RACGP

Handbook for the management of health information in general practice

3rd edition

Handbook for the management of health information in general practice, 3rd edition

Disclaimer

The information set out in this publication is current at the date of first publication. It is intended for use as a guide of a general nature only and to flag issues for GPs and general practices for their further consideration. It may or may not be relevant to particular practices or circumstances.

This publication is not and does not seek to be an exhaustive assessment of the subject matter. The contained material is tailored toward general practice, and reviews only a portion of the relevant law.

Persons implementing recommendations contained within must always exercise their own independent skill or judgement or seek appropriate professional advice relevant to their own particular circumstances. Compliance with recommendations does not guarantee discharge of any law, or duty of care owed to patients and others coming into contact with the health professional and the premises from which the health professional operates. Nor does it guarantee the satisfaction of any legal or regulatory requirements.

To the extent permitted by law The Royal Australian College of General Practitioners (RACGP), its employees and contractors do not make any representation or warranties of any kind (express or implied), and disclaim all 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.

Recommended citation

Handbook for the management of health information in general practice,
3rd edn. Melbourne: The Royal Australian College of General Practitioners, 2014

The Royal Australian College of General Practitioners
100 Wellington Parade
East Melbourne Victoria 3002 Australia
Tel 03 8699 0414
Fax 03 8699 0400
www.racgp.org.au

ISBN 978-0-86906-380-4 (web)
ISBN 978-0-86906-381-1 (print)

First edition published October, 2002
Second edition published July, 2012
Third edition published July, 2014, amended April, 2016

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

RACGP

Handbook for the management of health information in general practice

3rd edition

Acknowledgments

The *Handbook for the management of health information in general practice* (3rd edition) was produced by the Royal Australian College of General Practitioners.

The Handbook is based on the first edition developed in conjunction with the Committee of Presidents of Medical Colleges and the General Practice Computing Group in 2002.

The RACGP gratefully acknowledges the assistance provided by the National Standing Committee – General Practice Advocacy and Support, and Associate Professor Patricia Williams (PhD) from Edith Cowan University.

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 regulatory framework for the management of health information.

Addressing this need, and as part of its ongoing member focus, the RACGP has revised the *Handbook for the management of health information in general practice* (the Handbook). The revised Handbook aligns with current best practice, including commentary on the recent amendments to the *Privacy Act 1988* (the Privacy Act). The Privacy Act understandably sits prominently in considerations of health information management.

Significant amendments to the Privacy Act commenced in March 2014. While many obligations affecting the management of health information carry over, some amendments are significantly different from the former provisions, and place additional obligations on practices to safeguard personal information.

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.

This publication broadly reviews the management of health information in the general practice setting. It examines the current privacy legislative framework that incorporates the new Australian Privacy Principles and the various Health Records Acts, including providing guidance and examples for compliance with each, and generally examines information management within a general practice setting. This publication also reviews the manner in which data is maintained.

There are several other publications referenced within the Handbook. As the Handbook is designed to provide a broad overview, it defers to these publications for readers to obtain more detailed information. The RACGP publication *Computer and Information Security Standards (Second Edition)* (CISS) is one such publication that complements this Handbook. It is strongly recommended this Handbook is read in conjunction with each of the resources named in this guide.

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

As a matter of expediency, only a select subset of the total material has been examined. This subset is an assessment of the regulation most likely to affect general practice. Individual advice should always be sought for a more comprehensive understanding of the framework in which information is regulated or for answers or insights to particular circumstances.

Contents

Part 1. Key concepts

1. Glossary

Australian Privacy Principles or APPs

As of March 2014, the APPs replace the previous Information Privacy Principles and the National Privacy Principles. They provide a consolidated and universal set of principle-based laws, focussing 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

Generally, confidentiality refers to a set of obligations imposed through law or ethics. General practice has elements of each, and confidentiality underpins the doctor–patient relationship. It is usual for a patient to disclose information to their GP on the understanding the information will only be used within the practitioner–patient relationship.

The National Health and Medical Research Council (NHMRC) defines 'confidentiality' as 'the general non-legal principle concerned with 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]

Consent

Refers to informed consent (for more information refer to *Chapter 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] If health information is de-identified it falls outside of the regulation of the Privacy Act and the relevant health records legislation.

Health information

Health information includes information or opinions about the health or disability of an individual, a patient's wishes about future healthcare, or a health service provided to an individual. Importantly it includes information collected in connection with the provision of a health service (and thus names, addresses etc).[2]

Health information is a subset of personal information. As it is also 'sensitive information', (information or opinions about sensitive matters such as race, associations, religion etc), its collection, use and disclosure is more tightly regulated.

Held

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

Personal information

Personal information includes any information or opinion about an individual from which they are identified or are reasonably identifiable (sometimes expressed as whether the identity of the person is apparent or can reasonably be ascertained).[2] Personal information includes names and addresses, signatures, contact details, birth date, medical records and bank account details.

It does not matter whether the information is true. It is also media neutral, so it does not matter whether it is recorded in material form. Personal information can be held in any media, so in the general practice setting it will exist on paper and in electronic records, x-rays, CT scans, videos, photos and audio recordings (such as dictation tapes). It includes information gathered by a GP directly from the individual, as well as information obtained by a healthcare service provider from a patient or a third party in the course of providing a healthcare service.

Practice

In the Handbook, 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. The practice may operate under one of a range of different business structures.

Privacy Commissioner

The Privacy Commissioner is the national regulator of privacy, conferred by the Privacy Act and other laws.

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 general 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 general 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 also disclose health information if they discuss a patient's conditions with other practitioners.

2. Privacy legislation

2.1. The Privacy Act

The Privacy Act applies to the collection of personal information. Its laws apply to sole traders, corporate bodies (including companies and owner corporations), government agencies, partnerships and unincorporated associations, unless an exception applies.

Although some exceptions apply for smaller businesses, general practice is subject to stringent privacy obligations by virtue of providing health services and holding health information.

The obligations of the Privacy Act cut across and influence most aspects of health information management. The March 2014 amendments to the Privacy Act have strengthened the privacy regime and, more importantly, impose massive increases to the penalties for breach. Individuals found liable of infringements of privacy can face penalties of up to $340,000. Corporations found liable for infringements face penalties of up to $1,700,000.

