is conducted in a discreet manner protecting the information from unauthorised access
- obtaining a patient's consent to the use or disclosure of health information by practice employees (including doctors, locums, registrars and other authorised healthcare service providers)
- obtaining the patient's consent to the use or disclosure of health information for the purposes of medical research, quality assurance and improvement (where relevant)
- providing patients with access to their health information
- de-identifying health information
- ensuring health information is appropriately disclosed where authorised
- classifying health information, to ensure disclosure is limited to that authorised
- ensuring protection against unauthorised access across each medium the practice employs (eg hard copy or electronic records, verbal disclosures)
- ensuring protection against any loss of data
- retention of individual medical records to satisfy health record law requirements (refer to Section 3.3.3. Retention and destruction of medical records).

Your practice's internal procedures should include information about privacy and confidentiality training. All staff handling health information must be aware of and comply with the practice's internal procedures.

It is recommended to nominate one person who will be responsible for overseeing the implementation and operation of the privacy policy and to be the point of contact for privacy concerns.

2.5 A patient's right to anonymity and pseudonymity

Key points

- Wherever it is lawful and practical to do so, patients must have the option of not identifying themselves or using a pseudonym when requesting healthcare.
- Anonymity and pseudonymity take their ordinary meaning, although it is important to understand they are distinct concepts.

The nature of general practice and the provision of healthcare do not easily accommodate the notions of anonymity and pseudonymity. Medical histories are required and identities need to be confirmed before a GP can make a diagnosis or prescribe medications. GPs are obliged by law to report communicable diseases and child abuse. These circumstances should be explained to the patient.

A patient may experience detriment in their treatment if they choose to remain anonymous. This should also be explained to the patient.

Where practical, offering the option of anonymity and pseudonymity should be integrated into usual practice. A telephone service for general or referral advice or providing general assistance (for basic information or on issues such as quitting smoking or mental health) are examples of when anonymity or pseudonymity may be used.

2.6 Patient access to medical records

Key points

- Patients may access all their personal information held by your practice, subject to limited exceptions.
- Your practice must respond to requests for access within a reasonable period (generally 30 days).
- It is important to verify the identity of the requesting person.
- Practices are not required to provide access if they reasonably believe:
  - it would unreasonably impact the privacy of another
  - it may threaten the life, health or safety of another or the public.

  Other exceptions to providing access may apply.
- Refusal to grant access must be communicated in writing with reasons and the process for lodging a complaint.

2.6.1 Scope of access

The scope of a patient's access rights is quite broad and encompasses all of a patient's personal information. A patient's medical record includes all information created by the treating GP(s) or received from other practitioners, and usually exists in both electronic and hard copy documents. Therefore, such requests will affect information held on the practice's administrative system as well as in the medical record.

Your practice must be able to identify those records containing another patient's personal information, or have the capacity to search relevant medical records where necessary. This commonly occurs in the family setting.

2.6.2 Managing access

Some state legislation requires access requests be made in writing. In any event, it may be preferable to request the patient to put it in writing.

Some requests may involve collating a significant amount of information. A written request will permit greater clarity on the information being sought. A written request also provides a record of the request.

Where a patient is provided with access to their medical record, it may be desirable for the usual treating GP to be available to clarify its contents and to discuss any concerns with the patient.

Alternatively, it may be appropriate to refer the patient to the original author of a record (such as when health information is received from a specialist).

In some circumstances, GPs may discharge their obligation to provide access to health information by arranging for the patient to obtain the information from an intermediary, such as a referring doctor. This might be the preferred option for a pathologist, for example, who has had no direct contact with the patient. In all cases, however, the intermediary must be mutually agreed upon.

Some states only allow the use of intermediaries where there is a serious threat to the life or health of the requesting patient.

2.6.3 Manner of access

Requests will usually be for access to a patient's entire medical record. However, requests for particular information may be received by email, phone or in person.

A practice may not be comfortable in providing entire medical records (although they may choose to do so); however, merely being uncomfortable or asserting proprietary rights is not a valid ground for refusal. The privacy laws require access as requested, where reasonable and practical, or in a mutually agreed way if not reasonable or practical.

