THE SOUTH AFRICAN SOCIETY OF OCCUPATIONAL MEDICINE

SASOM
South African Society of Occupational Medicine
FOUNDED IN 1948

GUIDELINE ON MEDICAL RECORDS IN INDUSTRY

GUIDELINE DOCUMENT 16

SASOM
South African Society of Occupational Medicine
FOUNDED IN 1948

16

THE SOUTH AFRICAN SOCIETY OF OCCUPATIONAL MEDICINE

GUIDELINE ON MEDICAL RECORDS IN INDUSTRY

GUIDELINE DOCUMENT

Author:
Dr JNR Lapere

Peer reviewed by:
Dr F Fox
Dr G Kew
Dr H Williams

ISBN: 978-1-919727-73-8

First Revision: 2014
Third Revision: 8 June 2023

TABLE OF CONTENTS

Transmittal note

Reason for revision:

Since the last publication

1. The relevant HPCSA guidelines have been updated.
2. The Protection of Personal Information Act (Act 4 of 2013) has taken effect.
3. Queries were received by SASOM in respect of medical records.

1. Introduction

1.1. A patient's medical record is the longitudinal collection of that 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.

1.2. Medical records include hand-written or electronic contemporaneous notes by all health practitioners attending health care, communications between practitioners, laboratory results, imaging, graphs, audio-visual records, print outs of monitoring, any forms completed during the health interaction, death certificates and autopsy reports.

1.3. Maintaining adequate medical records is a general requisite in medicine. Besides being a legal and ethical requirement, the keeping of accurate and up-to-date patient records is fundamental to good professional practice.

1.4. For registered medical practitioners, the purpose of keeping patient medical records is to be a reminder of what has been found, decided on or has been done, to promote and ensure continuity of care, and to provide evidence of the standard of care. Medical records can be used to promote good clinical practice, to conduct clinical audits, to promote teaching and research, for administrative purposes, as evidence for occupational disease and injury compensation and as evidence during litigation.

1.5. There is a statutory duty to create, maintain, safeguard, retain or delete medical records containing prescribed information for every user of health services.

1.6. Medical records are subject to Information legislation for both access by parties and for the protection of the personal information which they hold.

1.7. All standards applicable to medical records apply equally to occupational medical records; additionally, the creation, maintenance, control, retention and access of occupational medical records of employees is a duty of the employer, the occupational medicine practitioner, the person in charge of an occupational health service and the employer's Information Officer.

1.8. It is important that the occupational medicine practitioner (OMP) and any person involved in the management of occupational medical records at an employer is fully versant with the statutory duties

defined in the applicable legislation and the ethical guidelines of the Health Professions Council of South Africa.

1.9. Ownership and control, format and quality, storage and safety, access and retention of occupational medical records, all necessitate planning and ongoing management; the standards for such management are well defined in general medicine, but there are specifics applicable to occupational medical records, which are the subject of this Guideline.

1.10. The updates in this guideline emanate from the activation of the Protection of Personal Information Act ('POPI Act'), changed labour legislation and the revised ethical guidelines from the Health Professions Council of South Africa (HPCSA).

1.11. Managing hard- or soft copy medical records in industry forthwith requires formal written procedures, training, appointment of accountable persons, internal audit of compliance and continuous improvement.

2. Scope of this guideline

2.1. This Guideline formulates a standard for the management of occupational medical records.

3. Types of occupational medical records

3.1. Medical records may be hard copy only, soft (electronic) copy only or a mixture of both.

3.2. The occupational medical records may consist of separate or integrated personal records of employees' health data relating to:

a. Fitness for work medical examinations.
b. Health surveillance medical examinations.
c. Sick certificates.
d. Sick absence and fitness for duty assessments and reports.
e. Ill health incapacity assessments and reports.
f. Primary medical care, including all interventions at the workplace.
g. Injury on duty and occupational disease management records.
h. Special issue-based records.

