This document provides advice to members on record keeping and the legal obligations of optometrists, under the Federal Privacy Act 1988 and the accompanying Australian Privacy Principles (APPs).

Note: These guidelines should not be used as a substitute for statutory responsibilities and optometrists must ensure that they comply with relevant State and Federal Laws.

Executive Summary: Record Keeping

- Accurate record keeping is important for the provision of healthcare, for fulfilling the legal requirement of allowing patient access to records and for the protection of an optometrist should there arise a question about the care provided to a patient.
- The Federal Privacy Act¹ and the Australian Privacy Principles² govern the way patient information is collected, stored, disclosed and accessed.
- Individuals can complain about interferences regarding their privacy to the Office of the Australian Information Commissioner (OAIC). The OAIC may investigate and may attempt to resolve the matter by conciliation between the parties. The Commissioner also has a range of enforcement powers.³
- Patient records are defined very broadly and do not just include the written or typed records related to a consultation; they may include appointment books and other material relevant to the management of the patient. Patient records can be paper, electronic or a combination of the two. With the advent of My Health Record⁴,⁵ practices are encouraged to consider moving to the use of electronic record keeping.
- The content of a patient record is guided by the Optometry Board of Australia Guidelines, Medicare Australia and any relevant requirements for professional indemnity insurance. A patient record must be accurate, up to date and contain legible information that reports relevant details of clinical history; clinical findings; investigations; information given to patients; and medications/management prescribed or recommended.
- Records must be securely and safely stored so that only authorised people can access files.
- Only authorised persons should amend patient records; this should be done with appropriate care and all amendments recorded.
- A patient record should be destroyed if it is no longer needed for any purpose for which the information was collected. Federal laws do not prescribe a time however state laws do.
- When permitted, records need to be securely destroyed. In Victoria, NSW and ACT a record is to be kept detailing when and what was destroyed.
- When converting from paper to electronic records, optometrists need to consider storage of paper files if they are not scanned and management of the dual system during the transition.
- There are requirements for notification of patients under certain practice ownerships changes.
Introduction

Accurate record keeping is essential for:

- effective patient care as records are the means by which the presenting symptoms, assessment and test results, diagnoses and management over time for each patient can be tracked.
- the provision of excellent patient care in a multi-practitioner setting. The record should be easy for another optometrist who may assume the management of the patient to interpret, so that they are sure of the findings and the management resulting from previous visits.
- the protection of the optometrist in the event of an accusation of negligence as the patient record is the legal documentation that provides evidence of the adequacy or otherwise of service provision. If records are subpoenaed in legal proceedings, they must meet reasonable standards of record keeping. If actions taken by an optometrist are not recorded in the patient record, it may be difficult for the optometrist to later establish that they had been performed.
- use in My Health Record; a subset of a patient record may be included in a generic My Health Record for access by the patient and other health care professionals.

Privacy Law obligations

Patient health records are governed by Federal, State and Territory privacy legislation, which imposes legal obligations in relation to the collection, amendment, management and destruction of healthcare records.

The Australian Privacy Principles (APP) are:

Part 1: Consideration of personal information privacy

APP 1 — Open and transparent management of personal information
APP 2 — Anonymity and pseudonymity

Part 2 — Collection of personal information

APP 3 — Collection of solicited personal information
APP 4 — Dealing with unsolicited personal information
APP 5 — Notification of the collection of personal information

Part 3 — Dealing with personal information

APP 6 — Use or disclosure of personal information
APP 7 — Direct marketing
APP 8 — Cross-border disclosure of personal information
APP 9 — Adoption, use or disclosure of government related identifiers

Part 4 — Integrity of personal information

APP 10 — Quality of personal information
APP 11 — Security of personal information

Part 5 — Access to, and correction of, personal information

APP 12 — Access to personal information
APP 13 — Correction of personal information
Agencies and organisations are required to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure (APP 11).³

Private optometry practice

The Privacy Act 1988 generally applies to all organisations that provide a health service, including an organisation that is a small business,² and hence applies to health service providers in the private sector throughout Australia. Thus, processes for the development and storage of patient records created in private optometry practices must abide with Australian Government privacy laws.

State and Territory privacy and health privacy legislation, together with privacy requirements for State and Territory public sector health service providers, such as public hospitals, are detailed on the Office of the Australia Information Commissioner website⁶

In the event of an inconsistency between a State or Territory law and a Commonwealth law, the Commonwealth law will prevail.⁷

Public hospital or publicly funded healthcare clinic

Where an optometrist works within a public hospital or publicly funded healthcare clinic, it is generally the case that the medical record remains subject to management by the public sector hospital, and therefore comes under relevant State/Territory legislation - regardless of clinical entries in those records by public or private sector providers.

If an optometrist treats a patient in a public hospital, but retains records (including copies) in a private clinic or other place away from the public hospital, these records would be subject to the Privacy Act.¹

Laws related to record keeping

Records must comply with the Australian Privacy Principles contained in the Privacy Act 1988. The law includes a broad definition of ‘record’ which includes documents and electronic or other devices but not items generally available to the public.⁸

Requirements for practice owners in relation to privacy laws

The following summary of APP obligations may be useful for optometrists:²

Part 1: Consideration of personal information privacy

APP 1 — Open and transparent management of personal information

• Your practice must have a clear and up-to-date APP Privacy Policy about how personal information is managed.⁹ (Optometry Australia has a sample privacy policy available for members.¹⁰) The Privacy Policy must contain
  • the kinds of personal information collected and held
  • how personal information is collected and held
  • the purposes for which personal information is collected, held, used and disclosed
  • how an individual may access their personal information and seek its correction
  • how an individual may complain if the APPs or any registered binding APP code, are breached and how the complaint will be handled
  • whether the practice is likely to disclose personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy

Other material that may be relevant for inclusion is:
  • who, other than the individual, can access personal information, and the conditions for access
  • the situations in which a person can deal with the entity by not identifying themselves or by using a pseudonym
  • information retention or destruction practices or obligations that are specific to the entity
• Your practice must implement practices, procedures and systems to ensure you comply with the APPs and any binding registered APP code, and are able to deal with related inquiries and complaints e.g. procedures for identifying and managing privacy risks at stages of the information cycle, including collection, use, disclosure, storage, destruction or de-identification; security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure
• Your practice must take reasonable steps to make your APP Privacy Policy available free of charge in an appropriate form and, upon request, in a particular form

APP 2 — Anonymity and pseudonymity
• individuals must be able to deal anonymously or by pseudonym with your practice unless the practice is required or authorised by law or a court or tribunal order to deal with identified individuals, or it is impracticable for the practice to deal with individuals who have not identified themselves
• personal information or identifiers are not collected
  Note: the need to interact with Medicare and Health Funds, keep accurate records, provide and receive reports and referrals, ensure reliable payment and prescribe spectacles, contact lenses and medications, means it would be difficult for an optometric practice to deal with a patient on an anonymous basis. Patient requests to be known generally or addressed by a pseudonym should be respected, but it is likely that optometric practices will need to deal with people by the name under which they are known to Medicare.11

