



UNPACKING HPCSA BOOKLET 9: ETHICAL RECORD-KEEPING IN THE DIGITAL AGE



WHY CLINICAL RECORDS MATTER

Clinical records are far more than just notes on a file — they are the backbone of safe, ethical, and effective patient care.

Accurate, detailed records help ensure continuity of treatment, protect both patient and practitioner in the event of complaints or claims, and serve as a valuable source of information for teaching, research, and public health. The Health Professions Council of South Africa (HPCSA) sets clear expectations for how practitioners should capture, store, and manage these records. From documenting the patient's history and clinical findings to recording informed consent and treatment outcomes, practitioners are expected to keep records that are complete, legible, contemporaneous, and securely maintained.

Where a practitioner is accused of medical negligence or unprofessional conduct, clinical records provide important evidence, central to their defence.

Here we share questions frequently asked by specialists in private practice seeking practical guidance on what the HPCSA requires, and how to handle common challenges in day-to-day practice.

EthiQal, trading under Titan Risk Services (Pty) Ltd, an authorised financial service provider FSP 51361.

Disclaimer: This resource provides a simplified overview of HPCSA Booklet 9, related ethical guidelines, and South African laws. It aims to help healthcare practitioners understand key principles of clinical record keeping but is not a substitute for the official HPCSA publications or legal advice. Practitioners should refer to the full guidelines and seek professional guidance when needed. EthiQal is not responsible for any loss arising from the use of this resource. Information is current as of October 2025. © 2025 EthiQal.

ETHIQAL
Your professional indemnity partner

IS IT BEST TO KEEP ELECTRONIC OR HARD COPY CLINICAL RECORDS?

There isn't a one-size-fits-all answer — both electronic and hard copy records are acceptable, as long as they meet the HPCSA's requirements for accuracy, legibility, confidentiality, integrity, retrievability, and secure storage.

The law does not prescribe one format over the other. What matters most is that whichever system you choose:

- Records are complete, clear, and updated promptly.
- Patient confidentiality is always protected.
- You have a reliable way to store and retrieve your patients' records if needed in the future.

Hard copy (paper) records

Hard copy records can feel straightforward and familiar, but they come with practical challenges:

- They take up space, can be misplaced, and are vulnerable to fire, water damage, or theft.
- They can be more difficult to back up and share securely.
- Handwritten notes must be legible, dated, and signed by the practitioner.

However, paper records remain compliant if stored safely and managed in line with HPCSA requirements.

Electronic (digital) records

Electronic records offer many advantages:

- They improve legibility and searchability.
- They can be securely backed up and easily retrieved.
- They can facilitate continuity of care through controlled sharing with colleagues (e.g. within a multidisciplinary team).

If, however, you are unfamiliar with setting up IT systems, you will need technical support to ensure that patients' personal information is protected against unauthorised access, loss or alteration:

- Access to patient records should be password-protected and limited to authorised personnel only.
- Regular data backups and cybersecurity safeguards are essential.
- The system should allow audit trails and timestamped entries to preserve record integrity.

Many practices are moving towards electronic systems because of the convenience and security benefits, but if you prefer paper, that's fine too — just make sure you have safe storage and a plan for archiving and easy retrieval.

If you move from paper to electronic, or from one electronic system to another, ensure a proper migration plan so that no information is lost and access to old records remains possible.



Format	Pros	Cons
Hard copy	Easy to start. No tech skills needed. No risk of system crashes.	Takes up space. Hard to back up. Risk of fire, water damage or loss Illegibility issues.
Electronic	Easy to search, share and back up. Saves space. Improves legibility.	Requires software, training, and secure IT systems. Risk of data breaches if not protected.



Paper or digital, what matters most is that your records are clear, relevant, secure, and accessible when needed.

CAN CLINICAL RECORDS BE UPDATED RETROSPECTIVELY OR CORRECTED?

Yes — but with caution.

