synapse optometry

Q&A on Healthcare Records

Dr Nina Kriel

2 CEUs (Ethics/ Medical law/ Patients' rights)

One of the benefits of lecturing is that it forces me to frequently review and update what I know, because after decades in the profession, one can become complacent. None of what I've included here should be news to you, but I hope it triggers a brush-up of your record keeping in the practice, as it has mine.

What is considered a patient health record?

According to the HPCSA, *'a patient health record is the longitudinal collection of an individual's personal and health information, recorded by a healthcare practitioner or at the directive of the healthcare practitioner, regardless of the form or medium used to make such a record.'*

Why do we keep health records?

Besides the obvious fact that we need to be reminded of what we have found, and decided to do about it, they also serve to promote and ensure continuity of care. In case of a complaint or litigation, they serve as evidence of our standard of care, and that we applied the principles of good clinical practice. They may be useful should you choose to teach, or do research, or when you've learned something new and wish to contact a segment of patients, e.g. all of your contact lens patients. They may be needed as evidence for occupational disease and injury compensation, and obviously they serve an important administrative purpose.

How long should I keep records?

Section 14 of the Protection of Personal Information Act (POPI Act) deals with this subject in great detail.

'Subject to [other parts of the POPI Act], records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—

- *retention of the record is required or authorised by law;*
- *the responsible party reasonably requires the record for lawful purposes related to its functions or activities;*
- *retention of the record is required by a contract between the parties thereto; or*
- *the data subject or a competent person where the data subject is a child has consented to the retention of the record.*

Records of personal information may be retained for periods in excess of [the above] for historical, statistical or research purposes if the responsible party

has established appropriate safeguards against the records being used for any other purposes.

A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must—

- *retain the record for such period as may be required or prescribed by law or a code of conduct; or*
- *if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.*

A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record…

The destruction or deletion of a record of personal information… must be done in a manner that prevents its reconstruction in an intelligible form.

The responsible party must restrict processing of personal information if—

- *its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;*
- *the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;*
- *the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or*
- *the data subject requests to transmit the personal data into another automated processing system.*

The HPCSA considers it ideal to store patient health records indefinitely, particularly with the ease of doing so electronically. Otherwise, *'a patient health record should be stored for at least a minimum of six (6) years as from*

the date that a patient health record has become dormant (dormancy commences at the time when a patient was last treated by a healthcare practitioner).'

There are important exceptions:

- Minors - records should be kept until they are 21, i.e. 18 years to reach majority and from then, patients have 3 years to make a claim against practitioners.
- Mentally incapacitated patients – records should be kept for all their lives
- Records for patients treated under the Occupational Health and Safety Act 85 of 1993 must be kept for 20 years after treatment.
- Patients with health conditions that take a long time to manifest e.g. asbestosis, should be 'kept for a sufficient period to allow such patients equitable access to the care they may require at a later stage. The recommendation is that this period should not be less than 25 years.'
- Statutory obligations may prescribe how long to keep patient health records should be kept
- State patient health records shall only be destroyed if such destruction is authorised by the Deputy Director-General concerned.

Aim for a balance between the costs, risks and potential benefits of retaining records indefinitely.

What should I record?

All clinical findings, including the examination, the differential diagnosis, any information or advice given to the patient, clinical decisions made, by whom and when, agreement or consent given by patient, and dates. Treatment, procedures, drugs, doses, further investigation ordered or referrals made, results from those investigations and referrals, future appointments or recall dates. Any other documentation related to the patient's health. Records should reflect by whom the patient is seen and who is keeping the record, the dates that they are consulted and any other e.g. telephonic/ online/ written/ virtual clinical interactions (with dates and times) with patients and/

or relatives, discussions with colleagues and any correspondence related to the patient's care. Records should be contemporaneous, i.e. made during or as soon as possible after consultation/ interaction. If they are made later, times and reasons should be given.

The following patient details are compulsory, according to the HPCSA: Identification and particulars, full biopsychosocial history of a patient, including allergies and idiosyncrasies; the time, date and place of consultation; their assessment and proposed management, including medication and dosage prescribed, referrals to specialists or other healthcare professionals. Patient's progress and response to treatment, including adverse effects, investigations done and their results and any time that patients are booked off for work or other responsibilities. Written proof of informed consent for procedures when this is relevant. The POPI Act does not specify that consent must be in writing, but does place the onus on the data processor, which practically requires consent to be written or otherwise recorded.

Who owns the patient records?

Technically and legally, 'owns' is not the right word. If you think of a frame or a piece of equipment in your practice, you own those because you exercise exclusive control over them and you have the right to exclude others, you can prove that you own them e.g. with an invoice or proof of payment or in the case of a property or car, a title deed or registration document. If you own a thing, you have the right to its use and enjoyment, and any income or benefit that it produces. You may sell, gift or dispose of it in any way you choose.