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

2.2. Health records legislation

Health records in Victoria, New South Wales and the Australian Capital Territory are also regulated by health records legislation.[4-6] These state and territory acts limit the handling of health information, as detailed in sets of principles. The principles operate concurrently to the APPs. They are broadly consistent with those in the Privacy Act. Their respective definitions of personal information and health information are also broadly similar.

However, the state and territory health records legislation also imposes additional requirements in certain situations (for example, refer to *Chapter 12 – Sale or closure of a practice*), and care should be taken to ensure compliance with both sets of laws where necessary.

2.3. Doctor–patient confidentiality

The Medical Board of Australia's *Good Medical Practice: A Code of Conduct for Doctors in Australia* describes the expectation of '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'.

According to the *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'. Good medical practice, including examples of what is appropriate in the context of general practice, can be found in that publication.

2.4. Professional advice

This publication has been developed to provide 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.

3. Patient consent

Patients have the ethical and legal right to make informed decisions about their health. Obtaining a patient's informed consent should be the key guiding principle for GPs when dealing with health information.

Consent forms the basis for many Privacy Act exceptions, permitting collection, use and disclosure. A failure to acquire informed consent forms the basis of many medico-legal proceedings.

The requirement to obtain informed consent also applies to research undertaken by a practice.[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), the importance, any benefits and risks, or referral or treatment needs. Patients should also be informed if it is likely their information will be sent overseas and if so, where.

Further information regarding informed consent is available in *Standard 1.2.2 Informed patient decisions* in the RACGP *Standards for general practices* (4th edition).

3.2. Implied or express consent

Consent may be verbal or written, and may be provided by way of:

- express consent, such as where the patient signs or clearly articulates their agreement
- inferred consent, where the circumstances are such to reasonably infer the patient has consented.

Express consent should be sought wherever practicable. A signed document is an example (and easier to demonstrate), but an informative and well-documented discussion with a patient may equally satisfy this requirement. There is no legal requirement for consent to be written (it is merely prudent).

Implied (or inferred) consent should be relied on only when express consent cannot be obtained. If so, care must be taken not to overestimate the scope of that consent.

For example, it is reasonable to infer 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 consent conversations are thoroughly documented. Problems may arise if a patient does not understand the potential uses of their health information. In circumstances where a GP must establish implied consent, comprehensive and contemporaneous consultation notes are extremely valuable. Notes should refer to the information provided, the nature of the discussion and the patient's response.

3.3. Withheld consent

GPs should be cautious of patients who refuse to provide certain health information or withhold consent for particular healthcare.

This is particularly problematic where the possibility of detrimental outcomes exist 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.

3.4. Competence, capacity and maturity to provide consent

Some patients, because of illness or disability, are not competent to provide adequate consent.

Various state and territory guardianship legislation provides a framework for obtaining substitute consent on behalf of patients who are incompetent because of 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 or young person 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 GPs to assess the child's maturity to determine whether they adequately understand. Other states and territories do not have specific legislation.

The Privacy Act does not stipulate age, however 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 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.

Part 2. Information management relating to patients

4. Collection of health information

Key points

- Practices must not collect health information unless the patient consents, it is conducted lawfully and fairly (without intimidation and not unreasonably intrusive) and the information is reasonably necessary for delivery of their health services.
- Consent is not required where:
  - the health information is collected in accordance with the law or rules established by 'competent health or medical bodies'
  - 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.
- Other exceptions apply.
- Unsolicited information (received without asking) must be destroyed unless the practice would ordinarily have lawfully collected that information.

Prior to providing health information, patients should be notified of how their information may be used or disclosed, and what rights of access will apply. Only then can they make an informed decision about whether to provide the information.

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, consider taking a full patient medical history as necessary, where clinically appropriate.

The Privacy Commissioner cites the *Personally Controlled Electronic Health Records Act 2012* (Cth) as an example of rules established by competent bodies.[3] It may also be feasible to consider the medical records requirements under the Medical Board of Australia Code of Conduct or the Australian Medical Association Code of Conduct, as satisfying the requirement for rules. GPs should confirm this with the Privacy Commissioner before relying on it.

4.1. Health information from third parties

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

Where information is received without the GP taking active steps to collect it, GPs should first establish whether the information should be destroyed or de-identified and, if not, whether they would ordinarily have been permitted to collect the personal information.

In many situations, such as where GPs collect a family medical history from a patient, it is rarely practicable to obtain their family's consent. GPs should be aware that the collection of family, social and medical histories in this context is currently permitted.[8]

5. Notification

Key points

- Upon collecting health information, or as soon as possible afterward, GPs must take reasonable steps to notify the patient of the collection.
- Notified information must include the details of the organisation holding or owning their medical record, who their health information may be disclosed to and whether it will be disclosed to an overseas recipient (if so, where).

5.1. Notification obligations

Extensive prescribed notification requirements ordinarily apply to the collection of health information. Many of these notification requirements are obvious in the general practice setting.

For example, it is unnecessary to notify a patient if their health information is being collected during recurring consultations, as it is clearly apparent. It is also 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 straight forward. 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.

Patients need to be made aware of the potential use and disclosure of their health information. 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 6.8 – Information transferred overseas*).

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

5.2. Privacy notices

Practices should also consider whether privacy notices (also known as ‘collection notices’ or ‘APP 5 notices’) addressing the prescribed notification matters in a predetermined format and medium, would be an appropriate medium for notifying patients. Such notices may include information about:

- disclosure within a multi-disciplinary 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.

Openness on the part of the GP about what information is collected, used and disclosed – and by whom – can assist the patient to gain a better understanding of their medical condition. It can also promote shared expectations and a relationship of trust between the GP and patient.

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 expectations of the patient as well as increasing the likelihood further uses of that patient’s health information will constitute secondary use (refer to *Chapter 6 – Use and disclosure of health information*).

A practice’s privacy policy will often double as the privacy notice (refer to *Chapter 7 – Privacy policies*).

6. Use and disclosure of health information

Key points

- A GP's primary purpose for collecting health information is to provide healthcare services.
- Practices may use and disclose it for that 'primary' purpose.
- Health information may be used or disclosed for another 'secondary' purpose where:
  - the patient consents
  - the patient would reasonably expect use or disclosure, which is directly 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.