Part 2 — Collection of personal information

APP 3 — Collection of solicited personal information
• you may only collect personal information (other than sensitive information), where it is reasonably necessary for, or directly related to, your functions or activities
• unless an exception applies, you may only collect sensitive information where it is reasonably necessary for, or directly related to, your functions or activities and the individual concerned consents to the collection
• personal information must only be collected by lawful and fair means
• personal information must be collected from the individual concerned, unless this is unreasonable or impracticable
  Note: solicited personal information collected for inclusion in a record may include
  * personal information provided by an individual in response to a request, direction or order
  * completed form by an individual
  Note: An organisation may collect health information about an individual if the health information is necessary to provide a health service to the individual, and either:
  * the collection is required or authorised by or under an Australian law (other than the Privacy Act), or
  * the health information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

A permitted health situation might apply where a participant in the My Health Record system collects health information included in a consumer’s e-health record as authorised by the My Health Records Act 2012.12

Health information about an individual may be collected for the ‘management, funding or monitoring of a health service’ by:
• a quality assurance body
• an oversight body
• a health insurer, of information relevant to possible fraud or an incorrect payment.
APP 4 — Dealing with unsolicited personal information

Unsolicited personal information is personal information received by an APP entity that was not requested by the entity. If you receive unsolicited personal information, you must, within a reasonable period after receiving it, determine whether or not you could have collected the information under APP 3 (collection). If not, contact the person who sent the information and arrange to return it; if that is not possible you must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so. (Note that a record of details relating to receipt and destruction of such information should be maintained).

APP 5 — Notification of the collection of personal information

An APP entity that collects personal information about an individual must take reasonable steps, before, at the time of collection of personal information or if this is not practicable, as soon as practicable after collection, either to notify the individual of certain matters or to ensure the individual is aware of those matters.

The matters include:
- the APP entity's identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- the consequences for the individual if personal information is not collected
- other APP entities, bodies or persons to which the personal information is usually disclosed
- information about the entity's APP Privacy Policy including access and correction of personal information
- whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

Part 3 — Dealing with personal information

APP 6 — Use or disclosure of personal information

Personal information can only be used or disclosed for a purpose for which it was collected ('primary purpose'), or for a secondary purpose if an exception applies. Exceptions include:
- consent by the individual to a secondary use or disclosure
- the individual would reasonably expect their personal information to be used or disclosed for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
- use or disclosure is required or authorised by or under an Australian law or a court/tribunal order

APP 7 — Direct marketing

Personal information must not be used or disclosed for direct marketing unless an exception applies. One exception is if the individual has consented to the use or disclosure for that purpose. The organisation must provide a simple way for the individual to opt out of receiving their direct marketing communications.

APP 8 — Cross-border disclosure of personal information

Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.

APP 9 — Adoption, use or disclosure of government related identifiers
APP 9 restricts the adoption, use and disclosure of government related identifiers by organisations.
(An identifier is a number, letter or symbol, or a combination of these, that is used to identify the individual or to verify the identity of the individual.)

Part 4 — Integrity of personal information

APP 10 — Quality of personal information
You must take reasonable steps to ensure that the personal information you collect, use and disclose is accurate, up-to-date and complete. With respect to use and disclosure the information must also be relevant.

APP 11 — Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified, unless the personal information is part of a Commonwealth record, or the APP entity is required by law or a court/tribunal order to retain the personal information. (Ensure that material is not destroyed or de-identified earlier than the minimum time specified for retention of records in your jurisdiction - see Table 1).

Part 5 — Access to, and correction of, personal information

APP 12 — Access to personal information
On request, an APP entity must give an individual access to personal information held about that individual. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

An APP entity must be satisfied that a request for personal information is made by the individual concerned, or a person who is authorised to make a request on their behalf.

An APP entity must take reasonable steps to ensure an individual is aware that the entity's APP Privacy Policy contains information about how the individual may access their personal information held by the entity.

There are minimum requirements in relation to giving access, including how access is to be given, when access can be refused, charges for access, response time, and the need to give a written notice, including the reasons for the refusal, to the individual if access is refused.

An organisation must respond by giving access or notifying refusal of access within a reasonable period of receiving the request; this time should not exceed 30 calendar days. An organisation may impose a charge for giving access to requested personal information, provided the charge is not excessive. Items that may be charged for include staff costs in searching for, locating and retrieving the requested personal information, and deciding which personal information to provide to the individual, staff costs in reproducing and sending the personal information, costs of postage or materials involved in giving access, costs associated with using an intermediary.

APP 13 — Correction of personal information
You must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. This requirement applies both when the APP entity considers there is a need and when the individual requests the entity to correct the personal information. If an APP entity refuses to correct personal information as requested by an individual, the entity must give the individual a written notice covering
a number of areas (see section 13.54 of the Australian Privacy Principles guidelines. Privacy Act 1988 (2014)). An APP entity cannot impose any charge upon an individual for correcting personal information under APP 13.

Breaching privacy principles and complaints from patients

The Office of the Australian Information Commissioner (OAIC) can investigate privacy complaints from individuals about private sector organisations covered by the Privacy Act 1988. The individual making a complaint should first complain directly to the practice and allow 30 days for it to respond. If no response is received within 30 days, or the individual is dissatisfied with the response, they may then complain in writing to the OAIC.

More information about investigation and resolution of complaints is available at https://www.oaic.gov.au/individuals/what-happens-to-my-complaint

What is a patient health record?

A patient health record contains all the health information held about a patient. Records include:
- hand-written or electronic optometry records, including those by optometry students;
- test results (including retinal photographs, OCT images, visual field results etc);
- documented procedures;
- correspondence to and from the optometrist to third parties (patient, specialists, health funds, etc);
- pathology reports;
- documents provided to the patient (for example photographs, literature, pamphlets, video tapes);
- accounting and financial records;
- samples;
- copies of certificates documenting issues (e.g. Workers Compensation, Centrelink, insurance claim forms, sick leave certificates);
- diary records;
- appointment books.

Conversations and correspondence between an optometrist and the professional indemnity provider or an optometrist’s lawyer do not form part of a patient’s records and should be kept separate from clinical files.

What should be included in a Patient Record?

Patient records should contain ordered information that is legible, complete, objective and precise and utilises conventional terminology and abbreviations. The areas to be covered include:

- Patient identification
- General information
- Case history
- Examination findings
- Diagnosis/diagnoses
- Summary of information provided to the patient
- Prescription records
- Medicare information

Recorded information must be:
- objective and non-judgemental; value judgements should never form part of a record;
- able to demonstrate the source of information (for example, GP letter, practice staff observations, parental report);
• able to demonstrate that professional opinions and prognoses are based on objective data or observations and are factual, relevant and devoid of any unnecessary personal details; and
• dated and kept in chronological order (where there are a number of pages/cards for a patient, each must have the patient name, be page numbered sequentially and all must be securely attached together; in some practices, cards are stapled and then placed in plastic envelopes prior to filing).