In terms of the POPI Act (section 24), a data subject (patient) may request that their personal information be corrected or deleted and may request an update to inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained unlawfully

information. Ownership in the legal sense would not allow another party such rights. So more accurately, then, we **control** or **manage** patients' records.

Nevertheless, the HPCSA does use the word, saying 'a patient health record is owned by the health practitioner or the entity generating such a patient health record,' but the patient is entitled to have access, and to obtain the information contained in their records. In terms of the Children's Act, any person from the age of 12 years must be provided with their health records. Parents may apply for access to records for their child younger than 16 years, but such access should only be given on receipt of written authorization by the patient (Promotion of Access to Information Act). In general, the HPCSA confirms and repeats the requirements of the POPI Act and adds specific circumstances under which healthcare practitioner may give third parties access to records, even without the written authorisation of the patient:

- In case of a court order
- If the records are required in defence by a practitioner facing disciplinary or legal action
- If the health practitioner is under a statutory obligation to disclose certain medical facts, (e.g. reporting suspected child abuse (Children's Act)
- Where non-disclosure would represent a serious threat to public health (National Health Act).

State institutions must retain records and images and make copies available to doctors and patients, for which they may charge a reasonable fee in terms of the Promotion of Access to Information Act. Private patients should be allowed to retain their own results, unless the practitioner deems it necessary to retain them to monitor, releasing the originals should patient need them e.g. to seek a second opinion. It can get complicated in multi-disciplinary practices, so it's best to develop guidelines for the practice.

In the event of a practitioner's death, their patient health records are included in the estate, to be dealt with by the executor. Typically these are carried over to the remaining partner(s)/ practitioners or the new owner. The new practice owner must inform patients of the change of ownership, and that they may choose to continue with the practice or request their records be transferred elsewhere. If none of the above happens, the executor must keep the records safe for at least 12 months, and has authority to further deal with the files as s/he may deem appropriate after that.

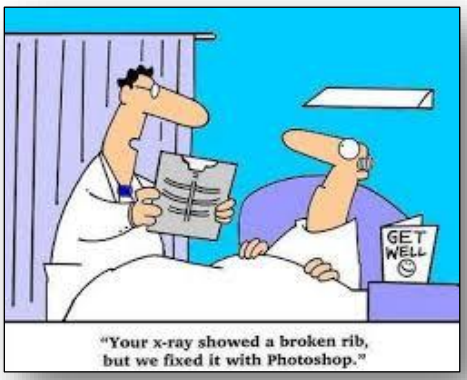
Private practitioners choosing to close their practice (e.g. retirement, change in profession, voluntary erasure, etc.) must within three months of closure inform all their patients in writing that the practice has closed, and how to request the transfer of their health records to their next provider. An identified health practitioner or institution must keep the records safe for at least 12 months.

Does the HPCSA have a health record checklist?

"I had trouble reading your doctor's handwriting, but I think I figured it out. However, if you start to drool uncontrollably or gain more than 15 pounds in a week, stop taking them."

- Records should be complete and comprehensive, but concise. Section 10 of the POPI Act deals with minimality, and requires the personal information processed to be 'adequate, relevant and not excessive.'
- Writing must be clear and legible. Abbreviations should be clear, unambiguous and consistent.
- Records should follow a standardised format (e.g. history, physical findings, investigations, diagnosis, treatment, and outcome.)
- Give facts only, and draw conclusions essential for patient care, avoiding unsolicited comments.

- Where records need alteration, it is better to add a new note referring to the correction without altering the initial entry. Otherwise, a line in ink should be put through the original entry so that it remains legible; alterations should be signed and dated.



- All entries, original and alterations, should be attributable, i.e. the person making the notes should be identified. This is particularly important when multiple healthcare professionals are responsible for a patient health record e.g. in the case of hospital or multi-disciplinary settings. Each entry should be dated and signed.
- Billing records should be kept separate from patient care records.
- Attached documents such as diagrams, laboratory results, photographs, charts, etc. should always be labelled. Sheets of paper should not be identified simply by being bound or stapled together – each individual sheet should be labelled.

What needs to be included in a sick note?

Sick notes must contain

- the name, address and qualification of the practitioner;
- the name of the patient;
- the employment number of the patient (if applicable);
- the date and time of the examination;
- whether the certificate is being issued as a result of personal examination or report from the patient;
- a description of the illness, disorder, or malady in layman's terminology with the informed consent of the patient. Without consent, the practitioner can only say that based on their examination of the patient, the patient is unfit to work;

- whether the patient is totally indisposed for duty is able to perform less strenuous duties, and exact time frame for either…
- the date of issuing the certificate of illness; and
- a clear indication of the identity of the practitioner who personally and originally signed

Can I use pre-printed stationery for writing prescriptions?

