CLINICAL GUIDELINE

Accessing patient health records

This Guideline provides information to members about accessing patient’s health records. It should not be used as a substitute for statutory responsibilities and optometrists must ensure that they comply with relevant laws.

The legal framework

From time to time, optometrists may be asked by a variety of people for access to information from a patient’s health records. These requests may come from the patient themselves and other third parties such as family members, from police or the courts.


Optometrists practising in New South Wales, the Australian Capital Territory and Victoria are also required to abide by state privacy legislation when practicing privately. Where relevant this Guideline provides information for optometrists practising in these locations.

The relevant legislation is:

Commonwealth: Privacy Act 1988 and Australian Privacy Principles (APPs)

Victoria: Health Records Act 2001

New South Wales: Health Records and Information Privacy Act 2002

ACT: Health Records (Privacy and Access) Act 1997

In the event of an inconsistency between a State or Territory law and a Commonwealth law, the Australian Constitution provides that the Commonwealth law will prevail.1

---

1 Letter from Office of Privacy Commission to OAA dated 15 October 2010.
## Contents

Checklist for Accessing Patient Records.......................................................................................... 3

1. Attachment A: Model Privacy Policy .......................................................................................... 7

2. Attachment B: Exceptions to patient request for access: APP 12. ........................................ 10

3. Attachment C: Guidelines to recovery of reasonable costs .................................................. 11

4. Attachment D: APP 6 & 7 exceptions ....................................................................................... 12

5. Attachment E: Common third party requests for accessing information............................... 15
Checklist for Accessing Patient Records

☐ **Anticipate patient requests to access their records**

Federal privacy laws require that patients have access to their health records. This right is also mirrored in state and territory laws. The law is not prescriptive in the form of access to be provided to an individual. Typically patient requests may be to:

- have a copy of the records;
- inspect their records; and
- have a copy provided to a third party (e.g. a solicitor).

A patient is not obliged to tell an optometrist why they want to access their records and optometry practices must respond to any request within a reasonable period and give access in the manner requested by the individual, provided it is reasonable and practicable to do so.

☐ **Develop a policy on accessing health records**

Every optometrist practice must, in compliance with Australian Privacy Principle (APP) 1, maintain a privacy policy (APP privacy policy) which sets out the practices policies, procedures and systems on handling personal information and to make this available to anyone who requests it. An example of a policy covering access to health records is at Attachment A, comprising the minimum information that must be maintained as per APP 1.4. Practices need to take reasonable steps to make its privacy policy available free of charge upon request. It is common for a privacy policy to be made available via a practice website.

Practices must take reasonable steps to implement practices, procedures and systems that will ensure the practice complies with the APPs including what processes ought to be followed should a request by a patient is made to access their health records during the optometrist’s absence when there may be another optometrist or a locum in the practice.

☐ **Best practice for patient requests and identity checks**

It is advisable to have the request for access from the patient in writing, although there is no legal requirement for a request to be in writing. In order to conform with APP 11, which requires an optometrist to take reasonable steps to protect personal information they hold from misuse and loss and from unauthorised access, interference, modification or disclosure, a patient’s identity should be checked to ensure that the person requesting the information is actually the patient (ACT, NSW and Victorian legislation requires this also).

The manner in which an optometry practice approaches satisfying APP 11 will depend on office practice. An optometry practice may already have identity validation procedures in place as part of their normal business practice and this may be sufficient.

☐ **Respond in a reasonable time**

An optometrist should respond to the request in a reasonable time. Federal privacy law does not define what a reasonable time is however in ACT, an optometrist must respond in 14 days; and in both NSW and Victoria, an optometrist must respond within 45 days.
A practice can charge a fee for providing access to health records

For optometrists practising in Queensland, Northern Territory, Western Australia, South Australia and Tasmania, federal privacy laws permit charging for access to health records. Recommended fees are not specified other than costs ought to be reasonable, not excessive and should not prevent patients in financial hardship from exercising their legal right to access information held about them. At the same time, the cost of giving access should not create an unreasonable burden on health service providers. The Privacy Commissioner has provided some advice to APP entities which can assist practices set reasonable fees which is set out in Attachment C.

Victorian legislation allows optometrists to seek reimbursement for accessing health records. Fees may only be charged for granting access under the Act where this is permitted by the Act itself or the regulations and there is a maximum fee level set under the Act. More information about the Act can be located at: www.health.vic.gov.au/healthrecords

ACT legislation allows a fee to be charged if a copy of the health record is required or the health record is explained to the patient. The legislation sets no specific level for the fee.