Clinical records should always be written at the time of the consultation or procedure, or as soon as possible thereafter, i.e. be contemporaneous, as notes written at the time of an event are the most reliable and trustworthy. However, there are times when you may need to correct or add to a record afterwards. Whilst both actions involve amending an existing record, there is a subtle distinction:

- A correction fixes an error in the original entry, i.e. there is a change to factual information recorded previously (for example, an incorrect date or wrong dosage of medication prescribed).
- A retrospective entry adds new or late information that was not available at the time (for example, test results, follow-up details, or additional history).

Irrespective of the distinction, the same legal and ethical principles apply to both - the record must remain accurate, complete, traceable, and credible.

If you need to correct or update a record after the fact:

- In the case of paper records, draw a single line through any incorrect entry so the original remains visible. For electronic records, use the “amend” or “correction” function in the electronic system.
- Never delete, obscure, or overwrite the original note — instead, add the correction or clarification alongside it.
- Clearly mark the alteration as a “late entry”, “correction” or “addendum”.
- Explain why the alteration was made, if relevant (e.g. “additional lab results received” or “patient provided further history” or “incorrect reading captured”).
- Record and sign the actual date and time of the alteration. In the case of electronic records, ensure your electronic system automatically timestamps and records your user ID.

Legal and ethical rationale

Amending records transparently ensures continuity of care and preserves the evidential integrity of the record. Altering notes without indicating they were added later may amount to:

- Unprofessional conduct under the Health Professions Act and HPCSA Rules;
- Misrepresentation or fraud under common law; or
- Obstruction of justice if the record is under examination in legal proceedings.



*You can update records afterwards —
just be transparent, date your entry, and never delete and rewrite history.*

WHO 'OWNS' THE NOTES THAT DOCTORS KEEP?

ARE CLINICAL RECORDS DOCTORS' INTELLECTUAL PROPERTY?

This is a common question.

The record — whether the paper file or electronic record system — is generally owned by the practitioner, the practice or the institution that created or maintains it. However, the information contained within the record (the patient's personal health information) belongs to the patient. In other words, the doctor or practice is the custodian of the record, while the patient is the owner of the information within it.

As custodian, you are responsible for safeguarding, storing, and maintaining the record in accordance with the National Health Act, HPCSA guidelines, and POPIA.

You may not deny the patient access to their information, nor may you share it without their consent unless legally authorised.

COMMON SCENARIOS

A patient asks for their clinical file to take to a new doctor.

- You must provide a copy (not the original file) of all results, summaries, and your personal notes within a reasonable time.
- You cannot refuse because of unpaid accounts. You may however charge a reasonable fee for making and delivering the copies.
- Originals should always be retained by you in case of future legal enquiries.
- As the patient is entitled to a copy of your notes, only write what you are comfortable for the patient to read. Use professional, objective language and avoid disparaging or judgmental comments.

A lawyer requests a patient's records for a case.

- You may only release them with the patient's written consent (unless required by law, e.g. a subpoena).

You capture your clinical notes on the hospital system and then take a photo to transcribe these into your own note-keeping system.

- Where a practitioner records notes in the hospital's records or electronic system and then retains or transcribes a copy for their own records, both the hospital and the doctor are considered lawful custodians of the same information.
- To avoid patient confidentiality and data security being breached during the transcription process, it is important not to store identifiable patient information on unsecured personal devices (e.g. phone photos, unencrypted drives).

A locum or employed doctor leaves a practice and wants to keep copies of patient notes.

- Clinical records created in the course of employment or a locum engagement generally belong to the practice or institution, not the individual practitioner.



- The departing doctor may not take original records or copies containing identifiable patient information without the patient's consent or a written agreement with the practice.
- If continuity of care requires the doctor to retain information about patients they continue to treat privately, this should be arranged with the patients' explicit consent and in compliance with POPIA.
- The practice remains the lawful custodian of the records created during the engagement period.

A doctor wants to use anonymised case notes or images for teaching or publication.