3.3. Fitness for work medical examinations

a. Fitness for work records relate to the assessment of an employee's fitness to perform risk work.
b. Where special testing is required, the dated records of these tests must accompany the medical record.
c. Fitness for work records are subject to specific legislation[1] and access may be requested by Inspectors of Government Departments (e.g., Department of Labour, Department of Mineral Resources and Energy etc.).

3.4. Health surveillance records

a. Health surveillance records document pre-placement-, transfer-, periodical-, special surveillance-, exit- or post-employment occupational medical examinations and are linked to the occupational risk profile, including:
    i. Health risks and the level thereof, and
    ii. The use of special- and or personal protective equipment.
b. Where special testing is required, the dated records of these tests must accompany the health surveillance record.
c. Biological monitoring results are included and linked to the medical record.
d. Health surveillance records are subject to specific legislation and access may be requested by Inspectors of Government Departments. As with fitness for work records, these records should be kept separate from the primary health care records.

3.5. Sick certificates, sick absence and fitness for duty assessments

a. Sick certificates may be kept in the medical file and are confidential documents.
b. Return to work assessments or fitness for duty assessments, which may include alcohol- or drug tests, are preferably kept separate from health surveillance or fitness for work records.

3.6. Ill health incapacity assessments

Records of ill health incapacity assessments, disability assessments and corresponding reports to the employer or to an underwriter.

3.7. Primary medical care interventions at the workplace

Records of primary medical care interventions at the workplace include communication with the employee's treating doctors, copies of pathology tests or imaging records, clinical records of primary care consultations etc.

3.8. Injury on duty and occupational disease management records

Injury on duty and occupational disease management records may include records generated at the

[1] Occupational Health and Safety Act (Act 85 of 1993), Mine Health and Safety Act (Act 29 of 1996), National Health Act (Act 61 of 2003).

employers' occupational health service, records from treatment by other doctors, statutory reporting forms and communications from the Compensation Commissioner or Insurer.

3.9. Special issue-based records,

Records relating to disability assessments for underwriters or for the purpose of the employer's employment equity program, records relating to notifiable health conditions (such as the vulnerability assessment in the 2020 Covid-19 pandemic) etc.

4. The lifecycle of the occupational medical record

4.1. The occupational record is based on the occupational medical examination, requiring questioning, examining and testing the employee at the request of:

a. The employer in the case of fitness for work, health surveillance, sick absence, fitness for duty and ill health incapacity assessments.
b. The employee in the case of primary medical care, injury on duty and occupational disease assessments.

4.2. Processing health information in a medical record

a. A medical record is the result of the 'processing' of personal health information, i.e., the 'collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation and use of data concerning a person's health'.
b. Upon performing an occupational medical examination, the OMP is obliged to process the personal health information, keep a medical record and, at times, issue a certificate requested by a third party.
c. The duty to keep a medical record vests with the
    i. OMP, as per the National Health Act, OHS Act and MHS Act.
    ii. The employer as per the labour acts, OHS Act, MHS Act, transport acts etc.

4.3. Communication (further processing) of health information and access to the medical record.

a. Some occupational health information and access to the health record needs to be shared with other members of the occupational health team, including current and future OMP's, professional nurses, technical staff (audiology, spirometry), administrative staff, IT personnel.
b. Occupational health information must be reported to the employer, e.g., fitness for work certificates, ill health incapacity assessments, occupational disease, health surveillance abnormalities etc.
c. The employee and other parties may request access to the medical record.

4.4. The medical record must be stored and archived; these processes require safeguarding from physical and security risks.

4.5. The lifecycle of the medical record may end with the destruction of the medical record or the deletion or de-identification of the personal data.

4.6. For each of the processes in the lifecycle of the medical record, risk-based procedures must be implemented, maintained and compliance auditing must ensure continuous improvement.

4.7. The length of time that the record must be retained may vary according to the specific legal requirements concerning the exposures in the workplace (see 'retention of medical records and statutory retention periods').