It is strongly recommended practices consider these reasonable and practical exemptions carefully in response to a request for a full medical record. Although the obligation is to provide the information in the manner requested by the patient, in the general practice setting it may be unreasonable to hand over an entire medical record. It is advised that practices do not release the original paper file. Practices are entitled to make this assessment and should consider acceptable alternatives. In providing alternatives, the needs of the practice and the patient should be considered.

In many cases, patient requests for access to health information may be satisfied by way of an up-to-date summary containing all relevant material. However, this may prove more administratively burdensome, and in any event a patient will retain their right to access their full medical record. Another alternative is to provide access to a patient's medical files in a room at the practice.

2.6.4 Refusing access

It is recommended that your practice is familiar with the grounds on which it may refuse to provide access, when and where necessary, and therefore can defer to the appropriate provision when required.

In particular, your practice should consider the risk of distress to other patients. For example, practices may consider refusing access when:

- that access would lead to significant distress or lead to self-harm or harm to another person[3]
- the health information of another patient is contained within the medical record
- the requesting patient's information was disclosed by another patient in confidence
- the possibility of domestic abuse or child abuse exists.

If a GP is considering refusing access, they should obtain professional advice.

When third-party patient records are involved in the request for access, the practice may consider approaching the affected patient for their consent. It is not recommended practices attempt to de-identify third-party information for this purpose as it is unlikely to be effective. However, practices may delete or make unreadable the relevant information from the file prior to providing access.

Case study 3: Access through an intermediary

Mary has requested her medical file.

In assessing her request, the practice manager notes Mary has recently moved away from the practice. Satisfying the request would mean sending a copy of the medical record by courier. The practice determines the costs of doing so would be quite high.

In addition, Mary's treating GP does not want to send the full medical record. She is concerned Mary would not understand some of the information, and the inevitable internet searching that would follow to clarify unknown medical terms, would only cause further stress.

In consultations with the GP, the practice manager determines it would not be reasonable or practical to send the medical file to Mary. However, they contact Mary to inquire whether sending the record to a closer GP would assist her. Mary agrees and is able to discuss the contents of the record with her local GP in an informed environment.

2.6.5 Access fees

Your practice can charge a fee for providing a patient access to their personal information, but not for merely requesting access. You should therefore only consider imposing fees (if at all) after the request is made.

A practice may levy reasonable fees to cover the cost of:

- administration for file searching, collating, etc
- copying or printing records
- postage or courier fees
- facilitating access with intermediaries.

Your practice may wish to consider the patient's individual circumstances and their capacity to pay prior to determining and/or waiving access fees.

Practices should keep in mind the potential to align a patient's access request with a consultation, or being compensated through reasonable administrative fees. Appropriate legal advice should be sought to determine where this is allowable and practical within the context of the practice.

2.6.6 Policy on access

It is recommended your practice develops and implements a policy covering patient record access. Such a policy would have information about:

- how and to whom requests for access should be made
- the process for identity verification
- how access will be granted
- response times
- whether access fees will apply, and in what circumstances (if any) these charges will be waived.

This information may be incorporated into your practice's privacy policy (refer to Section 2.4. Privacy policies).

2.7 Correction of health information

Key points

- Your practice must take reasonable steps to correct health information it holds about patients:
  - if your practice is satisfied that information is inaccurate, out of date, incomplete, irrelevant or misleading
  - if a patient requests it to do so.
- It is important to verify the requesting person's identity.
- Correction requests must be responded to within a reasonable period.
- Refusals must be communicated in writing with reasons and the process for lodging a complaint.
- Your practice must take reasonable steps to notify affected third parties of the corrected information.

It is expected that reasonable care will be taken in the development and maintenance of the records when correcting information (refer to Section 3.3.1. Maintaining accurate and complete medical records).

2.7.1 Notification to third parties

In the event of corrections, your practice must notify any third parties to whom the affected health information has been disclosed. In order to do so, it is recommended to keep reasonable records of any disclosures.

2.7.2 Policy on correction

Similar to access requirements, your practice may wish to implement procedures regulating the management of requests for health information correction. These may be incorporated into the practice's privacy policy.

It is important to note that the rights concerning correction differ to those for access, and practices cannot force patients requesting correction to follow a particular procedure or use a particular form. Policies should instead use a pragmatic approach to addressing the requests.