- You may use de-identified clinical information for legitimate educational or research purposes, provided no patient can be identified directly or indirectly (e.g. through unique details, dates, or images).
- If the information includes identifiable features (such as clinical photographs, imaging, or unusual cases), you must obtain specific, written consent from the patient before using it.
- Even when the case is anonymised, you still act as custodian of the information and must ensure it is used ethically and with respect for patient dignity and confidentiality.



***In short, you keep the file, but the patient owns the story inside it.
You cannot share the patient's story without their agreement or
without the law requiring you to do so.***

WHERE RECORDS ARE REQUESTED BY A PATIENT AND/OR THEIR APPOINTED REPRESENTATIVES, WHAT IS A REASONABLE PERIOD WITHIN WHICH TO RESPOND?

The HPCSA requires practitioners to release records “without unreasonable delay”. What this means in practice depends on who is asking and why.

COMMON SCENARIOS

A patient asks for their clinical records

(e.g. to change doctor, seek a second opinion, or for personal use)

- These should generally be treated as a priority, particularly when continuity of care is at stake. Records should be shared as soon as reasonably possible, considering the urgency of the patient’s situation.

Patient’s records are requested via a legal process

(eg. subpoena, medicolegal enquiry, court order)

- Requests made in relation to legal enquiries often come with their own specified deadlines. However, not all deadlines specified by attorneys or third parties are legitimate. For example, personal injury attorneys often stipulate short deadlines but statutory requests under PAIA allow 30 days for production.
- Where no deadline is given, practitioners are expected to prioritise the request and act promptly, given the potential legal consequences of delay.
- These types of requests are best dealt with by professional indemnity providers.

Patient records are required for an insurance claim

(e.g. disability, workmen’s compensation, RAF, medical aid)

- These requests can have a direct impact on a patient’s livelihood or access to benefits. It is best practice to respond within a timeframe that does not cause unnecessary prejudice to the patient’s claim.
- In a similar vein, insurers and financial advisors submitting these requests have a responsibility to make the process clear and user-friendly for practitioners. Complex or incomplete forms can create unnecessary delays — so streamlined, well-prepared requests help everyone, especially the patient.

Regardless of who requests the information, the guiding principle is timely access without unnecessary obstacles. Where you are not bound by legally defined deadlines, a sound principle is to respond within a timeframe wherever possible that you would expect of others if you were asking.

Always remember to ***only release patient records with their written consent, or if required by law*** (eg. under a subpoena or court order).

If in doubt about the validity of any request, confirm that proper consent or legal authority exists before disclosing.



Let urgency and patient impact guide what ‘reasonable’ means.

Don’t delay sharing of records unnecessarily.

HOW LONG SHOULD CLINICAL RECORDS BE KEPT FOR AND WHEN CAN THEY BE DISCARDED?

WHAT HAPPENS WHEN I CLOSE MY PRACTICE OR WHEN A PATIENT LEAVES MY PRACTICE?

Ideally patient health records should be kept indefinitely, especially if this can be done electronically. At a practical level, however, a balance must be struck between the cost of storing records indefinitely (as well as space limitations where a practice is paper based) and the risk of not having them available when needed.

Minimum retention periods (HPCSA guidance and legal framework)

Category	Minimum Retention Period	Legal / Ethical Basis
Adults	At least 6 years after the last consultation or treatment.	HPCSA Booklet 9, guideline 9.2; NHA s17
Children (minors)	Until the patient reaches 21 years of age, as generally civil claims may be instituted up to 3 years after reaching majority (majority = 18 years).	Prescription Act 68 of 1969; HPCSA Booklet 9, guideline 9.3
Patients with mental disability	Retain for the lifetime of the patient, since no prescription period applies while incapacity continues.	Prescription Act s13; Booklet 9, guideline 9.3.2
Occupational health or toxic exposure cases	At least 20 years after last treatment or exposure).	As required by Occupational Health and Safety Act 85 of 1993
Deceased patients	Retain for at least 6 years after death, or longer if litigation or an inquest is possible.	Medico-legal best practice; Booklet 9

When a practice closes or changes hands

When a practitioner retires, emigrates, dies, or sells their practice, they remain responsible for ensuring that records are securely handed over and stored for at least the required period. Options include:

- Arranging safe custody with another practitioner or successor practice.
- Using a reputable archiving service compliant with POPIA.