Rule 17: 'A practitioner - (a) shall be permitted to issue typewritten, computer-generated, pre-typed, pre-printed, or standardised prescriptions for medicine scheduled in schedules I, II, III and IV of the Medicines and Related Substances Control Act only with personal and original signature.

How does general legislation align with the HPCSA's Guidelines on the Keeping of Patient Health Records?

There is significant overlap between the HPCSA's regulations, the Protection of Personal Information Act (POPI Act), the Promotion of Access to Information Act (PAIA), the Consumer Protection Act and the Children's Act. The POPI Act anticipates potentially conflicting legislation and specifies that it should be interpreted in a manner that '*does not prevent any public or private body from exercising or performing its powers, duties and functions in terms of the law as far as such powers, duties and functions relate to the processing of personal information and such processing is in accordance with this Act or any other legislation.*' Such concurrent legislation, especially where instructions differ, should be dealt with in the best interest of the patient, considering the information we have and our clinical knowledge. Regulators can, and do refer matters to one another. During my term of office, our board received 2 complaints referred from the Consumer Council.

HPCSA: Patient records should be accessible and readily available when needed at any point in the healthcare facility. Important information should be highlighted and updated e.g. allergies and adverse drug reactions, particular instructions or needs.

POPI: Section 16 specifies that information should be current, complete and accurate and serve the purpose that it was gathered for. No more, and no less or it is effectively inaccurate.

HPCSA: Records must be securely stored in terms of s17 (1) of the National Health Act. The person in charge of a health establishment in possession of a patient's health record, must set up control measures to prevent unauthorised access to those records and to the storage facility, or system by which records are kept.

POPI: Section 3 described how information should be safeguarded and section 8, the responsibilities of the responsible party. As the name implies, the responsible party must ensure compliance with the 8 conditions set out in the Act, right from the time of determination of the purpose and means of the processing and during the processing itself. In a healthcare practice, that's from when we start to collect the information at first contact. Do you use a booking app? Or do members of your staff request IDs and medical aid details when making the appointment? Do you send out questionnaires before you see the patient? Your data collection, and therefore your responsibility, starts there. PAIA designates the head of the business as the Information Officer. Depending on the type of business, the Information

Officer will therefore be the sole trader, a partner in a partnership or CEO (or equivalent) in a company e.g. a hospital.

What sort of fines are imposed by regulators?

The South African Information Regulator – the regulating body created by the POPI Act – issued its first administrative fine in 2023. The Department of Justice and Constitutional Development (DoJ&CD) was fined R5 million for its failure to comply with an enforcement notice. The DoJ&CD had suffered a security compromise in 2021 resulting in the loss of approximately 1 204 files that contained personal information. On investigating, the regulator found that the DoJ&CD had failed to implement adequate security measures and to comply with the duty to notify security compromises.
The maximum fine at the SA Information Regulator is R10 million, having considered the nature of the personal information involved, the duration and extent of the contravention, the number of data subjects affected, the likelihood of damage or distress, and whether the responsible party could have prevented the contravention or has previously committed an offence in terms of POPIA.

The HPCSA has jurisdiction over practitioners registered with its 12 professional boards. Matters concluded by Prelim committees may have fines of up to R70 000, depending on the transgression. If the matter is referred for an inquiry, higher fines are possible.

A complaint about privacy breaches related to practitioner record keeping can be brought to, and dealt with by either of these regulators. Appeals for decisions by both regulators lie to the High Court, or in plain English, are extremely costly.

What did the regulator instruct the DoJ&CD to do in the enforcement notice?

The department was ordered to submit proof within 31 days that it had

- put in place adequate technical security measures;

- renew its anti-virus and software licences, including its intrusion detection licence which would have flagged access to its network by unauthorised persons;
- to notify the Regulator of the security compromise:
- instituted disciplinary proceedings against the officials responsible;
- provided training on POPIA to all staff;
- implemented reasonable measures to identify internal and external risks to personal information; and
- implemented a POPIA compliance framework & incident response plan.

How should I secure my patient records?

Section 19 of the POPI Act requires a responsible party to secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical measures, but doesn't specify them. Responsible parties need to identify potential risks, establish safeguards, and check that they have been implemented. Can your filing cabinet lock? Is it locked? If you store information on a cloud, is it password protected and do you have reasonable and current security in place. It mentions generally accepted information security practices and procedures which may apply to specific industries, or professional rules and regulations. It allows for a Code of Conduct, e.g. if your group practice wants to follow a more secure process.

Any requirements for a Code of Conduct?