3. Information management relating to general practice

3.1 The business of general practice

Key points

- It is reasonable to infer consent for the use of health information for internal business practices.
- If your practice rotates GPs (such as by the use of shifts) patients should be made aware of this.
- Consent should be obtained prior to disclosing and collecting health information between related bodies corporate or service trusts.

3.1.1 The use of health information for business purposes

Patients would reasonably expect their personal information to be used for the following secondary purposes. Therefore, specific consent would not be required for:

- 'normal internal business practice, such as auditing, business planning'[3]
- billing or debt-recovery (confidentiality should be maintained).

This expectation will likely extend to practice staff having access to patient health information for these same purposes.

Advice confirming this should be sought prior to a particular disclosure to a third-party service provider engaged for these purposes.

3.1.2 Group practices

In group practices that allocate GPs to patients on the basis of availability, a patient's health information will be disclosed to and used by whichever GP sees the patient.

New patients should be made aware of this rolling or rotating use of GPs. Patients should be made aware of the consulting GP when booking their appointment. It is reasonable to infer consent to the use and disclosure of the patient's health information in this context if the patient does not otherwise object to seeing the allocated GP.

This principle extends to the incorporation of new GPs into existing practices or partnerships. While the primary purpose of using the health information is the provision of healthcare services by the practice, it is still technically a disclosure requiring prior consent under the privacy laws. It is possible to infer consent when a patient has sought a consultation with the new GP.

3.1.3 Transfers between related bodies corporate

There is no express permission to transfer health information between related bodies corporate or service trusts. Ideally patient consent to this transfer should be obtained.

Corporate practices and practices employing service trusts should therefore ensure each involved entity has sufficient consent to undertake its activities (one discloses, the other collects) to avoid interfering with a patient's privacy.

3.2 Sale or closure of a practice

3.2.1 Privacy considerations

A significant proportion of a general practice's asset value is contained within the practice's patient roll, and it is unlikely that a practice would be sold without it.

The Privacy Act is not particularly well adapted to the sale or transfer of medical records. Medical records would be transferred when a sale by a sole practitioner or an unincorporated practice involved the transfer of the general practice business (the medical files being one asset of that business).

Although the transferring of records containing health information occurs as part of a business sale, it is unclear whether consent is required from each patient whose medical record is being transferred and which parties require that consent. Some organisations suggest the transfer of medical records in this circumstance involves practicality issues and therefore consent need not be sought.

However, where possible and practical, a long settlement period is recommended for business or asset sales involving medical record transfer. This will allow consent to be obtained from a greater number of patients (either express or inferred) through consent forms or prominent notices of the transfer of the records, either in the practice or provided to the patient.

Prior to and during this settlement period, vendors must be careful to maintain the records securely and prevent unlawful access, modification, use or disclosure, and avoid inadvertent and unlawful disclosure of any personal information to the purchaser.

When asked to facilitate due diligence, vendors may consider restricting access to only selected purchaser personnel and only permitting the inspection of medical records (and not their reproduction). Providing de-identified documents may be appropriate.[11]

Vendor GPs should also be aware that medical records may need to be retained (or at least accessed) for insurance or other medico-legal purposes. It is important the sale agreement and patient consents permit this.

If the sale is of shares in an incorporated general practice, there is no transfer of personal information (it is retained within the company), and privacy concerns will not apply to the transfer itself.

3.2.2 Deceased GPs

If a practice closes due to a GP's death, the practice staff (or the executor in the case of a sole practitioner) should take reasonable steps to notify patients and organise transfer of their medical records to another GP.

3.2.3 Health record legislation

There are additional requirements for the transfer or closure of a general practice under current health records legislation.

For example, legislation in Victoria and the ACT require practices to publish a notice in a local newspaper stating that the practice is closing or being sold, and detailing the manner in which the practice proposes to deal with the medical records.

Where necessary, advice should be sought.

3.3 Medical records

Key points

- Your practice must ensure the health information it collects, uses or discloses is relevant, accurate, up-to-date and complete.
- Your practice must take reasonable steps to ensure health information that is no longer practically or legally needed is destroyed or de-identified.
- Medical records are usually owned by the practice, not the patient.

3.3.1 Maintaining accurate and complete medical records

It is important medical records are accurate, up-to-date, comprehensive and legible. GPs must take reasonable steps to ensure the health information and consultation notes they hold are well organised. Medical records should at all times be sufficiently detailed and accessible to allow another GP to continue the management of the patient.