6.1. Use for primary and secondary purposes

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

Health information is usually collected for the primary purpose of providing particular healthcare services. A practice will always be able to use or disclose health information for the primary purpose.

In certain circumstances, the practice can choose to use health information for other purposes. The two key circumstances for general practice to use health information for another 'secondary' purpose include where the patient consents, or where 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.

It is recommended practice information notices are considered for this purpose. When used appropriately, such notices assist patients to understand how their health information is used and disclosed.

For example, if it is made clear to the patient (either at the commencement of the doctor–patient relationship or during relevant consultations) their health information is collected for a particular activity, it is more likely to be expected by patients.

This information may also be considered for inclusion in the general practice's collection notice (refer to *Chapter 5 – Notification*), and incorporated into the practice's privacy policy (for more information on privacy policies, refer to *Chapter 7 – Privacy policies*).

For more information on secondary use of health information, see the resources developed by the General Practice Data Governance Council (GPDGC) at www.gpdgc.org.au. The GPDGC developed protocols to ensure that general practice clinical data disclosed externally is used in accordance with relevant legislation, ethical principles and practice and with appropriate informed consent.

6.2. 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, each of which being directly related to their receipt of healthcare services. 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
- quality assurance or clinical audit activities
- disclosure to clinical supervisors.[9]

Some practices may also use or disclose health information for medical research. As medical research is 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 *Chapter 18 – Health research*).

Box 1. Case study 1: Primary and directly related purposes

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

Laura's GP recognises Laura's healthcare needs will be greater than what she can provide alone. Laura's healthcare will need a coordinated effort between her treating healthcare professionals, including her neurologist, rehabilitation team and practice nurse.

Laura's GP realises that Laura, in her currently distressed state, may not expect her GP to organise this multidisciplinary team. Accordingly, her GP organises a consultation with Laura to discuss the benefits of coordinating her care. Laura's GP is careful to discuss the benefits of the multidisciplinary care, so that Laura can make an informed decision to accept it. Laura's treating GP carefully notes the conversation and Laura's express consent.

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

However it is unclear whether Laura would have expected her GP to disclose elements of her health information to other health practitioners. This disclosure is likely to 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.

As it was unclear whether Laura would reasonably expect the disclosure to the multidisciplinary team, Laura's GP has done the prudent thing and sought consent. Additionally, by discussing the care plan and the scope of involvement of the multidisciplinary team, Laura's GP has managed Laura's 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.

6.3. Use for business practices

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

For more information on health information in the context of general practice as a business, refer to *Part 3 – Information Management relating to general practice*, and specifically *Chapter 11 – The business of general practice.*

6.4. Medical records for training and education purposes

It is important GPs are able to train in real life environments for continuing professional development and other purposes. However, patients are often not aware their health information may be used in such a manner.

Without consent, it is likely to be unreasonable for GPs to expect patients will permit their health information be used for training and education purposes. However, this expectation may be influenced by the nature of the training activity. For example, videotaping 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 health services, such as reflective discussion with peers.

In the absence of consent, health information should be de-identified before use for training or educational purposes. Training and education in some cases may be as effective when using de-identified case studies, or by using simulated data.

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

To ensure patients understand and have reasonable expectations of quality improvement activities, practices are encouraged to include information about these activities and clinical audits in the practice policy on managing health information. If a practice intends to use de-identified information, it is still worth notifying patients of that fact in your privacy notice.

For more information, refer to *Standard 4.2.1 Confidentiality and privacy of health information* in the RACGP *Standards for general practices* (*4th edition*).

6.5. Limiting disclosure

Where health information must be disclosed to a third party, practices must consider what information is relevant for the proposed purpose. Unnecessary disclosure is unlikely to be expected by patients. In contrast, the disclosure of only the necessary subset of their health information, along with third party access restrictions, is likely to be reasonably expected by patients.

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 has no bearing upon the condition to which the referral relates.

Prior to disclosing any health information, practices should carefully examine their authority for disclosure and seek advice where necessary. It is important practices only release health information stipulated and appropriately authorised (including by subpoena or court order; refer to *Section 6.6 – Subpoenas and disclosure required by law*). Producing an entire medical file in answer to a limited request requiring only certain documents may result in a claim for infringement of a patient's privacy.

Box 2. Case study 2: Limiting disclosure

Laura has commenced her stroke rehabilitation. Her treatment is being led by her GP, who has coordinated her neurologist, the rehabilitation team and the practice nurse. Laura visits her neurologist on regular occasions, and the consultation recommendations are provided to Laura's treating GP, and onto the other healthcare professionals.

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

Later, Laura's treating physiotherapist talks to Laura about her depression. Laura is surprised and embarrassed by this. Although Laura and her healthcare team understood Laura's health information was to be shared, Laura did not expect her physiotherapist to receive information disclosed to her neurologist.

It is reasonable to expect Laura consented to her GP disclosing those aspects of her health relevant to the treating team member. However, Laura's GP did not contemplate that Laura was unlikely to consent to unrelated disclosures, and was unlikely to consent to her physiotherapist becoming aware of her depression. This is likely to 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. Her GP could also have managed what information was collected in her general file, and what was stored separately. Further, to ensure Laura held reasonable expectations of the information disclosure within the members of her healthcare team, Laura's GP could have discussed with Laura what information was collected in her medical file, and how (and with who) this information would be shared.

6.6. Subpoenas and disclosure required by law

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

GPs may also from time to time 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. Unfortunately, GPs are commonly involved in claims for negligence, malpractice, product liability, assault and workers compensation claims.

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 substantiate this position to the court.

GPs have the right to charge reasonable administration charges for the production of these documents. Organisations such as the Australian Medical Association recommends GPs establish a schedule of professional fees for this work and communicate this to requesting solicitors.[10] However given the nature of doctor–patient relationships, it is uncommon for these fee schedules to cover the time and effort involved.

6.7. Transfers of medical records

Privacy legislation does not expressly cover the transfer of medical files between practices, such as during a sale. Care should be taken to ensure transferring patients' records is done in accordance with the relevant laws, (for more information, refer to *Chapter 12 – Sale or closure of a practice*).

6.8. Information transferred overseas

It is particularly important to consider privacy implications in transferring health information outside Australia, as many 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. However, information that is merely stored on an international server, but which only the relevant Australian users are able to access, is not generally considered a disclosure.