NSW legislation allows fees to be charged (section 27 of the Health records and information privacy Act 2002) but sets no rules as to the level.

Limited circumstances when a request can be refused

Optometrists may deny a request from a patient to access their own health records in certain limited circumstances. These occasions would arise infrequently, particularly in optometry. Federal Privacy Law APP 12.3 lists the limited circumstances where a request may be denied. A copy of these exceptions is located at Attachment B. These circumstances are mirrored in ACT, NSW and VIC legislation.

Optometrists are not required to agree to a patient’s request to access to their records where providing access to health information would pose a serious threat to the life, health or safety of any individual.

- The threat may be to the patient, practitioner, relative, staff or other patients.
- The threat may be to physical or mental health.

The Federal Privacy Commissioner has provided detailed advice about how to deal with these limited circumstances. This information can be accessed at www.oaic.gov.au.

Under Federal Privacy laws, APP 12.5, an optometry practice must consider using an intermediary to allow limited access to information that would otherwise be denied to an individual by one of the exceptions under APP 12.3.

An intermediary is a person or persons acceptable to both the optometry practice/optometrist and the individual asking for access. The role of the intermediary is to enable an individual to get access to

3 Section 32 of the Health Records Act 2001
4 Section 10(5) of the Health Records (Privacy and Access) Act 1997.
and have the content of the personal information explained where access would otherwise have been denied. More information on the use of intermediaries may be found at www.oaic.gov.au.

☐ What to do when denying a request

If information is denied because of APP 12.3 an optometrist must give the individual written notice with an explanation why the information request is refused and the mechanism to complain about the refusal.

The explanation should include which exception under APP 12.3 the optometrist is relying on to refuse access. Having the explanation in writing may assist in the patient's understanding the reasons for the refusal and help avoid unnecessary complaints and also provides the optometrist with an accountability trail in the event of a complaint.

☐ Releasing information without patient consent

Other than when a patient has consented to the use or disclosure of health information, under the Privacy Act an optometrist may generally only use or disclose their patients’ health information without consent under the following circumstances:

1. For the primary purpose for which it was initially collected. The context in which optometrists collect health information will be important in determining the primary purpose for which the health information can be used or disclosed.

The primary purpose for an optometrist to collect information would be to diagnose and treat a particular condition or set of symptoms related to the eye. E.g. an optometrist speaking with an ophthalmologist about the patient’s symptoms. In order to avoid doubt, an optometrist is advised to inform the patient about the likely uses and disclosure of the information when it is being collected.

2. For another directly related purpose the individual would expect, such as for:
   a. prescription purposes;
   b. Medicare purposes;
   c. health fund claiming purposes
   d. case conferencing and multi-disciplinary team care;
   e. hospital admission; or
   f. referral to a specialist.

An optometrist may use or disclose health information if the secondary purpose for using or disclosing the information is directly related to the primary purpose and it is within the patient's reasonable expectations. A patient's reasonable expectations are what a reasonable individual with no special knowledge of the health sector would expect to happen to their health information in the given circumstances. Those expectations are likely to be informed by, amongst other things, what they are told may happen to their health information during the course of the consultation. In some cases, an

---

6 For further information see Chapter 6, APP Guidelines at www.oaic.gov.au/applying-privacy-law/app-guidelines/ and APPs 6 and 7 are useful in assisting an optometrist determine the primary purpose.

7 For more information, please access Private Sector Information Sheet 25 – Sharing Health information to provide a health service at www.oaic.gov.au.
optometrist may wish to canvass with the patient the likely scenarios when their health record needs to be disclosed to a third party is there is any doubt the patient would disagree.

3. Where disclosure is required or authorised under law, such as the issuing of a subpoena or mandatory reporting such as driver’s licence reporting.

4. Where disclosure is reasonably necessary for one or more enforcement related activities, conducted by, or on behalf of, an enforcement body.

5. Where disclosing information is considered under a permitted general situation (under section 16A of the Privacy Act) or permitted health situation that exists (under section 16B of the Privacy Act).

Permitted general situation include:

a. Where disclosure would lessen a serious and imminent threat to someone’s life, health or safety.

b. Where suspected unlawful activity or serious misconduct is noted

c. Disclosure to a person responsible for the patient e.g. parent, guardian where the patient is unable to provide consent.

d. Disclosure of a communicable disease related to public safety.

Permitted health situations include:

a. Disclosure by and organisation if necessary for research or statistical analysis if it is impractical for the organisation to obtain consent and they believe the recipient of the health information will not disclose the information, or personal information derived from that information

b. Disclosure by an organisation of genetic information about an individual of the organisation reasonable believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative

A full list of the exceptions is found at Attachment D. Attachment E includes some common third party requests.
Attachment A: Model Privacy Policy

Model Privacy Policy

[ ] Practice is committed to protecting and preserving the privacy rights of our patients.