Whether a practice closes or changes hands, the HPCSA expects practitioners to inform patients at least three months before practice closure or transfer of their intentions.

- To ensure continuity of clinical care and easy access by patients to their records, they must be given clear instructions on where and how their records can be accessed.
- Communication regarding this should be kept on record for accountability purposes.



When can records be discarded?

Records may only be destroyed or permanently deleted after:

1. The relevant retention period has passed, and
2. There are no ongoing or foreseeable clinical, legal, or administrative reasons to keep them.

Disposal must always protect confidentiality and comply with POPIA's data destruction requirements — e.g. shredding paper files or permanently deleting digital records. Even where patients have left a practice with their personal health information, practitioners should - for their own medicolegal protection - keep the records for the minimum period specified.



*Ideally keep records indefinitely —
but if not practical, follow HPCSA minimums and ensure safe
handover or archiving if closing or selling a practice.*

CAN PRACTITIONERS HAND OVER RECORD-KEEPING TO ANOTHER PARTY?

WHO IS ACCOUNTABLE FOR CLINICAL RECORDS WHEN RECORD-KEEPING IS OUTSOURCED?

Even if you hand over record-keeping to someone else - such as an administrative assistant, billing company, IT provider, or an outsourced records storage company - you, the practitioner, remain ultimately accountable for the integrity and safety of the records.

That means

1. You are responsible for ensuring records are complete, accurate, secure, and accessible when needed.
2. Delegation does not absolve you of liability if records are lost, incomplete, mishandled, or accessed inappropriately.
3. If you use a third-party service (like cloud storage, practice management software, or off-site archiving), you must:
 - Verify that they have sufficient security safeguards (physical, technical, and contractual).
 - Enter into a written data processing agreement that ensures compliance with POPIA and protects patient confidentiality.
 - Periodically review or audit their compliance with these safeguards.

COMMON SCENARIOS

Practice staff disclosing patient information in public

Your practice manager telephonically shares confidential patient information with a medical scheme whilst sitting at the front desk of your waiting room that is filled with patients.

- It is your responsibility that patient confidential information is always protected and transmitted securely without breaching confidentiality.
- Train staff to discuss patient information in private areas and through secure channels.

Outsourced physical storage damaged

You have a contract with a storage company to keep your patient files off-site. Following a burst water pipe, some of the files have been damaged severely.

- Before outsourcing the management of your files, you should inspect the premises or request evidence of appropriate measures being in place to avoid physical damage and security breaches.
- Even if the damage occurred at their premises, you remain legally accountable as the record custodian.



Cyber breach of practice computer

Your patients' records are accessed following the hacking of your practice manager's computer.

- As the custodian of the records, it is your responsibility to ensure that relevant security measures are in place to prevent illegitimate access to records. This includes:
 - Strong passwords and encryption;
 - Training of your staff in basic online IT security;
 - Limiting access to authorised users only.
- If a breach occurs, POPIA requires you to notify both the Information Regulator and affected patients as soon as reasonably possible.

Transfer of patient records on practice closure

You close your practice and a colleague agrees to take over patient files, but your software systems are incompatible (i.e. digital data cannot be transferred easily).

- You must ensure records are securely converted (e.g. to PDF or encrypted format) and remain readily accessible to the successor practitioner.
- It is your responsibility to ensure that patients' information is easily accessible.
- Patients should be notified of the transfer and advised how to access their records thereafter.



You can delegate the task of keeping and managing records, but never the responsibility.

Accountability always stays with the practitioner.

WHAT MUST I DO WHEN A MEDICAL FUNDER (MEDICAL AID/INSURER) REQUESTS MY PATIENT'S CLINICAL RECORDS?