Attachment A outlines the guidance provided to optometrists from the Optometry Board of Australia, Medicare Australia and Optometry Australia's Professional Indemnity Insurance policy. Taking into consideration this information, Optometry Australia recommends that patient health records contain the following information:

Patient identification

Note that a patient may wish to be anonymous or pseudo anonymous, in which case there will need to be some other mechanism for being able to associate a record with that individual.

To identify the patient the clinical record should include the patient's full name, date of birth and individual healthcare identifier number. Other information that may assist in the identification of the patient includes:

• name of parent or guardian (if appropriate)
• gender
• address
• Aboriginal and Torres Strait Islander status
• telephone number(s)
• Medicare number†
• health insurance details
• ethnicity (where clinically relevant).

General information

The record may contain the name and contact details of the person the patient wishes to be contacted in an emergency.

Information for each visit should include:

• the date and where necessary the time of the visit;
• the reason for the visit and the problems presented;
• the name of the attending optometrist (when an optometric assistant performs delegated tasks or pre-testing their name should be included on the record); and
• the tests performed and the results of these tests.

Case History

The case history should record:

• a clear indication of the main patient concerns or complaints that led them to seek a consultation;
• presenting symptoms and other concerns and symptoms elicited through history taking;
• previous ocular, visual and general health history, including current medications
• family medical and ocular history;
• the patient's occupation, hobbies and sports (if relevant to presenting problem or treatment); and

---


† Note: you may not adopt an identifier assigned to the individual by a Commonwealth agency as your own identifier of an individual. Collection of Commonwealth identifiers by private sector health organisations should only be for the purpose of providing care and treatment to a client; where such care and treatment is authorised by, and will be financed by, a specific government agency - eg. collecting the Medicare number for treatments under the Medicare Benefits Scheme, or the Department of Veterans- Affairs (DVA) Card number for treatment under DVA entitlements.
• allergies and adverse reactions (patients with allergies and severe adverse reactions to medications should have this marked in a prominent place both outside and inside the record card; a red sticker on the card can be used to draw attention to this fact; a comparable method could be employed to mark a computer record).

Examination findings

The examination findings should be presented as a careful record of observations with the results of every test and procedure performed (preferably in the order performed), even if the results are negative or normal. If a test is not recorded and interpreted it may be difficult for the optometrist to later establish that it had been performed. Recordings such as WNL (within normal limits) or NAD (no abnormality detected) should be preceded by the name of the tissue or structure examined. Recordings such as ‘ophthalmoscopy NAD’ are inadequate to describe observations, or the extent of examination. Instrumentation used and the time at which the results were obtained should be included for tests such as tonometry.

Any unusual ocular sign or ocular pathology should be drawn and clearly labelled or presented photographically or as a digital image. Where appropriate, the size, depth or elevation and location of lesions, and their colour, vascularity, shape, texture and density should be recorded. Accurate recording of pathology through diagrams and/or photographs/images provides a means of determining the progression of ocular conditions over time and assists in determining management strategies. The inclusion of drawings of an external eye, a cross-section of the lens and an optic nerve head on the record card provides a basis for diagram drawing for paper records. Drawings should be done as soon as possible after observation. Colour can be used to differentiate lesions, arteries and veins.

Photographs and results of computerised or other tests (such as visual fields or corneal topography) should be carefully labelled and dated and ideally stored with the record. If computer files and referrals, paper records, visual field results and so on are stored in different locations within the practice there must be clear cross-referencing on the patient record card/computer record to ensure that all patient information can be easily located and retrieved by authorised staff.

Prior to their inclusion with the patient record or filing elsewhere, results of computerised tests should be signed and dated by the optometrist. These results can be printed at any time and may be performed by a person other than the optometrist; a signature and date provide a record that the reports have been sighted and interpreted by the optometrist. (An alternative method is needed where all sections of patient records are computerised).

The name and dosage of all medications or diagnostic drugs used during the examination and any abnormal response to them should be recorded.

Diagnosis/diagnoses

The diagnosis/diagnoses derived from investigations should be included. Where there is incomplete information or where patient symptoms are not adequately explained by the current diagnoses, further indicated assessment and management should be recorded.

Summary of information provided to the patient

The record must contain a summary of information provided to the patient. The record should demonstrate an adequate explanation of diagnoses and options for management or treatment to the patient to indicate that they have had the opportunity to give informed consent to management. Management options should correlate with patient symptoms and concerns and diagnoses derived from investigation. The chosen management option should be specified so that the care provided can be followed logically from the record.
Notes should be made of any advice or warnings given to the patient and where appropriate, the patient’s response should be recorded. Patient information regarding the presence of any abnormality, need for review, referral, recall, risks or special recommendations should be recorded.

Prescription records

The record should include prescriptions and dispensing details of spectacles or contact lenses (for example, lens type, segment heights, monocular and binocular PDs, tints, coatings, frame and so on) and charges for appliances. The optometrist should indicate the expiry date of the prescription.

Therapeutic prescriptions

Where therapeutic medication is prescribed, supplied or administered by the optometrist, the patient record must include the date and details of the medication prescribed together with instructions given to the patient.

In Victoria, requirements for record keeping by therapeutically endorsed optometrists who use, transfer within and between premises, administer, sell, supply or dispose of Schedule 4 poisons are detailed in the Drugs, Poisons and Controlled Substances Regulations 2017.14

Medicare information

When an optometrist seeks patient information from the Department of Human Services to determine appropriate itemisation of accounts, receipts or bulk-billed claims, the optometrist must ensure that:

(a) the patient is advised of the need to seek the information and the reason the information is required;

(b) the patient’s informed consent to the release of information has been obtained; and

(c) the patient’s records verify the patient’s consent to the release of information.15

Where multiple attendances by a patient are made on the one day with the same optometrist the time of each attendance should be stated on the account (e.g. 10.30 am and 3.15 pm) in order to assist in the payment of benefits. Times do not need to be specified where a perimetry item is performed in association with a consultation item.15

Details of costs to the patient and Medicare item numbers claimed on a patient’s behalf should be included on the record card as benefits can only be claimed where ‘a service has been performed and a clinical record of the service has been made’.15 When billing items 10912, 10913 or 10914, the optometrist must document the significant changes in visual function (item 10912), the new signs or symptoms (item 10913), or the nature of the progressive disorder (item 10914) suffered by the patient on the patient’s record card.15 For item 10944, the optometrist must document the nature of the embedded corneal foreign body (sub-epithelial or intra-epithelial), the method of removal of the foreign body and the magnification used, and the method of removal of the rust ring and the magnification used. For telehealth items (10945 to 10948), the optometrist must keep contemporaneous notes of the consultation including documenting that the service was performed by video conference, and the date, time and the people who participated. Only clinical details recorded at the time of the attendance count towards the time of the consultation.15

Other matters related to the contents of health records

1. Referral Letters and Reports

Other documentation such as referral letters and reports (both to and from the optometrist) and other communications with other professionals regarding a patient should be kept for a minimum of two years and attached to the patient’s record (or cross referenced if they are scanned and stored on computer or the paper version is stored elsewhere) and should include the date and the name and
address of the professional. The optometrist should initial and date any reports received from other health care practitioners or other sources prior to having them included with the patient's record or scanned. This is to provide a record that the reports have been seen by the optometrist and where necessary, followed up.