Your practice should use a follow-up system (subject to patient consent) to ensure patients are regularly seen and medical records are maintained accurately and contain up-to-date information. The marketing aspects of such a system should be considered (refer to Section 3.4. Marketing).

3.3.2 Ownership

Patients do not own their medical record. Ownership may vary as follows:

- Sole practitioners retain full ownership over their medical records.
- Contract and employee GPs are likely to be creating medical records for their principal or employer, and unlikely to own these themselves.
- GPs operating in a partnership may have a claim to a shared partnership interest over some or all of the totality of medical records.
- GPs who own an incorporated practice own its assets and this usually includes the medical records; in the absence of any agreement specifying otherwise, multiple owners own the medical records jointly.

The ownership of medical records is most often settled by written agreement. In the absence of such an agreement, ownership may be dependent on the nature of the relationship between the GPs.

It is recommended the ownership of medical records is clarified before GPs commence at a new practice, to avoid any later dispute when a departing GP proposes to take records with them. It is recommended that appropriate advice is sought prior to entering into any such agreement.

Despite the above, GPs are required under the Medical Board of Australia's *Good medical practice: A code of conduct for doctors in Australia* to promptly facilitate the transfer of health information when requested by a patient.[7]

3.3.3 Retention and destruction of medical records

Your practice should retain health information as required, and in accordance with the applicable laws.

The Privacy Act requires health information to be destroyed or permanently de-identified once it is no longer needed for any authorised use or disclosure.

However, the ACT, NSW and Victoria require medical records to be retained until a child turns 25, and for adults, for seven years from the date of the provision of the last health service. This overrides the Privacy Act.

Under some state and territory legislation, the destruction of any medical record is prevented when such record is likely to be involved in legal proceedings. It is recommended to seek advice on the current limitation periods applicable to your practice.

GPs must take reasonable steps to destroy or permanently de-identify health information following the expiry of these periods.

3.3.4 De-identification

Your practice may choose to permanently de-identify health information rather than destroy it. Care should be taken to ensure there is no prospect of the patient being identified from the remaining information.

The de-identification of health information is more than simply removing the patient's name. Any identifying information contained in the medical record must be deleted or destroyed to ensure anonymity.

Whenever the information is in the form of individual data sets, there is a risk the data set could be linked to a particular individual based on details of age, postcode and medical condition. The more information included in the data set, the greater the risk of identification.

Even where data is aggregated, care is needed to ensure the number of people in each 'cohort' or sub-group is sufficient to ensure the privacy of the individuals is not compromised. For example, the relevant NHMRC guidelines specify a minimum of five sets of individual's data in each cohort.[12]

3.4 Marketing

Key points

- Health information must not be used or disclosed for the purpose of direct marketing without patient consent.
- Your practice must currently obtain patient consent to ordinary services with commercial aspects, such as vaccinations.
- Sending unsolicited commercial communications to your patients is generally prohibited.

3.4.1 Prohibitions on direct marketing

General practices may not ordinarily consider themselves to engage in marketing activities. However, any promotion of a practice's services, even as scheduled reminders or as part of good clinical practice, may technically constitute direct marketing and therefore an interference with privacy.

Direct marketing refers to a marketing technique in which the ordinary retail environment is bypassed with the vendor promoting goods and services directly to customers. The regulation of direct marketing is much tighter with health information, and its boundaries in general practice are currently unclear. Practices should note many day-to-day clinical initiatives may inadvertently breach these laws. For example, letters that use or disclose personal information promoting commercial services to advise patients about flu vaccinations are likely to constitute direct marketing.

In contrast, the Australian Privacy Commissioner considers that letters relating to ongoing care are less likely to contravene privacy laws, especially if the letters merely inform the patient of scheduled assessments and do not specifically promote any services.

To avoid inadvertently breaching these laws practices should obtain patient consent by:

- requesting consent (via opt-in or opt-out mechanisms) on patient registration sheets and recording this consent in the management software
- asking for consent as patients present to the practice
- undertaking a directed consent campaign.

GPs must ensure they have adequate procedures in place to ensure marketing messages are not sent to patients who have expressed their refusal.