5. Separation of medical records

5.1. There is a distinct advantage in physically splitting medical records which emanate from different statutory requirements.

5.2. The following should be considered.

a. Keep occupational health data (for fitness for work and health surveillance) as a separate entity: the employer has a statutory duty to keep these records and may require access. Inspectors of the Department of Employment and Labour or of the Department of Mineral Resources and Energy have a governance duty in respect of these records.
b. Keep wellness, primary care data, medical reports and certificates relating to non-occupational illness as a separate entity. Unless the employee consents, an employer or inspector have no business with these records.
c. Keep occupational injury and disease records separate as these are governed by specific legislation.

6. Legal and other standards for occupational medical records

South African Legislation

6.1. Health legislation

a. National Health Act (Act 61 of 2003).
b. Nursing Act, 2005 (Act 33 of 2005).
c. Hazardous Substances Act (Radiation) (Act 15 of1973).
d. Medicines and Related Substances Control Act (Act 101 of 1965).
e. Mental Health Act (Act 17 of 2002).
f. Health Professions Act (No 56 of 1974) and notices from the Health Professions Council of South Africa:

i. General ethical guidelines for the health care professions.
ii. Guidelines for the Management of Patients with HIV Infection or Aids.
iii. Confidentiality: Protecting and Providing Information.

iv. Guidelines on the Keeping of Patient Records.
v. Seeking patient's informed consent: ethical considerations.

6.2. Occupational health and safety legislation

a. Civil Aviation Act (Act 13 of 2009).
b. Compensation for Occupational Injuries and Diseases Act (Act 130 of 1993).
c. Merchant Shipping Act (Act 57 of 1951) & Merchant Shipping Act Regulations 2004.
d. Mine Health and Safety Act (Act 29 of 1996).
e. National Road Traffic Act (93 of 1996).
f. Occupational Diseases in Mines and Works Act (Act 208 of 1993).
g. Occupational Health and Safety Act (Act 85 of 1993).
h. Railway safety Regulator Act (Act 16 of 2002).
i. South African Maritime Safety Authority Act (Act 5 of 1998).

6.3. Labour legislation

a. Basic Conditions of Employment Act (Act 75 of 1997).
b. Labour Relations Act (Act 66 of 1995).
c. Employment Equity Act (Act 55 of 1998).

6.4. Information legislation

a. Promotion of Access to Information Act (Act 2 of 2000).
b. Protection of Personal Information Act (Act 4 of 2013).
c. Electronic Communications and Transactions Act (Act 25 of 2002).

6.5. Other

a. Criminal Procedure Act (51 of 1977).

National and international standards

6.6. ISO/IEC27002:2013 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC).

6.7. ISO 27799: 2016 – Health Informatics: Information Security Management in Health.

Reference documents

- Medical Records in South Africa: An MPS Guide © Medical Protection Society 2016.

7. Overall impact of legislation on the management of medical records

7.1. Introduction

a. The creation and lifecycle management of medical records is a statutory duty in terms of health and labour legislation.
b. The medical record contains personal information and is therefore also governed by information legislation.
c. This mixture of legal requirements creates essential characteristics and the rules for medical record management.

7.2. Medical records in information legislation

a. The medical record is subject to the requirements of the Promotion of Access to Information Act (PAI Act) and a party may request access in the prescribed manner.
b. The medical record is subject to the requirements of the POPI Act; a medical record, its lifecycle and all participants therein must conform to this act and meet the universal conditions of accountability, limitation on processing, purpose specification, limitation on further processing, quality, openness, security safeguards and data subject participation (see FAQ).
c. The POPI Act is superior to any other legislation that regulates the processing of personal information unless this legislation provides for conditions that are more extensive, in which case, the extensive conditions prevail.