[ ] Practice collects information from our patients in the course of providing optometry services and products *(strike out if not applicable).*

[ ] Practice is bound by the Federal Privacy Act 1988 and the Australian Privacy Principles. This policy sets out how [ ] Practice treats personal information of our patients. It is available to all members, staff and the public, free of charge and further information on our information handling processes is available on request.

Collection

[ ] Practice / we collect(s) and uses personal information of patients to provide eye care and related health care needs. The specific uses to which [ ] Practice puts patients’ personal information include to treat, coordinate and implement care plans for the treatment of eye care or related health care needs. Generally speaking most personal information is collected from the patient.

The type of information [ ] Practice collects about a patient includes:

*At the time of the appointment:* name and contact details to make the appointment.

*At the time of the consultation:* Patient’s name, address, date of birth, email address, gender, spoken languages, eye disease history including family eye disease history. The information collected will be relevant to the clinical needs of the patient.

At times patient information is acquired through a third party, such as Medicare, Department of Veterans Affairs or a health fund. This information only relates to eligibility for services provided by those bodies, and is not used except in office, for third party billing procedures.

Use and Disclosure of information

[ ] Practice will use personal information to provide an eye care related services or product.

[ ] Practice may disclose personal information about patients to third parties for the purpose for which that information was collected and also for related purposes that could reasonably be expected by the patient.

Clinically relevant patient information may be shared with other relevant health care practitioners for example, a referral to an ophthalmologist or General Practitioner with the patients consent.

Patient information may also be used to contact the patient to inform them about the need for a check-up or practice relocation. A patient may elect not to be contacted in this matter if they so wish.

Information may also be required to be released to courts, tribunals or regulatory authorities as agreed or authorised by law. In most cases this will require a court to order the release of the information, although information may also be released when the optometrist believes that this is necessary to prevent a serious and imminent threat to a person’s life, health or safety, or to public health and safety. Some information, such as the patient’s identity and the type of consultation provided, may be released in order to allow Medicare benefits to be claimed. Commonwealth legislation also allows
records to be inspected by representatives of the Medicare Australia in order to investigate whether Medicare benefits have been paid appropriately.

The Practice is unlikely to disclose personal information to an overseas recipient with the exception of such matters that arise in the course of providing eye care with the consent of the patient. An example would be the purchase of a specialty optical appliance for a patient that is unavailable in Australia.

Data quality

[ ] Practice will take reasonable steps to ensure that the personal information we collect from patients is accurate, complete and up-to-date. [ ] When a patient informs the Practice of any inaccuracy, it will be corrected as soon as possible.

Data Security

[ ] Practice will take all reasonable steps to ensure that the information we hold about a patient is protected from misuse, loss and unauthorised access, modification or disclosure.

(consider outlining security measures for patient records eg electronically stored, pass word protected, encrypted)

Record cards are kept for each patient. The only people who have access to patient records are the optometrists involved in the care of the patient, and practice staff, who need access for purposes such as optical dispensing and billing. No unauthorised persons are permitted to access the records. Practice staff are bound by confidentiality clauses in the terms of their employment.

Practice will also take reasonable steps to destroy information held about a patient once that information is no longer required, is not contained in a public record or the Practice is required to maintain under an Australia Law or court order.

Access to and correction of personal information

Patients may request access to, and ask [ ] Practice to make corrections to, the personal information that Practice holds about them.

[ ] Practice will, on request, provide a patient with access to his or her personal information, unless there is an exception which applies under relevant privacy laws. If we refuse to provide access to the information, we will provide reasons for the refusal and inform the patient of any exceptions relied upon.

A suitable time will be arranged for a viewing, with an optometrist available to interpret the information, or explain any terms used. A fee may be charged for this service. A response to a question for access must be provided within a reasonable time (14 days in ACT; 45 days in Victoria and NSW).

Under some circumstances, the Practice may refuse to provide access to the information held about a patient. This will only occur where releasing the information would pose a serious threat to the health of the patient or another person, would unreasonably impact on the privacy of another person, would interfere in legal investigations or other proceedings, or would otherwise be illegal.

The physical/electronic record and the intellectual property contained in it remain the property of the optometrist and/or the practice at all times.
Identifiers

[ ] Practice will not adopt, use or disclose any identifier assigned to a member by a government agency, except where required by law. Medicare numbers will only be used for the purposes of claiming Medicare benefits.