2. Follow up with patients who do not attend appointments and referrals

It is recommended that each practice develop a system to track patients who do not attend scheduled appointments, including documenting follow-up in a patient's record. This list could be developed by practice staff, however the relevant optometrist should review the list as soon as practicable and a decision made on possible follow-up taken either within the same session or by the end of the day. The following factors are important for an optometrist to consider in relation to follow-up with patients:

- the likelihood of the patient suffering harm if adequate follow up does not occur;
- the likely seriousness of the harm; and
- the burden of taking steps to avoid the risk of harm.

In the case of a clinically significant referral, the optometrist should systematically track these and only remove the required referral from their follow-up list when a letter or telephone call confirms that patient has attended the specialist.

If despite numerous reasonable attempts by the optometrist to convince them to do so, a patient refuses to attend an appointment or referral, case law in Australia has recognised that patients are responsible for their own actions and optometrists cannot compel a patient to attend a follow-up or referral appointment.

Any written communications with the patient and notes from telephone contacts with the patient should be attached to the patient record card (this is of particular importance if the optometrist needs to follow-up non-attendance at referral or review visits). The date that a recall letter for further investigations or periodic review was sent, and patient failures to return as scheduled, should be documented in the patient record.

3. Patient refusal of treatment or a referral

Where a patient declines an optometrist's recommended management plan (for example, referral) following adequate communication of the options, that rejection of advice should be carefully recorded in detail. If the patient has a potentially serious condition and has refused referral, the optometrist should write to the patient advising them of the need for referral and the potential consequences should they fail to heed the advice provided (a copy of this letter should be kept with the record or suitably cross-referenced). Some optometrists also get patients to sign a refusal form and sign that they have witnessed this. For some, this may be too extreme and a registered letter to a patient's home may be sufficient.

Similarly if a patient refuses a diagnostic procedure following appropriate explanation of the indications, benefits and possible negative factors, such refusal must be noted on the record. It may be advisable for the optometrist to request that the patient initial an appropriate comment on the record card at the time of the examination. (This will not be possible in the case of computer records so some sort of note may need to be made and scanned for inclusion with the record).

4. Transfer of patient information

Optometrists are obliged by privacy laws to take reasonable steps to protect the personal information they hold from misuse, loss and from unauthorised access, modification or disclosure. What are considered 'reasonable steps' will depend on the particular circumstances of the optometry practice and the information held.
Care must be taken to ensure no unauthorised person can access information during transfer of information from a patient record. Secure messaging system (involving encryption) used for the electronic transfer of confidential information should be considered.

If it is necessary to send data via fax, special care should be taken to check facsimile numbers before sending personal information, and confirming receipt of the fax by the intended recipient.

If someone requests information regarding a patient, it must be established that they are either the patient or a person authorised by the patient to access their data prior to the provision of personal information by telephone, in writing or electronically.

Amendments to patient records

‘APP 13 requires you to take reasonable steps to correct personal information you hold about a patient if it is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to the purpose for which it is held. ........When making corrections, it may be appropriate to keep the original incorrect records and details that reflect the record prior to the time of corrections, as evidence that the change was made and when it was made. However, it should be made clear to those inspecting the patient file or database that these records are incorrect.‘

When corrections or alterations to patient records are necessary

- Do not obliterate the mistakes or outdated material; it should remain legible. Where a mistake has been made, a correction should be placed clearly above or below the erroneous words through which a line that still leaves the words legible has been drawn; liquid paper should not be used.
- Corrections to contents must be signed, initialled and dated by the writer unless corrections are made immediately beside the mistake. If the record is in chronological order, an additional sheet that is signed and dated must be added for the purpose of correction with a note made on the original that the addition has been made. The note should also be signed and dated. The reason for the alteration should be noted.
- For computer records consider who has access to the password to start the computer as this access may allow that person to delete files. The optometrist must be sure that those people with access to computer records are aware of both the confidentiality of the content and the requirements of the Privacy Act in amending records.
- An electronic audit trail or a log file can be used to track changes made to a computer clinical record. The audit trail needs to contain a complete history of all transactional data and it and its associated software must be secure. The audit trail or log file needs to include:
  - the date and time of any change made;
  - a method to identify the person who made the change (unique electronic identifiers can be used for this purpose);
  - a method to identify the workstation from which the change was made
  - the type of alteration (addition, amendment and so on); and
  - the data that was in the record before and after the change.

Optometrists in Victoria are required to follow the Health Privacy Principles detailed in Schedule 1 of the Victorian Health Records Act 2001.

Optometrists in New South Wales are required to follow the Health Privacy Principles detailed in Schedule 1 of the NSW Health Records and Information Privacy Act 2002 No 71.

Optometrists in the Australia Capital Territory are required to follow the Privacy Principles detailed in Schedule 1 of Health Records (Privacy and Access) Act 1997 (ACT).

Rewriting patient records due to "going electronic"

As a general principle, transfer of old record cards to new ones is not recommended, unless there is a clear reason e.g. a genuine problem with the overall legibility/usability, or if the practice is moving to a new record keeping system, such as an electronic system.
If the originals are in good order, it is suggested that old records are retained and used. If a record is damaged or legibility is poor, it is appropriate for an optometrist to copy it onto a clean card, dating it and clearly noting it was a copy, made due to damage to the original. Scanning the original damaged record is advisable where possible.

If any information is being transferred/copied from old to new record cards, it is recommended that the transferring or copying be done by someone with an appropriate level of technical and clinical knowledge to ensure that records are copied accurately and without error.

Avant Medical Insurers recommends that if an optometrist is transferring records to a new system, a legible scanned copy of each original record is retained where feasible.

**Time limits to maintain records**

APP 11 requires an organisation to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any authorised purpose, but the Federal Privacy Act and Australian Privacy Principles (APPs) do not stipulate a specific timeframe in which health records need to be maintained. Legal requirements of individual States or territories should be followed regarding retention of health information by health service providers. See Table 1: Record Keeping Periods.

Determining the need to retain information will involve considering:

- The primary purpose for which the information was originally collected;
- Any secondary purposes that is both directly related to the original purpose of collection, and within the patient's reasonable expectation.
- Retaining information for the purposes of providing ongoing care to the patient, for public health reasons or to comply with State or Territory laws for the retention of health records.
- Whether a patient is being investigated or treated for a condition where there is potential for recurrence, or if the patient has expressly stated to the optometrist that he or she is dissatisfied with the service provided, or if the practice is aware that the patient has made or is investigating a claim.

Appointment books also constitute a component of practice records and should be kept for the same length of time as is required for patient records.

**Table 1: Record Keeping Periods**

<table>
<thead>
<tr>
<th>Location</th>
<th>Length of time records are to be kept</th>
<th>Legislation</th>
</tr>
</thead>
</table>
| Federal | Records are to be kept for a minimum of two years, including referrals and documents created as a condition of claiming an MBS item. | Changes to the Health Legislation Amendment (Improved Medicare Compliance and other measures) Bill 2018 came into effect on 1st July 2018 and introduced changes to various sections of the Health Insurance Act (1973). The key changes include:  
- a new requirement to keep records for a minimum of two years, including referral and documents created as a condition of claiming an MBS item,  
- Financial Administrative Penalties can be applied to a debt of more than $2500 if substantiating documents are not provided, or not provided within the required timeframe.  