A Code must incorporate all 8 conditions listed in the POPI Act. A less restrictive Code is not allowed. A regulator (e.g. the HPCSA) may issue a

Code of Conduct, usually to give responsible parties in a particular sector clearer guidance. The Information Regulator may revoke a Code.

How does the POPI Act relate to children?

The POPI Act adopts the UN definition of child as a person under 18, and in terms section 34 of the Act they may not consent to processing of their personal- or special personal information. The development of the Act follows foreign law and international trends to safeguard children, e.g. the Children's Online Privacy Protection Act (COPPA) in the US, which protects the personal information of children under the age of 13, with a list of conditions to be met. Following pressure from governments, parents and interest groups, platforms such as Instagram, for example, are adding privacy features. Their accounts are automatically private for 13 to 17-yr-olds, and can only be unlocked with a parent's approval. Of course, children probably know better than their parents how to bypass it, should they want to.

A problem may arise when children access healthcare and need to share personal and special personal information without an adult to consent to it. The Children's Act allows children over the age of 14 to consent to non-surgical medical treatment. They may have bank accounts from the age of 16, so practically, a child of 17 could have a consultation, and pay for it, except that they don't have the legal capacity to contract (under 18) or the capacity to consent to our processing their information. Practically, a parent calling to make the appointment, or sending the medical aid card and their ID with the child is taken as implied consent. Do remember to record their consent somehow if you are at all in doubt.

Read!

The HPCSA requires us to stay abreast of their regulations, so there's no choice there, but please don't be fearful, or avoid reading original legislation. The trend is for legislators to use more accessible language, especially when drafting legislation that develops our Constitution, many of which guide our interaction with patients. Here are the links to the Acts that I have referred to, either for your reading pleasure or to address your insomnia. I hope the former!

Protection of Personal Information Act 35 of 1998
Occupational Health and Safety Act 85 of 1993
Children's Act 38 of 2005
National Health Act 61 of 2003
Promotion of Access to Information Act 2 of 2000
Medicines and Related Substances Control Act 101 of 1965
Consumer Protection Act 68 of 2008

Here's the link to the HPCSA Booklet on Patient Records

Questions

1. Which Act requires a patient to consent in writing to the processing of their personal information?
   a. Protection of Personal Information Act
   b. Consumer Protection Act
   c. Health Professions Act
   d. None of the above

2. Who may develop a Code of Conduct relating to the protection of a patient's information?
    a. The HPCSA
    b. The SAOA
    c. Your multidisciplinary practice
    d. All of the above

3. Albert (accompanied by his parents) consults you for a dyslexia assessment at the age of 12. After discussing the outcome, where he is found NOT to be dyslexic, Albert never returns. How long must you keep his healthcare records?
    a. Six years in terms of the Health Professions Act
    b. Twenty five years
    c. Until he is 21
    d. Practitioners need to decide for themselves

4. Beryl is a busy body and likes to go through her neighbours' rubbish. She discovers a black bag full of patient records at her complex garbage collection point. Where should she direct her complaint?
    a. The body corporate of the complex
    b. The HPCSA
    c. The Information Regulator, created in terms of the POPI Act
    d. Both b and c are correct

5. Charles helps practitioners to stay compliant with both the POPI Act and the HPCSA's regulations. Which of the following is he NOT likely to advise?
    a. Update your anti-virus software
    b. Train staff to identify and safely process personal and special personal information
    c. Place all of your patient data (currently in a locked filing cabinet) on the cloud

d. Review technical security measures

6. Dr Dayimane is retiring from dentistry and has sold her practice. She is moving to the coast and may do a few locums if the need arises. Whom does she have to tell that she is leaving the practice?
   a. Notify her patients within three months
   b. Notify her bankers within six months
   c. Notify the HPCSA
   d. Notify the Board of Healthcare Funders within 12 months

7. The HPCSA has found your psychologist friend Mr Ericson guilty of poor record keeping and fined him R10 000. He is unhappy with this decision and absolutely determined to defend himself at all costs. What do you advise?
   a. Deregister from the HPCSA
   b. Appoint an attorney and take the case to the High Court
   c. Complete Form 2003 A to lodge an appeal to the HPCSA
   d. Contest the decision on the basis of lack of jurisdiction

8. In terms of the Children's Act, from what age can a child consent to medical investigation e.g. an eye examination?
   a. 14
   b. 16
   c. 18
   d. 21

9. The maximum fine at the HPCSA is
   a. Not specified
   b. R5 million
   c. R10 million
   d. R70 000

10. A sick note requires:
    a. The practitioner's name, address and qualification
    b. A diagnosis of the ailment or condition indisposing the patient for work
    c. A description of the tests performed and their outcomes
    d. An indication whether the condition is contagious or poses any risk to co-workers