It is good practice to seek patient consent before transferring health information outside Australia. 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, including in relation to enforcement of the privacy obligations.

7. Privacy policies

Key points

- Practices must have an up-to-date, patient-focussed policy about the management of their personal information (including health information).
- Privacy policies must accurately reflect the actual procedures of the practice and address certain prescribed requirements.
- A privacy policy must explain:
  - how personal information is collected, used and disclosed within the practice
  - how an individual may access and correct their health information
  - how privacy complaints can be made and how the complaint will be dealt with
  - whether health information is likely to be disclosed overseas and, if so, where.

7.1. External privacy policies

One of the most significant aspects of the March 2014 privacy amendments is the strengthened obligation to maintain an accurate privacy policy.

Practices must make this policy available in both print (available at the practice reception desk and/or seated waiting areas) and, where relevant, electronic versions (available on the practice website). They must be available free of charge and in appropriate mediums or formats. Practices should consider providing a poster, sign or notice indicating the availability of the policy and how to access it, to assist in meeting these obligations.

The precise content of the privacy policy will depend on the individual structure of each practice and the record keeping system used. In each case, however, practices must ensure the acceptable minimum standards of privacy protection and data integrity is achieved.

Establishing a practice policy on health information management will also enable the practice to better manage patient enquiries or complaints concerning their health information.

The RACGP has developed a privacy policy template (refer to Appendix 2 – The RACGP's *Privacy policy template for general practices*) as well as the *Compliance indicators for the Australian Privacy Principles: an addendum to the computer information security standards* outlining relevant steps a practice can take to assist in producing a compliant practice privacy policy.

These resources are available on the RACGP privacy webpage at www.racgp.org.au/ehealth/privacy In using these resources, it is important a practice adapts the template to ensure its accuracy and validity to that practice.

7.2. Internal privacy procedures

As part of the management of health information, it is strongly recommended each practice also has documented internal privacy procedures. This document should outline the practice's procedures for:

- 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 13.3 – Retention and destruction of medical records*).

The internal policy should make specific provision for staff training and education in relation to privacy and confidentiality. All staff must be aware of and comply with a practice's procedures for handling health information.

It is also recommended one person in the practice is responsible for overseeing the implementation and operation of the privacy policies, and acts as a single point of contact for privacy concerns.

7.3. Privacy compliance checklist

This Handbook contains a privacy compliance checklist (*Appendix 1*). Practices can use checklists such as this to determine their level of compliance to the laws governing health information.

This checklist will also assist practices to assess, achieve and maintain good privacy practice.

It is strongly recommended practices apply this or another equivalent checklist to their operations to identify areas requiring practice innovation and improvements, and get appropriate assistance where necessary.

8. A patient's right to anonymity and pseudonymity

Key points

- Wherever it is lawful and practicable 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 makes a diagnosis or can prescribe medications, and GPs are obliged by law to report communicable diseases and child abuse (the latter two being noted exceptions to the operation of these provisions).

In these circumstances, the fact that components of healthcare cannot be provided to anonymous patients should be explained to the patient.

A patient may experience detriment if they chose to remain anonymous. This could occur if patient records of previous tests or treatment cannot be obtained or further tests cannot be conducted. This should be explained to the patient.

However, in circumstances when the practice offers services that do not require identification, the possibility of anonymity and pseudonymity should be integrated into usual practice. A telephone service for general or referral advice or providing general assistance (on issues such as quitting smoking or mental health) are examples of when anonymity or pseudonymity may be used.

9. Patient access to medical records

Key points

- Patients may access all their personal information held by a practice subject to limited exceptions.
- Practices must respond to requests for access within a reasonable period.
- 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 on another
  - it may threaten the life, health or safety of another or the public.
- Other exceptions to providing access apply.
- Refusal to grant access must be communicated in writing with reasons and the process for complaining.

9.1. 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.

Importantly, it may also include patient information stored on other patients' medical records. This commonly occurs in the family setting. Practices must be able to identify those records that contain another patient's personal information, or have the capacity to search relevant medical records where necessary.

9.2. Managing access

Some states impose a legal requirement that access requests must be made in writing. Outside of this, if a verbal request is complex, it may be preferable to request the patient then put it in writing. Some requests may involve collating a significant amount of information from both paper and electronic sources. A written request will permit greater clarity on the information being sought, thus avoiding unnecessary time and expenditure gathering unnecessary information. 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 by 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, which 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.

9.3. Manner of access

Access requests will usually refer to a patient's entire medical record, however requests for particular information may be received, as may requests to receive the information by email, phone or in person.

It is unlikely a practice will be comfortable in providing full 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 practicable, or in a mutually agreed way if not reasonable or practicable.

It is strongly recommended practices consider these reasonableness 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. Practices are entitled to make this assessment and should consider acceptable alternatives. In providing alternatives, the needs of the practice and the patient should each be considered.

In many cases, patient requests for access for health information may be satisfied by way of an up-to-date summary containing all relevant material. However, this may also 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.

9.4. Refusing access

There are several grounds on which a practice may refuse to provide access. It is recommended practices familiarise themselves with these grounds to ensure they are prepared and can defer to the appropriate provision when required.

In particular, practices should consider the risk of distress to other patients. This is particularly acute in the general practice setting, and distress should be considered for all affected parties. 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
- where the possibility of domestic abuse or child abuse exists.

There are several other circumstances where access may be refused. If a GP is considering refusing access, they should obtain professional advice.

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

It is also open to the practice to consider approaching other involved patients to seek their consent to disclosure through an intermediary.

Box 3. 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. As Mary is frail, 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 the materials and the inevitable internet searching that would follow 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 more proximal GP would assist her. Mary agrees and is able to discuss the contents of the record with her local GP in an informed and less stressful environment.

9.5. Access fees

Practices can charge for providing a patient access to their personal information, but not for merely requesting access. The practice should therefore only consider imposing fees 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.

Practices may wish to consider the patient's individual circumstances and their capacity to pay when determining access charges. The circumstances (if any) in which these fees will be waived (eg. on grounds of hardship) should also be considered.

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 practicable within the context of the practice.

9.6. Policy on access

It is within a practice's rights to implement administrative controls around a patient's right of access. It is recommended each practice develops and implements a policy covering these requests. Such a policy would cover:

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

The patient record access policies may be incorporated into the practice's privacy policy (refer to *Chapter 7 – Privacy policies*).