If you are ever subject to a compliance audit, you must keep any records related to substantiating items claimed for the notified period, even if this is longer than two years.  
Australian Privacy Principle 4: Dealing with unsolicited personal information  
Australian Privacy Principle 11: Security of personal information  
APP 11.2 requires an APP entity to destroy or de-identify personal information it holds but which it no longer needs for any purpose permitted by the APPs, unless the personal information is contained in a Commonwealth record or the entity is required by or under an Australian law, or a court/tribunal order, to retain the information. Consequently, personal information that is retained under APP 4.4 may nevertheless need to be destroyed or de-identified in accordance with APP 11.2 |
<table>
<thead>
<tr>
<th>Location</th>
<th>Length of time records are to be kept</th>
<th>Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>Adults - at least 7 years from the date the patient was last provided with medical services or treatment. Children (less than 18 years old) - for health information collected whilst the individual was under 18 years of age, the record must be kept until the patient attains or has attained the age of 25 years.</td>
<td>Health Records (Privacy and Access) Act 1997, principle 4.1. Principle 4.1. Storage, security and destruction of personal health information—safekeeping requirement. 1. A record keeper who has possession or control of a health record must ensure that— (a) the record is protected, by reasonable security safeguards, against each of the following: i. loss; ii. unauthorised access, use, modification or disclosure; iii. other misuse; and (b) if the record is given to another entity—everything reasonably within the power of the record keeper is done to prevent unauthorised use or disclosure of any information contained in the record. 2. A record keeper must keep, and must not destroy, a health record about a consumer, even if it is later found or claimed to be inaccurate. 3. However, clause 2 does not apply to the destruction of a health record about a consumer if— a. the destruction is required or allowed under a law of the Territory; or b. the destruction is not prohibited under any other law and happens after— i. if the consumer is under 18 years old when the information is collected—the day the consumer turns 25 years old; or ii. if the consumer is an adult when the information is collected—7 years after the day a service was last provided to the consumer by the record keeper. iii. Principle 4.2 also requires the creation of a register to track the destruction of records. c. an electronic copy of the record has been generated— i. by a method described in the Electronic Transactions Act 2001, section 11 (2) (b); and ii. when the record is destroyed it is reasonable to expect that the information contained in the electronic copy will be readily accessible so as to be useable for subsequent reference. Principle 4.2: Storage, security and destruction of personal health information—register of destroyed or transferred records 1. A record keeper must keep a register of records that have been destroyed or transferred to another entity. 2. The register must identify the following for records that have been destroyed or transferred: (a) the consumer to whom the record relates; (b) the period of time the record covers; (c) for a destroyed record—the date the record was destroyed; (d) for a transferred record—the entity to which the record has been transferred. 3. A record keeper need not keep a record on the register under clause 1 for longer than 7 years after the day the record is made.</td>
</tr>
<tr>
<td>NSW</td>
<td>Adults - at least 7 years from the date the patient was last provided with medical services or treatment. Children (less than 18 years old) - for health information collected whilst the individual was under 18 years of age, the record must be kept until the patient attains or has attained the age of 25 years.</td>
<td>Health Records and Information Privacy Act 2002 No 71. <a href="http://www.legislation.nsw.gov.au/#/view/act/2002/71/full">http://www.legislation.nsw.gov.au/#/view/act/2002/71/full</a> 1. A private sector person who is a health service provider must retain health information relating to an individual as follows: (a) in the case of health information collected while the individual was an adult— for 7 years from the last occasion on which a health service was provided to the individual by the health service provider, (b) in the case of health information collected while the individual was under the age of 18 years—until the individual has attained the age of 25 years. 2. A health service provider who deletes or disposes of health information must keep a record of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted or disposed of. 3. A health service provider who transfers health information to another organisation and does not continue to hold a record of that information must keep a record of the name and address of the organisation to whom or to which it was transferred. A record referred to in subsection (2) or (3) may be kept in electronic form, but only if it is capable of being printed on paper.</td>
</tr>
<tr>
<td>NT</td>
<td>No specified time.</td>
<td>Information Act 2002, Schedule 2: Information Privacy Principles: IPP 4.2 requires: “A public sector organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.”</td>
</tr>
<tr>
<td>Location</td>
<td>Length of time records are to be kept</td>
<td>Legislation</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>QLD</td>
<td><strong>Adults</strong>: Retain for 10 years after last patient/client service provision or medico-legal action.&lt;br&gt;<strong>Minors</strong>: Retain for 10 years from patient/client attaining 18 years of age; AND 10 years after last patient/client service provision or medico-legal action.&lt;br&gt;<strong>Deceased minors</strong>: Retain for 10 years from date of patient/client’s death; AND 10 years after last medico-legal action.</td>
<td>Health Sector (Clinical Records) Retention and Disposal Schedule QDAN683v.1 (<a href="https://www.forgov.qld.gov.au/schedules/health-sector-clinical-records-retention-and-disposal-schedule">https://www.forgov.qld.gov.au/schedules/health-sector-clinical-records-retention-and-disposal-schedule</a>) accessed 29 May 2017. (Note: This covers clinical records created by public sector health authorities such as hospital and health services, it does not cover the private sector).</td>
</tr>
<tr>
<td>SA</td>
<td>No specified time.</td>
<td>The Commonwealth Privacy Act 1988, protects the privacy of an individual's information where it relates to Commonwealth agencies, and private businesses (including not-for-profit organisations) with a turnover of more than $3 million.</td>
</tr>
<tr>
<td>TAS</td>
<td>No precise legislated length of time.</td>
<td>Schedule 1 of the Personal Information Protection Act 2004 Act requires:&lt;br&gt;4. Data security&lt;br&gt;(1) A personal information custodian must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure.&lt;br&gt;(2) A personal information custodian must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.&lt;br&gt;(3) A personal information custodian, the records of which are subject to the Archives Act 1983, must take the reasonable steps referred to in subclause (2) only with the approval of the State Archivist.</td>
</tr>
<tr>
<td>VIC</td>
<td><strong>Adults</strong>: 7 years after the last occasion on which a health service was provided to the individual by the provider.&lt;br&gt;<strong>Children</strong>: after the individual attains the age of 25 years; or 7 years after the health service has been provided, whichever is the later.</td>
<td>Health Records Act 2001, Schedule 1—The Health Privacy Principles, 4 Principle 4—Data Security and Data Retention&lt;br&gt;4.2 A health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless—&lt;br&gt;(a) the deletion is permitted, authorised or required by the regulations or any other law; or &lt;br&gt;(b) the deletion is not contrary to the regulations or any other law and occurs—&lt;br&gt;(i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or &lt;br&gt;(ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider— whichever is the later. &lt;br&gt;4.3 A health service provider who deletes health information in accordance with HPP 4.2 must make a written note of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted.</td>
</tr>
<tr>
<td>WA</td>
<td>No specified time.</td>
<td></td>
</tr>
</tbody>
</table>

**How to destroy records**

Where clinical records are to be destroyed, shredding or incineration should be used to ensure the maintenance of confidentiality of clinical information.