3.4.2 The Spam Act and Do Not Call Register

The Privacy Act defers to the operation of the *Spam Act 2003* and the *Do Not Call Register Act 2006*.

As a general rule, these acts prohibit practices from sending unsolicited communications (by email, text message or phone call) with the aim of selling goods or services, or inducing the sale of the same. Practices sending solicited communications must ensure they meet any requirements in doing so, such as providing an unsubscribe function for mobile text message reminders.

It is important practices are aware of the applicable prohibitions (and their exceptions) when sending electronic (email or text messages) or telephone communications.

3.5 Information security

Key points

- Your practice must take reasonable steps to protect personal information it holds:
  - from misuse, interference and loss
  - from unauthorised access, modification or disclosure.
- Cross-border disclosures must be preceded by reasonable steps to ensure no privacy breaches will occur.
- Practices should refer to the RACGP's resources on protecting your practice information to ensure best practice is followed for information security, available at www.racgp.org.au/your-practice/ehealth/protecting-information

3.5.1 Risk assessments

Adopting appropriate information security measures is vital to ensure health information is protected,[13] and these should cover information systems for storing, processing and transmitting information.

Practices should develop and implement appropriate policies and procedures specifying which staff have access to health information and under what circumstances. It is recommended practices regularly audit these measures and perform practice risk assessments as appropriate.

Physical measures for protecting the security of health information include having locked filing cabinets and security alarm systems to detect unauthorised access, and ensuring there is no unauthorised after-hours access to the practice.[13]

For information stored electronically, security measures may include password protection, automatic log offs, log file/electronic audit trails, firewalls, malware and virus protection, and ensuring the encryption of data for high-risk transmissions.

3.5.2 Electronic transfer of information

Electronic transfers of information are governed by the same privacy principles regarding the use and disclosure of that information.

Prior to sending any electronic communication GPs should ensure secure encryption protocols are in place and operating effectively. Although unlikely, email can be intercepted, retrieved and read by unintended recipients without authorisation.

For further information, refer to the RACGP's resources on using email in general practice, available at www.racgp.org.au/your-practice/ehealth/protecting-information/email

3.5.3 Patient communication via electronic mediums

The ease of and access to sending and receiving messages electronically means patients are using this medium more frequently to contact their general practice.

The Australian Health Practitioner Regulation Agency's *National Board policy for registered health practitioners: Social media policy*[14] is an adjunct to the Medical Board of Australia's *Good medical practice: A code of conduct for doctors in Australia* and should be read concurrently. Its provisions apply to all registered health practitioners.

Your practice needs to address what content is appropriate to send and discuss via electronic messaging. A policy should be developed concerning the safe use of electronic communication for both practice and patients. It should be noted the full implications of the Privacy Act apply to any electronic communication, and online privacy breaches may be far more significant than the same breach using paper communication.

Patients are highly unlikely to send encrypted emails, so content within an email should be limited in scope. Due to the inherent insecure nature of the internet, health information should not be sent through unsecured channels. Where possible, secure message delivery should be used between practices with compatible encryption processes.

3.5.4 Secure destruction and de-identification

Unnecessary health information should be destroyed securely to prevent unauthorised access. Prior to destruction, consideration needs to be given to the relevant retention requirements under any applicable health legislation (refer to Section 3.3.3. Retention and destruction of medical records).

Secure deletion occurs where the records are no longer accessible through normal or forensic means. Ordinarily, deletion from a database does not totally erase the record nor does it remove the record from the hard disk or other storage medium. Unless data is erased and overwritten multiple times, the data may remain on the storage medium and be accessible forensically.

Deleting individual patient records may not be possible due to practice software limitations. Where relevant, advice should be sought from software vendors or other professionals.

More information on secure deletion of data can be found in the RACGP's resource *Effective solutions for e-waste in your practice*, available at www.racgp.org.au/your-practice/e-health/protecting-information/e-waste

Case study 4: International consultation

Dr Murray, a GP, has been approached by a patient with a particular abscess on his leg.

During the consultation, Dr Murray recalls a seminar he attended that discussed very similar wounds, led by a professor from Canada.

Dr Murray considers it appropriate to refer the wounds to the professor, and so takes several photographs of the abscess on his patient's leg. These photographs were later emailed to Canada along with pertinent extracts of the patient's notes (including some personal information).