10. Correction of health information

Key points

- A practice must take reasonable steps to correct health information it holds if it is satisfied that information is inaccurate, out of date, incomplete, irrelevant or misleading, or if the relevant patient requests it is amended.
- It is important to verify the identity of the requesting person.
- Correction request must be responded to within a reasonable period.
- Refusals must be communicated in writing with reasons and the process for complaining.
- Practices must take reasonable steps to notify affected third parties of the corrected information.

There is no discretion in the obligation to take steps to correct patient health information – where reasonable, the corrections must be implemented.

Implicit in this requirement is the expectation reasonable care will be taken in the development and maintenance of the records (refer to *Section 13.1 – Maintaining accurate and complete medical records*).

10.1. Notification to third parties

In the event of corrections, practices must ensure they notify third parties to which it disclosed affected health information. Consequently, it is advisable for practices to keep reasonable records of the nature of the health information it discloses and to whom it was disclosed.

10.2. Policy on correction

Similar to access requirements, practices 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 however, the rights concerning correction differ to those for access, and practices cannot force requesting patients to follow a particular procedure or use a particular form. Policies should instead use a pragmatic approach to addressing the requests.

Part 3. Information management relating to general practice

11. The business of general practice

Key points

- It is reasonable to infer consent for the use of health information for internal business practices.
- A practice that rotates GPs (such as by the use of shifts) should make patients aware of this practice.
- Care should be taken when disclosing and collecting health information between related bodies corporate or service trusts.

11.1. The use of health information for business purposes

Patients would reasonably expect their personal information to be used for the secondary purposes of 'normal internal business practice, such as auditing, business planning or de-identifying the personal information'.[3] This expectation will likely extend to practice staff having access to patient health information for that purpose.

It will also extend to billing or debt-recovery purposes (confidentiality should be maintained and care and discretion exercised), however advice confirming this should be sought prior to a particular disclosure to a third party service provider engaged for this purpose.

Accordingly, specific consent covering these practices is not needed.

11.2. Group practices

In group practices each GP technically has access to all patient records, regardless of whether they access them. In those 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 also 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 health services by the practice, it is still a disclosure requiring authorisation under the privacy laws. It is also possible to infer consent when a patient has sought a consultation with the new GP.

11.3. Transfers between related bodies corporate

There is no express permission for the transferral of health information between related bodies corporate or service trusts (such as exists for basic personal information). Such sharing of information is simply a disclosure and falls under the general rules.

Corporate practices and practices employing service trusts should therefore ensure any transfer satisfies an exception to the collection and disclosure (one discloses, the other collects) requirements to avoid interfering with a patient's privacy. Ideally patient consent to this practice should be obtained.

12. Sale or closure of a practice

12.1. Privacy considerations

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

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.

However, the Privacy Act is not particularly well adapted to the sale or transfer of the medical records themselves. This would occur for a sole practitioner or an unincorporated practice, where the sale involved only the transfer of the general practice business (the medical files being one asset of that business).

Although the transferring records contain health information, it is unclear whether consent is required from each patient whose medical record is being transferred. Some organisations suggest the transfer of medical records in this setting 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 expressly or impliedly) 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 also 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 also be appropriate.[11]

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

Health record legislation usually considers the retention requirements for health records to be satisfied by their transfer in this manner.

12.2. Deceased GPs

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

12.3. Health record legislation

GPs should note additional requirements for the transfer or closure of a general practice exist under health records legislation.

For example, Victoria and the ACT require publishing a notice in a local newspaper stating that the practice is closing or being sold, detailing the manner in which the practice proposes to deal with the medical records. Notice periods of 21 and 30 days from publication, respectively, apply before the GP may effect the transfer or closure.

Where necessary, advice should be sought.

13. Medical records

Key points

- Practices must ensure the health information they collect, use or disclose is relevant, accurate, up to date and complete.
- Practices 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.

13.1. Maintaining accurate and complete medical records

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

Practices should consider using a recall system (subject to patient consent) to ensure patients are regularly seen and medical records are maintained accurately and contain up-to-date information. Considerations of the marketing aspects of such a system should be considered (refer to *Chapter 14 – Marketing*).

Further information regarding completeness and accuracy of patient health records refer to *Standard 1.7 Content of patient health records* in the RACGP *Standards for general practices* (4th edition) and the RACGP's *Quality Health Records in Australian Primary Care resource* available at www.racgp.org.au/your-practice/business/tools/support/qualityhealthrecords

13.2. Ownership

Patients do not own their medical record. Ownership is determined by the structure of each practice, and the nature of its engagement of GPs.

As a series of generalities:

- Sole practitioners retain full ownership over their medical records.
- Contract and employee GPs are likely to be creating medical records for their 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 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 interaction between the GPs and whether a common understanding existed.

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 also recommended that appropriate advice be sought prior to entering into any such agreement.

Despite holding the proprietary rights, GPs – as for all medical practitioners – are required under the Medical Board of Australia's Code of Conduct to promptly facilitate the transfer of health information when requested by a patient.[7] It is unclear, however, whether fees may be charged prior to this transfer, and seeking advice is recommended.

13.3. Retention and destruction of medical records

Practices should retain health information as required, and in accordance with state, territory and Commonwealth legislation.

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.

The ACT, NSW and Victoria have each enacted legislation regulating the retention of records. Each of these jurisdictions require medical records to be retained until a child turns 25, and for adults for 7 years from the date of the provision of the last health service.

Under some state and territory legislation, laws regulating litigation prevent the destruction of any record that is likely to be involved in legal proceedings. In addition to any other regulation, GPs should retain their records until the relevant limitation periods have expired. Appropriate advice on the current limitation periods should be sought where necessary and relevant.

In the case of health information collected by treating GPs, it is appropriate to retain this information indefinitely so that it is available, if necessary, to assist with the patient's future diagnosis and treatment.

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

13.4. De-identification

Practices may choose to permanently de-identify health information rather than destroy it. Care must 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. The process must be sufficiently thorough to ensure enough identifying information is deleted or destroyed to ensure the future anonymity of the medical record.