A medical funder (medical aid or insurer) is not automatically entitled to your patient's full clinical records. They may only receive information necessary to validate or audit a claim with the patient's informed consent, or as otherwise permitted or required by law.

However, most patients sign a general consent form with their medical scheme or insurer when they join, which allows the funder to request relevant medical information to authorise treatment or process claims. This means that, in most cases, you do not need to obtain new consent from the patient each time there is a legitimate and purpose-specific information request, provided that:

- the information requested falls within the scope of the patient's consent; and
- you disclose only what is necessary and relevant to the specific purpose.

However, consent forms differ. Some may cover only the main member and not the dependent or may limit the type of information that can be shared.

If there is any uncertainty, you should verify the scope of the consent before disclosing information.

In practice:

- If you receive a valid, purpose-specific request (e.g. to pre-authorise a procedure or process payment for treatment rendered), you may share information applying the **"minimum necessary" principle**.
- Provide only the details required for that purpose — such as diagnosis, treatment plan, or test results — and not the patient's entire medical history. If a request seems unusually broad or outside the scope of consent (for example, asking for "all medical records" or "complete notes"), pause and clarify the scope with the funder and/or confirm with the patient before releasing information.
- Keep a copy of the request, the patient's consent (or proof of funder's authority), and the records disclosed in the patient's file.
- As a good practice safeguard, you can include a clause such as the following on your practice's patient registration forms:

"I consent to the release of relevant medical information to my medical scheme/insurer for the purposes of processing claims, authorising benefits, or managing my membership. I understand that only information necessary for these purposes will be shared, and that my confidentiality will otherwise be protected."



Even where the patient's consent exists with their scheme, you remain responsible for protecting confidentiality by limiting disclosure to what is necessary.

WHAT MUST I DO WHEN AN EMPLOYER REQUESTS MY PATIENT'S CLINICAL RECORDS?

Employers do **not** have the same rights as medical funders to request relevant medical information. Even if they are paying for treatment or medical aid membership, they cannot automatically access a patient's clinical records. Contrary to requests by medical funders, patient consent cannot be assumed when employers request clinical information.

In practice, all patient information is confidential and may only be disclosed to an Employer:

1. With the patient's informed consent, or
2. As required or permitted by law (e.g. in limited statutory circumstances such as notifiable diseases or fitness-for-duty assessments conducted under specific legislation).

What you provide should usually be limited to a medical certificate or a short report (not the full clinical record) confirming:

1. Fitness for work; or
2. The expected period of incapacity or workplace restrictions.

Only if the patient specifically authorises release of more detailed information should you disclose it, and even then, restrict it to what is necessary for the purpose.

Special cases where disclosure may be legally required

In limited contexts, certain laws may authorise or require disclosure without express consent, for example:

- Occupational Health and Safety Act 85 of 1993: where medical surveillance or fitness assessments are part of statutory workplace health programmes (e.g. exposure to hazardous substances).
- Compensation for Occupational Injuries and Diseases Act 130 of 1993: for reporting work-related injuries or diseases.
- Notifiable diseases under public health regulations (e.g. TB, COVID-19).

Even in these cases, disclosure must still comply with confidentiality, proportionality, and security requirements.

SOME SCENARIOS

An employer asks for an employee's "full medical file" before allowing them back to work.

- This is not appropriate.
- Instead, with patient consent, you issue a medical certificate confirming fitness for duty, without diagnosis details.



An employer wants more detail about a chronic illness.

- Unless the patient expressly consents, do not share clinical notes.
- You may, if authorised by the patient, provide a short report that addresses only work capacity or necessary accommodations within the workplace.



***Employers do not have automatic access to medical records.
Always get patient consent first, and limit disclosure to a certificate or
focused report unless agreed otherwise by the patient.***

For a comprehensive overview, practitioners are referred to
the ethical guidelines contained in Booklet 9
found at www.hpcs.co.za/ethics.