Unwittingly, Dr Murray is likely to have breached the cross-border disclosure laws. Dr Murray could have managed the situation better if he:

- sent the photographs in a de-identified form
- sought the patient's informed consent to the disclosure
- investigated the privacy laws that apply in Canada
- sought the professor's assurance that the photographs would be examined in strict confidence, prior to sending them, and that they would be destroyed afterwards.

3.5.5 Security policy

It is recommended your practice develops and implements an information security policy. Such a policy will assist in ensuring organisational systems used for processing and storing, or transmitting, personal information, are managed and protected appropriately.

To be effective, security policies must be known by practice staff and monitored and reviewed on a regular basis.[3]

3.6 Mandatory data breach notification

From February 2018, the Privacy Act will impose a mandatory data breach notification scheme for 'eligible data breaches'.

An eligible data breach is an authorised access, disclosure or loss of personal information by your practice resulting in serious harm to your patients.

Data breaches occur from time to time in any office environment. Typically, this will occur through the loss of an electronic storage device or paper records containing personal information.

Other examples of common breaches include:

- employees accessing personal information outside the scope of their employment
- paper records stolen from insecure garbage or recycling bins
- when sending a patient's personal details and/or health information to the wrong recipient
- a practice being deceived into improperly releasing the personal information of another person
- accidental or inadvertent disclosure.

If your practice believes an eligible breach occurred resulting in serious harm to patients, the mandatory notification law requires you to:

- prepare as soon as practicable a statement for the OAIC detailing the breach
- subsequently notify each affected patient of the content of that statement (if not practical, your practice must publish a copy of the statement on its website).

It is recommended your practice develops a robust data breach response plan to take timely and efficient actions.

3.7 Healthcare identifiers

Key points

- Healthcare identifiers generated by your practice's desktop system should not include any information from:
  - the patient's name
  - the patient's date of birth
  - the patient's address
  - the patient's telephone number
  - the patient's Medicare number
  - any identifier assigned by a government agency
  - any other information that could identify the person.
- Your practice must not use or disclose a patient's Medicare number, Individual Healthcare Identifier or any other identifier assigned by or on behalf of a government agency, unless:
  - required to fulfil their obligations to that agency
  - to lessen or prevent a serious threat to life, health or safety or public health and safety
  - required or authorised by law, or for certain law enforcement purposes.

An Individual Healthcare Identifier is a unique number assigned to healthcare consumers, healthcare providers and organisations providing healthcare services. For example, an Individual Healthcare Identifier is automatically allocated to all persons enrolled with Medicare and anyone who is issued with a Department of Veteran's Affairs entitlement. It is available to all others who seek healthcare in Australia.

The use of healthcare identifiers instead of names is useful to protect privacy. However, the adopted identifier system used by your practice must not include any prohibited details. In addition, the identification number should not reveal any health information about the patient.

3.8 Health research

Key points

- Health research participant consent must be obtained.
- Research records should be de-identified at the earliest possible time.
- Researchers must strictly comply with both privacy and ethical obligations, in particular when conducting research using human participants.

The legal and ethical principles governing health research using human participants make it clear that research participant consent is paramount.

Patients should understand what the proposed research involves, the ways in which their health information will be used or disclosed, the risks and benefits of agreeing to participate, and whether the research will be published.

Ethical obligations include ensuring the research design clearly collects informed consent, avoiding publishing identifiable information (unless participants have consented otherwise) and informing participants of the potential to be identified even from de-identified material.

For more information, refer to the NHMRC's *National statement on ethical conduct in human research 2007 (updated May 2015)*,[1] and the Therapeutic Goods Administration's *Australian clinical trial handbook*.[15]

3.8.1 Considerations when participating in health research

Patients should be made aware your practice may use de-identified health information for public health research. This may be done by way of an information sheet in the waiting room or noting consenting patients.

In the case of epidemiological research, it will generally be unnecessary to keep patient identifiable data sets. In any event, all research records should be de-identified at the earliest possible time consistent with the proper conduct of the research.

3.8.2 Interaction between the Privacy Act and health research

In addition to privacy obligations, practices must comply with all ethical requirements imposed for research conducted on human participants. It is important researchers understand they must comply with both privacy and ethical obligations (as appropriate).