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. The relevant NHMRC guidelines specify a minimum of five sets of individual's data in each cohort.[12]

14. Marketing

14.1. Prohibitions on direct marketing

Key points

- Health information must not be used or disclosed for the purpose of direct marketing without patient consent.
- Practices must currently obtain patient consent to ordinary services with commercial aspects, such as vaccinations.
- The sending of unsolicited commercial communications through electronic mediums or to registered telephone numbers is ordinarily prohibited.

General practices may not ordinarily consider themselves to engage in marketing activities, particularly not in contravention of the Privacy Act. However, any promotion of the services of a practice, even as scheduled reminders or as part of good clinical practice, may constitute an interference with privacy. This is particularly true with direct marketing in the context of health information.

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. However, the Privacy Act appears to have little regard for preventative health measures; practices should note many day-to-day clinical initiatives may inadvertently breach these laws.

In particular, the Privacy Commissioner currently considers letters that use or disclose personal information promoting commercial services, for example to advise patients about flu vaccinations, are likely to constitute direct marketing.[13] The concepts of best practice and public health initiatives do not appear to factor into this assessment.

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

To avoid breaching the marketing provisions, practices must obtain patient consent. To achieve this, practices may consider:

- requesting consent (via opt-in or opt-out mechanisms) on patient registration sheets
- asking for consent as patients present to the practice
- undertaking a directed consent campaign by phone, email or mail.

The Privacy Commissioner considers a marketing campaign designed to obtain consent to subsequent practice mailouts is likely to be acceptable.[13] This appears to be on the basis such a mailout would not use health information – a key distinction or promote goods or services. Whilst care must be taken to ensure such a campaign does not breach other privacy laws, it is unlikely such a campaign will breach the *Spam Act* or the *Do Not Call Register Act* (refer to *Section 14.2 – The Spam Act and Do Not Call Register*).

Failing the obtaining of patients' consent, GPs must ensure they have adequate procedures in place to ensure marketing messages are not sent to the relevant patients.

14.2. The Spam Act and Do Not Call Register

The Privacy Act defers to the operation of the *Spam Act* and the *Do Not Call Register Act*, so that where they operate, the Privacy Act is silent.

As a general rule, practices are prohibited from sending unsolicited communications 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 SMS reminders.

A comprehensive and broad set of circumstances leading to these prohibited outcomes applies, effectively capturing both direct and indirect sales methods.

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

15. Information security

Key points

- Practices must take reasonable steps to protect the health information and other information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.
- Cross-border disclosures must be preceded by reasonable steps to ensure no privacy breaches will occur.
- Practices should download and continually refer to the CISS to ensure best practice is followed for information security.

15.1. Computer and information security standards (CISS)

The CISS is a highly recommended resource for practices to assist compliance with good security practice and to demonstrate implementation of such practices.

The CISS incorporates changes to the Australian legislation and the directives of the Privacy Commissioner. It has been designed to assist general practices and other office-based healthcare organisations to meet their professional and legal obligations in computer and information security.

In particular, the CISS provides general practice with a framework for evaluating risks, and guidance and solutions to improve competency and capacity in computer and information security.

The CISS resource is available from www.racgp.org.au/your-practice/e-health/protecting-information/ciss

15.2. Risk assessments

Organisations need to assess their security risks and respond appropriately to protect the integrity of their information systems and networks. Information technology systems inherently increase the risk of unauthorised disclosure, and the ease of mass-distribution must also be acknowledged.

Adopting appropriate information security measures is vital to ensure health information is protected,[14] and these should cover information systems for storing, processing and transmitting information.

The protective measures will depend on the circumstances and risks involved. Practices should develop and implement appropriate policies and procedures specifying which staff have access to health information and under what circumstances. It is also 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.[14]

It is important to recognise and implement security measures for information stored electronically. These may include password protection, automatic log offs, log file/electronic audit trails, firewalls, malware and virus protection, checking facsimile numbers before sending personal information and ensuring the encryption of data for high risk transmissions.[15]

For further information and templates for performing a computer and information security risk assessment, refer to *Standard 2: Risk assessment* in the CISS.

15.3. Electronic transfer of information

The use of electronic means for transferring health information (email and fax) make it easier to transfer large quantities of information. The privacy principles governing the electronic transfer of information do not differ from other modes of transferring health information – the laws regarding the use and disclosure of that information still apply.

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. Professional advice should be sought to address any further queries or comments.

For further information on sharing information electronically, refer to *Standard 12 – Security for information sharing* in the CISS.

15.4. 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 rise of email and social media in particular has led to the release of various social media guidelines.

Of note, the March 2014 release of the Australian Health Practitioner Regulation Agency's *National Board policy for registered health practitioners: Social media policy*'[16] is an adjunct to the Medical Board of Australia's Code of Conduct and should be read concurrently. Its provisions apply to all registered health practitioners.

Practices need 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 over 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 (SMD) should be used between practices with compatible encryption processes.

15.5. Secure destruction and de-identification

Unnecessary health information should be destroyed securely to prevent unauthorised access. Prior to destruction, consideration need be given to the relevant retention requirements under any applicable health legislation (see *Section 13.3 – 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 is problematic and may not be possible given electronic storage methods and software systems used in general practice. 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 *Effective solutions for e-waste in your practice*, available at www.racgp.org.au/your-practice/e-health/protecting-information/e-waste

Box 4. Case study 4: International consultation

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

Dr Murray is not comfortable in making an initial diagnosis. However, during the consultation, Dr Murray recalls a seminar he attended that discussed very similar wounds. The seminar was led by a professor from Canada.

Dr Murray considers it appropriate to refer the wounds to the professor, and so takes several photographs. 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 applying in Canada
- sought the professor's assurance the photographs would be examined in strict confidence, prior to sending them.

15.6. Security policy

To encourage an organisational culture that respects privacy and confidentiality, it is recommended practices develop and implement an information security policy. The implementation of an information security policy will assist in ensuring organisational systems used for processing and storing, or transmitting, personal information are managed and protected appropriately.[17]

To be effective, it is essential security policies are monitored and reviewed on a regular basis, and that the relevant staff are aware of the policy and procedures.[3]

The CISS provide comprehensive advice regarding the development of an access/security policy under *Standard 3 – Information security policies and procedures*, refer to www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-3

16. Data breach

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
- a practice mistakenly providing personal information to the wrong person (for example, sending a patients' personal details and/or health information to the wrong address)
- a practice being deceived into improperly releasing the personal information of another person.[18]

Under the Privacy Act, practices are obligated to take reasonable steps to protect personal information they hold.