Anonymity

It is a patient's right to be dealt with anonymously, provided that it is lawful and practicable. [ ] Practice will try to accommodate this wherever possible. However, it may not be possible for the Practice to provide optimal services without access to a patient's personal information.

Trans-border data flows

[ ] Practice will not transfer data about the patient to a recipient in a foreign country unless the data will receive at least the same level of protection as in Australia, unless the patient gives their permission for the practice to do so.

Sensitive information

[ ] Practice will not collect sensitive information about the patient without the patient’s consent, except where collecting such information is required by law, or where the patient (or their representative) cannot give consent and the information is needed to provide a health service to the patient or to reduce a threat to the life or health of another person.

‘Sensitive information’ is defined as information about a person’s health, their racial or ethnic origin, their political, religious or philosophical beliefs and affiliations, their membership in professional or trade associations or unions, their sexual preferences or practices, or their criminal record.

Requests, Complaints or Questions

If a patient wishes to gain access to his or her personal information, make a complaint about a breach of his or her privacy or have any questions on how his or her personal information is collected or used, the patient can forward his or her request, complaint or question to the address below:

(INSERT practice details including relevant contact person eg practice manager)

[ ] Practice will respond to a patient’s request, complaint or question within a reasonable time (14 days in ACT; 45 days in Victoria).

Patients may also make a complaint to the Office of the Australian Information Commissioner (OAIC) about the handling of their personal information as covered by the Privacy Act. Information on how to made a complaint to the OAIC can be found at www.oaic.gov.au or 1300 363 992.
Attachment B: Exceptions to patient request for access: APP12.3

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

a. the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
b. giving access would have an unreasonable impact on the privacy of other individuals; or
c. the request for access is frivolous or vexatious; or
d. the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or
e. giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
f. giving access would be unlawful; or
g. denying access is required or authorised by or under an Australian law or a court/tribunal order; or
h. both of the following apply:
   i. the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
   ii. giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
i. giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
j. giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.
Attachment C: Guidelines to recovery of reasonable costs

Recovery of reasonable costs

A fee for access, if any, may include:

1. Reasonable costs of resources (such as photocopying or reproducing records in other forms).
2. Reasonable costs for time and labour, including:
   - work performed by clerical staff; and
   - if necessary, professional costs (such as where a health professional needs to review the file before information is released, or provide access by way of an extra consultation).

Other relevant factors

3. Do not charge a fee for lodging an access request (the Privacy Act prohibits this).
4. Discuss with the patient what information they want access to, and the likely fees, before undertaking their request for access.
5. Do not include other outstanding bills (such as consultation fees) in a fee for access.
6. The cost of legal and other third-party advice should not generally be passed on to a particular patient, even though you may have sought the advice to help assess their access request.
7. Consider the individual’s capacity to pay. If possible, charge a reduced rate or waive fees where appropriate.
8. Consider other laws or health sector standards that may relate to fees for access.

---

Attachment D: APP 6 & 7 exceptions

Australian Privacy Principle 6 — use or disclosure of personal information

Use or disclosure
6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:
   a. the individual has consented to the use or disclosure of the information; or
   b. subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.
Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:
   a. the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
      i. if the information is sensitive information — directly related to the primary purpose; or
      ii. if the information is not sensitive information — related to the primary purpose; or
   b. the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
   c. a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or
   d. the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or
   e. the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:
   a. the agency is not an enforcement body; and
   b. the information is biometric information or biometric templates; and
   c. the recipient of the information is an enforcement body; and
   d. the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:
   a. the APP entity is an organisation; and
   b. subsection 16B(2) applied in relation to the collection of the personal information by the entity; the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure
6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.
Related bodies corporate

6.6 If:
   a. an APP entity is a body corporate; and
   b. the entity collects personal information from a related body corporate;
      this principle applies as if the entity’s primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:
   a. personal information for the purpose of direct marketing; or
   b. government related identifiers.