For example, even where human research has approval to publish identifiable health information, practices must ensure all relevant Privacy Act requirements are satisfied before doing so. The safest manner of doing so is through obtaining written participant consent.

The option to use health information for a secondary purpose is also left open by the Privacy Act, if it is reasonable to expect this information will be used in health research (refer to Section 2.3.1. Use for primary and secondary purposes). This may include use for quality improvement activities within the practice.

Where there is any doubt as to whether the proposed research is directly related to the purpose for which the information was collected or within the reasonable expectations of the patient, written consent should be obtained.

4. Privacy considerations

This list of considerations should be used as a guide only, and does not exhaustively describe the complete list of activities that should be undertaken when assessing privacy measures within your practice. Each privacy consideration has explanatory notes to guide you on what information should be included to address each question. The privacy considerations list is to help your practice:

- determine its level of compliance to the laws governing health information
- assess, achieve and maintain good privacy practice
- identify areas requiring practice innovation and improvements, and get appropriate assistance where necessary.

Establishing a practice privacy policy	
Does your practice have an up-to-date, accurate, accessible, and freely available privacy policy?	Your practice should have a policy that defines how to handle enquiries and complaints. Customise the RACGP's *Privacy policy template* to your practice, available to download at www.racgp.org.au/your-practice/ehealth/protecting-information/privacy
Quality and content of medical records	
Does your practice have processes in place to ensure it holds accurate and up-to-date data at all times?	Your practice should develop a policy for everyone to understand and follow regarding how data is accurately collected and safely held.

Patient consent	
Does your practice have a procedure for requesting and recording patient consent? ***Do your practice staff understand the requirements surrounding this?***	Consent may be sought for primary and secondary uses provided they are adequately stipulated. Although inferred consent may be relied upon in certain circumstances, express consent (a signature or a documented positive response to a question) should always be sought.
Collecting health information	
Does your practice have defined processes to inform patients of when, what and how the practice collects health information? ***Does your practice have a process or systems in place to handle requests for anonymity or pseudonymity?***	This may include manual procedures or the ability of your IT systems and software to handle the tasks.
Patient access to personal information	
Does your practice have procedures for handling patient requests for access to and correction of their information?	These procedures include assessment of requests, refusal procedures and administration fees.
Use and disclosure of personal information	
Does your practice have a process for patients to opt in or out of marketing communications?	The RACGP's Patient privacy pamphlet communicates marketing options to your patients and can be customised to your practice. Available to download at www.racgp.org.au/your-practice/ehealth/protecting-information/privacy
Medical research	
Does your practice have procedures for conducting health research, including participant consent and notification?	This includes procedures for how to deal with requests for the secondary use of data. Refer to the RACGP's resource *Secondary use of general practice data* for guidance and a decision-making support tool, available at www.racgp.org.au/your-practice/ehealth/data
Quality improvement and continuing professional development	
Does your practice have procedures to record occurrences of patient information use for quality improvement and continuing professional development?	Your practice's privacy policy should disclose whether patient information is used for continuing professional development purposes and/or for quality improvement activities.
Information security and data retention	
Does your practice offer an information security level sufficient to ensure the safe and proper protection of the information it holds? ***Does your practice have a process for document classification, retention, destruction and de-identification of patient information?***	This will provide documented evidence of good practice in information security, including the secure disposal and de-identification of information, and proper data retention periods.
Healthcare provider identification	
Does your practice have a process for identifying the need for, and recording of, the consent of a healthcare practitioner?	This occurs when sharing information identifies the practice, even though the patient health information may be de-identified.
Healthcare identifiers	
Do your practice staff understand the restrictions on use of healthcare identifiers?	Educate staff on the requirements of the *Health Identifiers Act* and other government initiatives that your practice is engaged in.
Mandatory data breach notification plan	
Does your practice have a data breach response plan?	Your practice should have a regularly tested emergency response plan to deal with data breaches and a plan outlining who should, and how to, communicate a data breach.