Notifying patients of any data breach is an important element of fulfilling security of personal information obligation under the APPs. Although mandatory data breach notification laws (*Personally Controlled Electronic Health Records Act 2012*) only apply to national eHealth records at present, the RACGP strongly recommends voluntary data breach notification for breaches of any patient health information.

Data breach notification is considered best privacy practice as it ensures the highest chance of compliance with the privacy laws, promotes openness and transparency about privacy practices, assists in restoring control over personal information, and rebuilds patient's trust. It is also recommended by the Privacy Commissioner and may eventually become a legal requirement under the Privacy Act.[19]

The RACGP has developed a 'Data incident/breach report template' specifically for a practice to use in the event of a data breach. It outlines the steps to follow in the event of a breach and the relevant follow up actions to take. The template is available as part of the CISS and is available at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/appendices/appendix-c

Further information is available in CISS under S*ection 2.9 – Data breach response and recording*.

17. Healthcare identifiers

Key points

- Healthcare identifiers generated by the clinical desktop system should not include any information from:
  - the patient's name
  - date of birth
  - address
  - telephone number
  - Medicare number
  - any identifier assigned by a government agency
  - any other information that could identify the person.
- Practices 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.

A healthcare identifier is a unique number assigned to healthcare consumers, healthcare providers and organisations providing health services. For example, an Individual Healthcare Identifier (IHI) is a unique identification number for individuals who seek healthcare. An IHI 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 (such as URLs) instead of names is useful to protect privacy. However, care should be taken to ensure the adopted identifier system does not use any prohibited details. In addition, the identification number should not reveal any health information about the patient.

18. Health research

Key points

- Patient consent should be sought prior to the use or disclosure of their health information for health research.
- Health information may be collected, used and disclosed for health research without patient consent if:
  - it is necessary for research, the analysis of statistics related to public health and safety, or the management, funding or monitoring of a health service
  - obtaining consent is impracticable
  - the research's purpose cannot be satisfied using de-identified data, and
  - the collection, use or disclosure is either required by or under law, or in accordance with rules established by competent health or medical bodies or guidelines approved by the Privacy Commissioner.
- Health research using human participants can only be conducted with ethical approval.

Health research is an important component of general practice in Australia. Practices are encouraged to participate in research both within their own practice and through reputable external bodies.

The legal and ethical principles governing health research using human participants make it clear 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 March 2014),[20] and the TGA's *Australian Clinical Trial Handbook*.[21]

18.1. Considerations when participating in health research

Patients should be made aware the practice may use their 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 identifiable data sets after the relevant information has been extracted from the patient records. In any event, all research records should be de-identified at the earliest possible time consistent with the proper conduct of the research.

18.2. Interaction between the Privacy Act and health research

In addition to privacy obligations, practices must also comply with all ethical requirements imposed for research conducted on human participants. It is important researchers understand these two sets of requirements impose separate obligations that must each be complied with (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.

Practices must ensure they have the right to collect, use and (where appropriate and relevant) disclose health information. The simplest manner of doing so is through obtaining participant consent.

The Privacy Act also leaves open the option of relying on secondary purposes, being the reasonable expectation of use in health research (refer to *Section 6.1 – 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.

References

1. National Statement on Ethical Conduct in Human Research 2007 (Updated March 2014). The National Health and Medical Research Council, the Australian Research Council and the Australian Vice-Chancellors' Committee. Commonwealth of Australia, Canberra.
2. Privacy Act of 1988, [statue on the Internet]. c2013. Available at www.comlaw.gov.au/Details/C2014C00076 [Accessed 26 June 2014].
3. Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines [Internet].2014. Available at www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines [Accessed 26 June 2014].
4. Health Records Act of 2001, VIC [statute on the Internet]. c2001. Available at www.legislation.vic.gov.au [Accessed 26 June 2014].
5. Health Records and Information Privacy Act of 2002, NSW [statute on the Internet]. c2002. Available at www.legislation.nsw.gov.au/ [Accessed 26 June 2014].
6. Health Records (Privacy and Access) Act 1997, ACT [statute on the Internet] c2014. Available at www.legislation.act.gov.au [Accessed 26 June 2014].
7. Good Medical Practice: A Code of Conduct for Doctors in Australia [Internet]. Melbourne: Medical Board of Australia; 2014. Available at www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx [Accessed 26 June 2014].
8. Office of the Australian Information Commissioner. Public Interest Determination 12. Canberra: Office of the Australian Information Commissioner, 2002.
9. Office of the Australian Information Commissioner. Information Sheet 25 (2008): Sharing health information to provide a health service. Canberra: Office of the Australian Information Commissioner, 2008.
10. Frequently Asked Questions – Fees [Internet]. Canberra: Australian Medical Association. Available at https://ama.com.au/frequently-asked-questions-fees [Accessed 26 June 2014].
11. Office of the Australian Information Commissioner, Private Sector Information Sheet 16 – A Application Of Key NPPs To Due Diligence And Completion When Buying And Selling A Business. Available at www.oaic.gov.au/images/documents/migrated/migrated/IS16_02.pdf [Accessed 26 June 2014].
12. National Health and Medical Research Council. Guidelines for Health Practitioners in the Private Sector. 2009. Canberra: National Health and Medical Research Council, 2009. Available at www.nhmrc.gov.au/guidelines/publications/e96 [Accessed 26 June 2014].
13. Personal communication, the Office of the Australian Information Commissioner, 11 April 2014.
14. Office of the Australian Information Commissioner. Guide to information security. Canberra: Office of the Australian Information Commissioner, 2013. Available at www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security [Accessed 26 June 2014].
15. The Royal Australian College of General Practitioners. Computer and Information Security Standards (Second Edition). Melbourne: RACGP, 2013.
16. Social Media Policy [Internet]. Canberra: Australian Health Practitioner Regulation Agency; 2014. Available at www.medicalboard.gov.au/Codes-Guidelines-Policies/Social-media-policy.aspx [Accessed 26 June 2014].
17. The Royal Australian College of General Practitioners. Standards for general practice (4th Edition). Melbourne: RACGP, 2010.
18. The National e-Health Transition Authority. Privacy Blueprint for the Individual Electronic Health Record. Report on Feedback. Canberra: The National e-Health Transition Authority, 2008.
19. Office of the Australian Information Commissioner. Data breach notification guide. Canberra: Office of the Australian Information Commissioner, 2013. Available at www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches#_Toc301281667 [Accessed 26 June 2014].
20. National Statement on Ethical Conduct in Human Research 2007 (Updated March 2014). The National Health and Medical Research Council, the Australian Research Council and the Australian Vice-Chancellors' Committee. Canberra: Commonwealth of Australia, 2007.
21. Australian Clinical Trial Handbook [Internet]. Canberra: Therapeutic Goods Administration; 2006. Available at www.tga.gov.au/pdf/clinical-trials-handbook.pdf [Accessed 26 June 2014].