Australian Privacy Principle 7 — direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions — personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:
   a. the organisation collected the information from the individual; and
   b. the individual would reasonably expect the organisation to use or disclose the information for that purpose; and
   c. the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
   d. the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:
   a. the organisation collected the information from:
      i. the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or
      ii. someone other than the individual; and
   b. either:
      i. the individual has consented to the use or disclosure of the information for that purpose; or
      ii. it is impracticable to obtain that consent; and
   c. the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
   d. in each direct marketing communication with the individual:
      i. the organisation includes a prominent statement that the individual may make such a request; or
      ii. the organisation otherwise draws the individual’s attention to the fact that the individual may make such a request; and
   e. the individual has not made such a request to the organisation.
Exception — sensitive information
7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception — contracted service providers
7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

a. the organisation is a contracted service provider for a Commonwealth contract; and
b. the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and
c. the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.
7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

a. for the purpose of direct marketing by the first organisation; or
b. for the purpose of facilitating direct marketing by other organisations;
   the individual may:

c. if paragraph (a) applies — request not to receive direct marketing communications from the first organisation; and
d. if paragraph (b) applies — request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and
e. request the first organisation source of the information to provide its

7. individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

a. if the request is of a kind referred to in paragraph 7.6(c) or (d) — the first organisation must give effect to the request within a reasonable period after the request is made; and
b. if the request is of a kind referred to in paragraph 7.6(e) — the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.
Attachment E: Common third party requests for accessing information

Requests from family members
Privacy Principle 6 and a general health situation (section 16A of the Privacy Act) allow for the disclosure of health information by an optometrist to a ‘person responsible’ for a patient (including a partner, family member, carer, guardian or close friend), if that patient is incapable of giving or communicating consent.

In determining whether to disclose information to a ‘person responsible’, an optometrist will need to consider whether this would be contrary to any known wishes of the individual (previously expressed), whether it is necessary for care and treatment or is for compassionate reasons.

Request from Parents to access to a child’s records
If a child is not able to give consent, then privacy principles allow an optometrist to provide access to a child's records by a parent (see above).

Requests from Courts
If an optometrist has clinical records subpoenaed or they are required to appear in court the law requires that subpoena be followed. Optometrists are advised to notify their indemnity insurer before responding to any subpoena. The Association’s indemnity policy requires an optometrist to notify them of any such request.

The Federal Privacy Act also allows the release of information where the practitioner has a reasonable belief that this is necessary for law enforcement or legal proceedings, however it does not compel this release unless subpoenaed.

When information has been released as a result of a subpoena, the Privacy Act requires a health service provider to make a written note of any use or disclosure of personal information that occurs under APP 6.3(e), (i.e. where the use or disclosure occurs in relation to law enforcement functions).

Requests from Police without a subpoena
If approached by the police or any law enforcement body without a subpoena requesting information about a patient, the optometrist should consider several issues carefully before deciding whether to release the information, such as:

a. Whether there is a legal requirement to provide the information - a court can order the optometrist to produce records or to testify about them.

b. The seriousness of the situation - an optometrist may feel that information should be released to assist a murder investigation, while a minor civil dispute might not justify release.

---

9 The Privacy Act defines a ‘person responsible’ as including: a parent of the individual; a child or sibling of the individual, who is at least 18 years old; a spouse or de facto spouse of the individual; a relative of the individual who is at least 18 years old and a member of the individual’s household; a guardian of the individual or a person exercising an enduring power of attorney granted by the individual that can be exercised in relation to the individual’s health; a person who has an intimate personal relationship with the individual; or a person nominated by the individual to be contacted in an emergency.

10 Section 6, subsection 62 of the Professional Indemnity Insurance Financial Services Guide, Product Disclosure Statement: Other things of which you must notify us 62. You must notify us in writing as soon as practicable of any inquiry, inquest, investigation or complaint brought by a registration board, tribunal, complaints unit, criminal court or coronial court directly relating to your practice as an optometrist.
c. Whether withholding the information places anyone in danger – the optometrist would not be justified in withholding information if this could cause a serious and imminent threat to another person's life, health or safety.

d. Whether access would affect the privacy of others (for example, if there is personal information about another party, such as a family member, in a patient's record), the optometrist should withhold information that would identify them taking care that the remaining information does not allow their identification through context. Alternatively, the optometrist could contact the third party to see if they consent to the release of the information, but before doing this, they need to consider whether this contact will compromise the patient's privacy.

e. Whether information relates to existing or anticipated legal proceedings, for example, if the records contain information relating to the legal proceedings, information can be withheld that would not be discoverable via the legal proceedings.

**Release of genetic information**

APP 6 and a permitted health situation (under section 16B of the Privacy Act) allow the use or disclosure of genetic information to a patient's genetic relatives, without the patient's consent if the organisation reasonably believes that there is a serious threat to life, health or safety of the relative and the use or disclosure is necessary to lessen or prevent that threat. More information on these changes can be found at [www.nhmrc.gov.au/media/media/rel09/091215-privacy.htm](http://www.nhmrc.gov.au/media/media/rel09/091215-privacy.htm) and Private Sector Information Sheet 29 – Use or disclosure of genetic information in the private health sector at [www.privacy.gov.au](http://www.privacy.gov.au).