The deletion of an electronic file may not necessarily remove all traces of electronically stored information. Special care should be taken to ensure electronic records are properly and securely disposed of when they are no longer needed. For example, secure disposal of electronic records could include overwriting records before they are deleted and ensuring the deletion of all back up files.

In Victoria, New South Wales and the ACT health service providers who destroy health information must make a written note of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted or destroyed. (Health Records Act 2001, Principle 4 - Data Security and Data Retention),20 Health Records and Information Privacy Act 2002
No 71 Section 25, Health Records (Privacy and Access) Act 1997 (ACT) Principle 4.2: Storage, security and destruction of personal health information—register of destroyed or transferred records.

Record systems

Patient records may be paper-based, computerised or a combination of the two.

APP 11 requires an organisation to take reasonable steps to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Regardless of the method of record keeping, storage of records must:

- preserve the confidentiality of the record;
- prevent damage, loss or theft of the record;
- allow access by authorised practice staff to ensure records are kept up to date; and
- be secure. The optometrist and their staff should make all reasonable attempts to protect the security of the files.

A practice security policy could be developed to detail all organisational systems used for processing, storing or transmitting personal information. The security risks faced by the optometry practice could be assessed in the development of the policy, and then cost-effective measures devised to reduce the risks to acceptable levels. To be effective, a security policy needs to be monitored and periodically reviewed. Staff and management must be aware of the protective security policies and how to implement them.

As noted above the APPs require reasonable steps to be taken. What is reasonable depends on the circumstances in which personal information is held. The sensitivity of personal information being stored is an important factor and higher levels of security could be expected for sensitive information. The costs of any security systems also need to be considered in relation to the risks faced by an optometry practice. Optometry practices collect healthcare information, which is regarded as highly sensitive.

Physical security

Optometry records may be stored in a range of paper based and electronic forms. Physical security measures must prevent unauthorised access to information and are relevant to all forms of storage. Optometry practices should consider physical security measures such as:

- lockable cabinets; security keys and containers such as filing cabinets, safes and compactuses;
- security alarm systems to detect unauthorised access; and
- access control measures.

Optometry practices should also consider adopting the following office management:

- recording file movements, especially if files are sent to secondary and other practices;
- encouraging a ‘clean desk’ policy;
- securely storing all files after use; and
- a security classification system to identify information needing special protection.

Paper Record cards

An optometrist may design a card that assists them in recording their data rather than using a blank card. Such a design could assist another optometrist needing to refer to the records. Consideration needs to be given to:

- the size of the record card;
• use of check lists and boxes for recording full names, Medicare numbers, health fund details, address, telephone numbers, date of birth etc;
• space for case history; whether there are individual sections for presenting reason, personal and family general health, personal and family ocular health, current medications and so on;
• inclusion of background diagrams (for example, the optic nerve head) to facilitate recording;
• sections for commonly performed tests and for details of the prescription; and
• sufficient space to record all information obtained, including diagnoses and an action plan.

**Filing/Indexing**

Filing and indexing of records needs to facilitate easy access by optometrists and relevant practice staff. Records are usually filed alphabetically. Clear labeling of the alphabetical range in a particular section assists in accurate filing. Indicate how surnames that could be filed in different ways are to be filed, for example whether ‘Mc’ is filed as ‘Mac’ or ‘Mc.’; whether ‘von B…..’ is filed under ‘V’ or ‘B’; whether ‘Le M…..’ is filed under ‘L’ or ‘M’; whether spaces or hyphens are incorporated, for example whether Smith-Black is filed under Smith with positioning based on the initial of the first given name or whether it is filed in a section after Smith.

A method to differentiate active from inactive files may be useful. Coloured stickers on files can be used to indicate contact lens patients, those receiving vision therapy, those attending for low vision consultations, patients with allergies and so on. A marker with the date of the last visit can be attached to a file to indicate when the patient is due for a recall; alternatively this can be done via computer.

Accounting details may be kept with the record cards. If kept separately, cross-referencing is necessary.

**Computer-based records**

Computer records reduce the possibility of lost and misfiled paper records, are easier to back-up than written records and allow remote access of patient records at other practices. Optometrists must abide by APP11 to ensure there is adequate data security.

Ensure you have adequate computer storage space and sufficient workstations at suitable positions in the practice if computers are not portable.

Laptops or iPads may assist optometrists who perform domiciliary visits or visit a number of locations that do not have compatible computer facilities. Issues of back-up and security must be considered. Memory bars or portable UBS storage devices are a useful option for backing up files at remote locations. Data may be stored over the internet (‘in the Cloud’) provided that the requirements of the APPs are met.

If you generally maintain computer records and a laptop/internet is not available for domiciliary visits, you will need to have an alternative method of recording data, with subsequent transfer to a computer record. If you revisit a patient whose record had been entered into the computer, you will need a print-out or screen shot of the previously obtained record.

The on-screen format for the computer record must facilitate data entry and should encourage the recording of all necessary information as it is obtained during the examination. There are a number of software packages designed for optometrists. The system needs to incorporate:

- a method to record patient data obtained at the consultation. This may be as:
  - text (for example patient history, presenting complaint, medications, allergies);
  - numeric data such as intra-ocular pressures, refractive errors and visual acuity;
  - graphical data such as visual fields;
images, for example, ocular fundus photographs that may be stored as .jpeg, bitmap or .tif files and can be embedded in the patient record or cross-referenced;

- a method to generate diagrams;
- the ability to scan reports received about the patient; and
- a word processing facility to address the preparation of reports and referral letters.

Practices may wish to apply their computer system to scheduling and recording appointments, sending recall notices, insurance matters, equipment details, ordering materials, financial records and stock inventory. Computer-generated prescriptions for spectacles, contact lenses or therapeutic drugs can help avoid errors in reading handwriting.

Where computers are used in the generation of therapeutic drug prescriptions, software can be used to provide information on the contra-indications and side effects of prescribed medications, interactions with other medications the patient uses and details of medications previously prescribed to the patient by the optometrist.

Optometrists must consider compatibility of computers and software when trying to link the record-keeping system to autorefractors, visual fields, imaging tools and dispensary. There must be careful cross-referencing and dating of entries or the software system may allow easy incorporation of information from scanned documents or from printouts.

Computerised records and litigation

Computer generated records that can be printed on paper can be used in legal proceedings provided the optometrist can demonstrate that the software package used has the ability to either prevent alterations to the document or to note when an amendment was made, by whom the amendment was made and the extent of that amendment (see below for amendments to computer records).

Security of computer records

Computer records can be copied easily. It is recommended that practices develop a security policy regarding confidentiality of, and access to, all patient records. This is required in the state of Victoria.‡

Optometry practices should consider assessing practice management of information systems for storing, processing and transmitting information. The appropriate protective measures will depend on the circumstances and risks involved. Depending on the practice’s circumstance and risk profile, measures could include:

- access control for authorised users, such as user passwords, screen saver passwords and limiting access to shared network drives to authorised staff;
- virus checking;
- IT support to deal with security risks; and
- auditing procedures and data integrity checks.