Appendices

Appendix 1. Compliance checklist

This checklist should be used as a guide only, and does not exhaustively describe the complete list of activities that should be undertaken when assessing compliance. If you are unsure whether your practice complies in a particular area then you should tick 'no' and focus on the relevant actions.

		Privacy Compliance Indicators	Y	N
1	Quality and content of medical records	*Does the practice have processes in place to ensure accurate and up to date data during information collection, use and disclosure?*		
2	Patient consent	*Does the practice have a procedure for identifying when consent should be sought, and for recording consent? Do practice staff understand the requirements surrounding this?* Consent may be sought for primary and secondary uses provided they are adequately stipulated. Although inferred and implied consent may be relied upon in certain circumstances, express consent (a signature or a documented positive response to a question) should always be sought.		
3	Collecting health information	*Does the practice have defined processes to know when, what and how the practice collects health information? Does the 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 information and computer systems to handle the tasks.		
4	Patient access to personal information	*Does the practice have procedures for handling patient requests for access to, and correction of their information?* These procedures include how to assess requests, refusal procedures and administration charges.		
5	Use and disclosure of personal information	*Does the practice have in place a process for patients to opt-in or opt-out of marketing opportunities?*		
6	Medical research	*Does the practice comply with the GP Data Governance Principles for secondary use of data?* This includes procedures for how to deal with requests for data for secondary use.		
7	Quality improvement and continuing professional development	*Does the practice have procedures to record occurrences of patient information use for quality improvement and continuing professional development?*		
8	Information security and data retention	*Does the practice comply with the RACGP CISS (to at least the minimum level defined for general practice compliance) to ensure the safe and proper protection of information held in the practice?* 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.		

		Privacy Compliance Indicators	Y	N
9	Document retention	*Does the practice have a process for document classification, retention, destruction and de-identifying patient information?*		
10	Healthcare provider identification	*Does the practice have a process for identifying the need for, and recording, the consent of a healthcare practitioner?* This occurs when sharing information identifies the practice, even though the patient health information may be de-identified.		
11	Health identifiers	*Do practice staff understand the restrictions on use of healthcare identifiers?* This will include requirements of the Health Identifiers Act and usage of the Personally Controlled Electronic Health record if the practice is engaged in this initiative.		
12	Establishing a practice privacy policy	*Does the practice have an up to date, accurate, accessible, and freely available privacy policy?*		
13	Data breach notification plan	*Does the practice have processes in place to detect, manage, and report data breaches?*		
14	Demonstrated compliance check	*Has the practice undertaken the RACGP Compliance Indicators for the APP check?* This provides demonstrated evidence of compliance with the Australian Privacy Principles and is available at www.racgp.org.au/download/Documents/Standards/cis-appcompliance.pdf		

Appendix 2. The RACGP's Privacy policy template for general practices

Download the RACGP's *Privacy policy template for general practices* from www.racgp.org.au/your-practice/ehealth/protecting-information/privacy/

RACGP | *Privacy policy template for general practices*

The Royal Australian College of General Practitioners (the RACGP) has developed a privacy policy template for general practices to adapt, for compliance with the requirements of the Australian Privacy Principles (APPs). It is important each practice uses this template as a guide and adapts its content to their individual procedures.

This template covers:

- practice procedures
- staff responsibilities
- patient consent
- collection, use and disclosure of information
- access to information.

The template is designed to communicate to patients how a practice manages personal information and to complement other practice policies such as complaint resolution and breach notification procedures. The sections in red text are for you to revise and adapt to the specific procedures of your general practice.

This template was developed with assistance from the Office of the Australian Information Commissioner (OAIC) and was current at time of publication.

For more information on privacy visit www.oaic.gov.au, or for privacy policies for GPs, visit www.oaic.gov.au/privacy/privacy-resources/training-resources/privacy-policies-for-gps

Make your policy freely available for your patients so they know that it exists and they can access it, eg display at your practice reception and on your website if you have one, make reference to it in your registration forms and other forms or notices.

This policy should be reviewed regularly to ensure it remains applicable to current practice procedure and legal requirements.

Appendix 3. Advice on compliance

Organisation	Website	Phone
Office of the Australian Information Commissioner	www.oaic.gov.au	1300 363 992
Information and Privacy Commission – NSW	www.ipc.nsw.gov.au	1800 472 679
Office of the Information Commissioner – QLD	www.oic.qld.gov.au	(07) 3234 7373
Office of the Information Commissioner – NT	www.infocomm.nt.gov.au	1800 005 610
Office of the Victorian Privacy Commissioner - VIC	www.privacy.vic.gov.au	1300 666 444
Human Rights Commission – ACT	www.hrc.act.gov.au	(02) 6205 2222
Privacy Committee of South Australia - SA	www.archives.sa.gov.au/privacy/committee.html	(08) 8204 8773
Ombudsman Tasmania – TAS	www.ombudsman.tas.gov.au	1800 001 170

Appendix 4. Resources

- The RACGP Standards for general practices (4th edition), www.racgp.org.au/standards
- The RACGP Standards for general practices offering video consultations: an addendum to the RACGP Standards for general practices (4th edition), www.racgp.org.au/your-practice/e-health/telehealth/gettingstarted/standards
- The RACGP Computer and Information Security Standards (2nd edition) 2013, www.racgp.org.au/ehealth/privacy
- Compliance indicators for the APP: an addendum to the Computer and information security standards (2nd edition), www.racgp.org.au/ehealth/privacy
- Data Privacy within the context of secondary use of data from general practice, www.gpdgc.org.au/papers.html

RACGP

Healthy Profession.
Healthy Australia.