5. Australian states' and territories' advice on privacy

Organisation	Website	Phone
Australian Government – Office of the Australian Information Commissioner	www.oaic.gov.au	1300 363 992
ACT – Human Rights Commission	www.hrc.act.gov.au	(02) 6205 2222
NSW – Information and Privacy Commission	www.ipc.nsw.gov.au	1800 472 679
NT – Office of the Information Commissioner	www.infocomm.nt.gov.au	1800 005 610
Qld – Office of the Information Commissioner	www.oic.qld.gov.au	(07) 3234 7373
SA – Privacy Committee of South Australia	www.archives.sa.gov.au/content/making-privacy-complaint	(08) 8204 8786
Tas – Ombudsman Tasmania	www.ombudsman.tas.gov.au	1800 001 170
Vic – Office of the Commissioner for Privacy and Data Protection	www.cpdp.vic.gov.au	1300 666 444

6. References

1. National Health and Medical Research Council, Australian Research Council, Australian Vice-Chancellors' Committee. National statement on ethical conduct in human research (2007) (updated May 2015). Canberra: NHMRC, 2015. Available at www.nhmrc.gov.au/book/national-statement-ethical-conduct-human-research [Accessed 4 April 2017].
2. Commonwealth of Australia. Privacy Act 1988. Canberra: Commonwealth of Australia, 1988. Available at www.comlaw.gov.au/Details/C2014C00076 [Accessed 4 April 2017].
3. Office of the Australian Information Commissioner. Australian Privacy Principles guidelines: Privacy Act 1988. Canberra: OAIC, 2015. Available at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines [Accessed 4 April 2017].
4. Office of the Chief Parliamentary Counsel Victoria. Health Records Act 2001. Melbourne: OCPC, 2001. Available at www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst9.nsf/DDE300B846EED9C7CA257616000A3571/831E52D30DC34D78CA2580B8001878C3/$FILE/01-2aa033%20authorised.pdf [Accessed 4 April 2017].
5. NSW Parliamentary Counsel's Office. Health Records and Information Privacy Act 2002. Sydney: PCO, 2002. Available at www.legislation.nsw.gov.au/#/view/act/2002/71/whole [Accessed 4 April 2017].
6. ACT Parliamentary Counsel's Office. Health Records (Privacy and Access) Act 1997. Canberra: PCO, 1997. Available at www.legislation.act.gov.au/a/1997-125/ [Accessed 4 April 2017].
7. Medical Board of Australia. Good medical practice: A code of conduct for doctors in Australia. Melbourne: Medical Board of Australia, 2014. Available at www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx [Accessed 4 April 2017].
8. Office of the Australian Information Commissioner. Business resource: Collecting, using and disclosing health information for research (draft). Canberra: OAIC, 2015. Available at www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-collecting-using-and-disclosing-health-information-for-research [Accessed 21 April 2017].
9. Office of the Australian Information Commissioner. Business resource: Using and disclosing patients' health information (draft). Canberra: OAIC, 2015. Available at www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-using-and-disclosing-patients-health-information [Accessed 5 April 2017].
10. Australian Medical Association. Frequently Asked Questions – Fees. Canberra: AMA, [date unknown]. Available at https://ama.com.au/article/frequently-asked-questions-fees [Accessed 5 April 2017].
11. Office of the Australian Information Commissioner. What happens if I sell my small business including a customer database? Canberra: OAIC, [date unknown]. Available at www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/businesses/what-happens-if-i-sell-my-small-business-including-a-customer-database [Accessed 5 April 2017].
12. National Health and Medical Research Council. Use and disclosure of genetic information to a patient's genetic relatives under Section 95AA of the Privacy Act 1988 (Cth) – Guidelines for health practitioners in the private sector. Canberra: NHMRC, 2014. Available at www.nhmrc.gov.au/guidelines-publications/pr3 [Accessed 5 April 2017].
13. Office of the Australian Information Commissioner. Guide to securing personal information. Canberra: OAIC, 2015. Available at www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information [Accessed 5 April 2017].
14. Australian Health Practitioner Regulation Agency. Social media policy. Canberra: AHPRA, 2014. Available at www.medicalboard.gov.au/Codes-Guidelines-Policies/Social-media-policy.aspx [Accessed 5 April 2017].
15. Department of Health and Ageing, Therapeutic Goods Administration. The Australian clinical trial handbook. Canberra: TGA, 2006. Available at www.tga.gov.au/sites/default/files/clinical-trials-handbook.pdf [Accessed 5 April 2017].

RACGP

Royal Australian College *of* General Practitioners

Healthy Profession.
Healthy Australia.