Audit trails

Use of audit trails and digital signatures that authenticate authorship and guarantee detection of unauthorised modification are procedures that should be considered. Computer files should be password protected with passwords strictly limited to practice personnel needing access to computer records; such passwords should be altered regularly to maintain security. Passwords should be stored in a secure location separate from the computer. There are alternatives to passwords such as smartcards and PIN codes. Two-factor authentication can enhance the security of passwords.

‡ The Victoria Health Records Act 2001 Health Privacy Principle 5 - Openness, requires that an organisation must set out in a document—(a) clearly expressed policies on its management of health information; and (b) the steps that an individual must take in order to obtain access to their health information. The organisation must make the document available to anyone who asks for it.²⁰
There must be safeguards to restrict modifications and additions to records (for example, electronic audit trails or log files and use of unique electronic identifiers). Computer records should be easy for authorised staff to retrieve, but the optometrist may wish to have restrictions on the levels of access for different staff members.

There are compliance obligations in relation to the handling of individual healthcare identifiers (IHIs) by healthcare providers. A record of every access to the Healthcare Identifier Service must be maintained.\(^\text{§}\)

**Back ups**

Consideration must be given to virus protection, regular backups and routine computer maintenance. Computer records should be easy for authorised staff to retrieve, but the optometrist may wish to have restrictions on the levels of access for different staff members.

There are compliance obligations in relation to the handling of individual healthcare identifiers (IHIs) by healthcare providers. A record of every access to the Healthcare Identifier Service must be maintained.\(^\text{§}\)

Staff must be aware of the need for back-up, so that if one person is away, back-up still occurs. Storage of back-ups over a number of days in a secure location removed from the practice is recommended. There are a number of commercial solutions to storage back-up that practices can access which automatically back-up records in a secure location.

For added security the practice should consider:

- the positioning of screens and printers so patients cannot observe information;
- the use of screen-savers (which can be associated with a password to discontinue them);
- automatic disconnection after a period of inactivity (this will require that there is an autosave after a period of time and particularly before the disconnection);
- care in closing a patient file before a new patient; and
- ensuring that staff log out of the workstation when they finish.

Staff must be aware of the need for back-up, so that if one person is away, back-up still occurs. Storage of back-ups over a number of days in a secure location removed from the practice is recommended. There are a number of commercial solutions to storage back-up that practices can access which automatically back-up records in a secure location.

Note that if back-ups are made to the ‘cloud’ you must ensure that personal information can be moved to the third-party service provider’s facilities securely, that those facilities are appropriately secure and that the arrangement meets the requirements of the Privacy Act (whether the information is stored within or outside Australia).\(^24\) MDA National recommends that the cloud server is located in Australia; but if this is not the case they advise that ‘Australian privacy law requires that before personal information is disclosed overseas, a practice must take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles’.\(^25\)

\(^\text{§}\) To ensure that a record of every access to the Healthcare Identifier Service is maintained, healthcare providers are required to do either one of the following:

- give the HI Service enough information to identify, by name, the authorised user making the request. That information may be given, for example, as part of the data sent to the HI Service from the healthcare provider’s practice management software. In this case the provider does not need to keep its own record of individual staff members’ access
- keep its own retrievable record of each occasion an individual authorised user has accessed an IHI. The record must include either the staff member’s name, or other information that can be used to identify the staff member.

If the provider keeps its own records, it only needs to inform the HI Service of the identity of the organisation, rather than the identity of the individual authorised user requesting the IHI, when accessing the HI Service. The healthcare provider must retain the relevant records for as long as a staff member is authorised to access IHIs from the HI Service, and for seven years from the day after they cease to be authorised.

If the HI Service makes a written request for the access record, the organisation must provide a copy to the HI Service within 14 days of receiving the request. It is an offence under the HI Act for a healthcare provider to intentionally not comply with such a request.

Because transfer of personal information to another entity is a ‘disclosure’ for the purposes of the Privacy Act, you must advise patients that their information will be stored in facilities provided by a third party.24

Issues to consider when determining whether cloud computing is suitable for your practice are detailed in the Royal Australian College of General Practitioners resource 2.3 Cloud computing.26

**Computer viruses**

The effects of computer viruses and computer systems being accessed by unauthorised people through cyber attacks or hacking can be very disruptive to the business and could negatively affect the confidence patients have in a practice. The following actions should be taken to ensure a practice’s computer system is secure:

- install and use security software; and
- ensure all staff are educated about online security which might compromise computerised patient record systems.


**Ceasing Practice: sale or practice closure; retirement or death of an optometrist**

Privacy laws also need to be kept in mind when there is a change in business arrangements at a practice. Information regarding your obligations when you sell or close a practice is available at https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/business-resource-change-of-business-circumstances-or-closure-of-a-health-service. Additional requirements in Victoria are detailed in the Health Records Act 2001. It is recommended that you seek legal advice when selling, merging or otherwise altering the ownership nature of your practice.

**Frequently Asked Questions and health records**

1. Delegation of record keeping not recommended

It is recommended that the optometrist does not delegate the role of transcribing patient records after the consultation to another staff member because of the risk of error in data entry and interpretation and confidentiality issues. If the optometrist does not enter the data there is a need for verification of the accuracy of the input.

2. Who owns the records?

Legally, patient records belong to the optometrist who made the record, or in the case of employed optometrists, to their employer. The records may belong to the employee optometrist if this is specified in their employment agreement. In a partnership, there is usually joint ownership of records. This is normally specified in any partnership agreement, along with procedures for handling the records in the event of the partnership ending.

Where optometrists participate in shared care arrangements or where they see patients in hospital settings, they may not have ownership of records, as these would belong to the employer. In these cases it would be important to clarify this issue and ensure that an optometrist providing the care is able to have access to the records in the future should the need arise, such as defending a future complaint.
3. Patient records when the optometrist visits health or medical centres

In some instances an optometrist may provide services at a medical or health centre on irregular occasions or at largely spaced intervals. Optometrists should ensure that staff who work at such centres are aware of issues relating to patient records and that they are aware that the optometrist should maintain responsibility for issues relating to the release of records or copies or summaries of records. It is also advisable that the optometrist makes a copy of records and maintains these in the event of enquiries. This also serves as a means of backing up files.

4. Visiting Optometry Work and record keeping

Optometrists undertaking consultations under the Visiting Optometry Scheme (VOS) must keep appropriate records.

Depending on how the VOS consultations are delivered, there may be different arrangements for record keeping. If providing optometry consultations within a local Aboriginal Medical Service (AMS) or Aboriginal Community Controlled Health Organisation (ACCHO), it is recommended that the optometrist comes to an agreement in relation to paperwork and record keeping with the AMS/ACCHO or the Regional Eye Health Coordinator. Regardless of the arrangement, it is recommended that the optometrist either makes an agreement that they can access the records if they remain the property of the AMS/ACCHO or they take a copy of the records.

5. Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service are permitted health situations under the Australian Privacy Principles, meaning that the information handling requirements imposed by APP 3 and APP 6 do not apply. 9

6. Shared or Multi-disciplinary care

Increasingly optometrists work with other health professionals to deliver ophthalmic care. A relevant example is the shared care of patients with glaucoma.

Generally, under APP6, health information may only be used or disclosed for a purpose for which it was collected (known as the ‘primary purpose’), or for a secondary purpose if an exception applies.Optometrists should be confident about their use or disclosure of health information where there is a clear, shared understanding with their patient about matters such as:

- the reasons that personal information is being collected;
- the circumstances when it may be used and disclosed eg for multi-disciplinary care; and
- to whom disclosures are likely to occur in the course of assessment, treatment or referral.

An optometrist does not always need the patient's consent to use or disclose their health information for another, directly related purpose - as long as the patient would reasonably expect the use or disclosure that the provider has in mind to provide care.

A patient's expectations can be effectively managed through good optometrist-patient communication. This usually means the patient has been told the use or disclosure would happen, or they would expect it to happen because of why they gave the information to the provider in the first place.

If the patient would not reasonably expect the use or disclosure that the provider has in mind, then the provider will usually need to get the patient's consent before proceeding. Other exceptions in the Privacy Act permit disclosure without consent in certain circumstances, such as to lessen or prevent a serious threat to life, health or safety, or where the disclosure is required or authorised by law.
7. Vision screenings and record keeping

Vision screening records must be created and stored securely for future reference. In order to be able to meet any insurance or legal claim in the future a copy of the original should be kept by the optometrist and/or the optometrist’s practice. For practical purposes a form with a carbon copy could be developed and a copy could be provided to parents, the school or business (depending on appropriate consent), with the original retained by the optometrist. The length of time records are kept is discussed in an earlier section and depends on the state in which the screening is conducted.

Records should contain:
- information necessary to identify the child/person
- any tests performed
- results of all screening tests performed
- the name of the optometrist who performed the screening
- the date and place where the screening was performed
- copies of any reports/referrals/recommendations
- parent/guardian consent forms

Any report provided to the parent/guardian of the child or to the adult undergoing a screening should be attached to the screening record card. This report should include:
- details of what examinations were performed
- the results of these examinations
- recommendations arising from the assessment such as further assessment, follow up, referral

Even where there are no anomalies detected it is important to indicate that the screening does not substitute for a full eye examination. Parent(s)/guardian(s) should be advised of appropriate intervals to seek full eye examinations for the child. A report can be supplied to the school provided the parent/guardian gives their permission, as the school may wish to keep a record of the report on file. This may be of particular use if further screening occurs in the future.

If the screening involves an adult, they should be advised to seek regular eye assessments.
Attachment A: Additional guidance to optometrists in relation to record keeping

Optometry Board of Australia

The Optometry Board of Australia, in its Code of Conduct for Optometrists\(^{27}\) recommends that records contain accurate, up to date and legible information that can be interpreted by another optometrist and that includes relevant details of:

1. clinical history;
2. clinical findings;
3. investigations;
4. information given to patients; and
5. medications and other management.

Avant

The Avant Professional Indemnity Insurance for Optometry Australia (OA)\(^{28}\) states that:

| Health professionals have an ethical and legal obligation to maintain accurate and adequate records for patients to ensure good patient care. Good records also assist in the defence of any claim or a complaint made.  
| Records should include the following:  
| • **Sufficient information to identify the patient to whom they relate and to allow another optometrist to continue management of the patient should the need arise.**  
| • **Any information known to the optometrist who provides the treatment relevant to their diagnosis or treatment such as:**  
| - Information concerning the patient’s medical history  
| - Results of any examinations  
| - The results of any tests performed on the patient  
| - Information concerning allergies or other factors that may require special consideration when treating the patient  
| - Particulars of any opinion reached by the optometrist  
| - Any plan of treatment and details of any prescriptions.  
| • All details of referrals to a medical practitioner, colleague or other person should be noted.  
| • Optometrists who work for or in association with non-optometrists should remember their duty and responsibility to manage all clinical and optometric information and ensure that confidentiality is maintained.  
| • It is important to be able to identify the author of any entry in the patient record.  
| • Copies of all relevant correspondence and notes of any telephone communications with the patient should be retained.  
| • It is particularly important to document if a patient indicates that they do not intend to follow the advice given by the optometrist.  
| • In general, records are owned by the optometrist who prepares them, not the patient. However, ownership may be unclear where optometrists are in practice together or where premises are shared. In these cases ownership depends on many factors such as the contractual arrangements between practitioners and the principal of the practice. It is always prudent for parties involved to clarify this at the outset of any arrangement.  
| • If a patient wishes to transfer their care to another optometrist at another practice, the new optometrist should be provided with such information as is required for the proper ongoing care of the patient by way of either a treatment summary or preferably a copy of the patient’s records. |
There is no obligation to provide original records. The patient should bear the reasonable cost of providing this information, but failure to pay should not be used as a reason to prevent relevant information being provided to the new optometrist. Patients should sign an authority to transfer their care and records to another optometrist and the authority should contain the name, date of birth of the patient whose records are to be transferred, to be signed by the patient and be dated. These guiding principles apply to both paper and electronic records.

Medicare Australia

Where it is necessary for the optometrist to seek patient information from the Department of Human Services in order to determine appropriate itemisation of accounts, receipts or bulk-billed claims, the optometrist must ensure that the patient's records verify the patient's consent to the release of information.

Medicare benefits may only be claimed when a service has been performed and a clinical record of the service has been made.

When charging item 10913 the optometrist should document the new signs or symptoms suffered by the patient on the patient's record card; when charging item 10914, the optometrist should document the nature of the progressive disorder suffered by the patient on the patient's record card.

Professional Services Review (PSR)

In a Professional Services Review a decision regarding inappropriate practice will consider whether or not the practitioner has kept adequate and contemporaneous patient records.

To be adequate, the patient or clinical record needs to:

1. clearly identify the name of the patient; and
2. contain a separate entry for each attendance by the patient for a service and the date on which the service was rendered or initiated; and
3. each entry needs to provide clinical information adequate to explain the type of service rendered or initiated; and
4. each entry needs to be sufficiently comprehensible that another practitioner, relying on the record, can effectively undertake the patient's ongoing care.

To be contemporaneous, the patient or clinical record should be completed at the time that the service was rendered or initiated or as soon as practicable afterwards. Records for hospital patients are usually kept by the hospital and the practitioner could rely on these records to document in-patient care.
References
15. Optometric Medical Benefits Australian Government Department of Health Medicare Benefits Schedule Book Optometrical Services Schedule Operating from 1 May 2016
17. Gough, K, You have responsibilities for patients who fail to attend an appointment, Avant Mutual Group, Australian Optometry, April 2010.
21. Health Records and Information Privacy Act 2002 No 71 (NSW) 
25. MDA National. Cloud Storage of Medical Records 
26. Royal Australian College of General Practitioners. 2.3 Cloud computing 
27. Optometry Board of Australia, Code of Conduct for optometrists, 
28. Avant Professional Indemnity Insurance for Optometry Australia (OA) 