7.3. Medical records in health legislation

a. Health legislation and ethical rules concerning medical records may provide for such more onerous standards than the POPI Act.
b. The HPCSA requires that medical records are comprehensive, contemporaneous, have integrity, be attributable, accessible and securely stored; they must include sufficient information and detail for other health care providers to assist with or take over care.

7.4. Medical records in labour legislation

a. The Occupational Health and Safety Act ('OHS Act') and the Mine Health and Safety Act ('MHS Act') impose a duty on an employer to perform risk-based fitness for work and health surveillance medical examinations and keep medical records.
b. The creation, maintenance, management, security, access control and retention of the medical records of these occupational medical examinations is an employer-duty.

8. Impact of the POPI Act on the OMP and medical record management

8.1. Introduction

a. Lawful processing of health information is subject to conditions set in the POPI Act.
b. There are other legal and ethical requirements, applicable to the OMP, which set more onerous or additional requirements for the processing of health information.

8.2. Accountability

The OMP, when Responsible Party, is the overall accountable person for the life-cycle of the occupational medical records and must ensure compliance by contracted operators or employees with delegated authority.

8.3. Processing limitation

a. Occupational medical records must only contain what is adequate and relevant.
b. The OMP must, at all times, be able to justify the lawfulness of the processing of the information in the occupational medical record.
c. The collection of an employee's personal information must be direct from that employee, unless the employee has consented to collection from another source.

8.4. Purpose specification

a. The occupational medical records fulfil a specific purpose and the data subject must be aware of this purpose.
b. Retention must be restricted to the statutory requirement or authorisation.
c. Identifiable data must be destroyed or deleted when retention is no longer authorised.

8.5. Limitation of sharing of information ('further processing')

a. OMPs must only share health information with other parties if this is part of the purpose for which it was collected (e.g., treatment, issuing a medical certificate of fitness to the employer).
b. In all other instances, the employee must consent, unless there is a serious and imminent threat to public health or public safety or to the life or health of the employee.

8.6. Information quality

a. The OMP must ensure that the personal information is complete, accurate, not misleading and updated where necessary.

8.7. Openness and privacy notification

a. The OMP must ensure that every employee, whose data are processed, has received notification from the Responsible Party.
b. This privacy notification must include:
    i. What information is being collected, and any source other than directly from the employee.
    ii. The name and address of the Responsible Party.
    iii. The purpose for which information is being collected.
    iv. Whether the employee may supply the information voluntarily or whether this is mandatory.
    v. The consequences of a failure on the part of the employee to provide the information.
    vi. Which law(s) authorise or require the collection of information.
    vii. Whether the Responsible Party intends to transfer information to a 3rd country or international organisation (e.g., through servers, drop box, clouds etc.).
    viii. The level of data protection which these third parties guarantee.
    ix. Any planned recipients or category of recipients of the information (such as HR, line management, nursing staff, other OMPs appointed by the employer etc.).
    x. The employee's right of access to and right to rectify personal information.
    xi. The employee's right to object to the processing of health information, the right to lodge a complaint with the information regulator and the contact details of the information regulator.

8.8. Security

a. The OMP (as Responsible Party) is responsible for the confidentiality of health data.
b. The OMP must prevent loss of, damage to, unauthorised- access or -destruction of medical records.
c. The Responsible Party must establish, maintain, regularly audit and update risk-based safeguards. The standard of these safeguards must be based on information security practices and procedures applicable in healthcare services.
d. The OMP, as Responsible Party, must enter into a written security contract with every operator.
e. Employees of the OMP must be instructed that they may only process health information if authorized, that all personal information must be treated as confidential and not disclosed unless required by law or in course of the proper performance of their duties.

8.9. Data subject participation

a. Employees can request the Responsible Party for a record or description of the health information.
b. Employees can request to correct or delete certain data or request destruction or deletion of health information which may no longer be retained.

9. Notification and consent(s) in respect of processing health information.

9.1. Consent may be required for the OMP to (1) perform the occupational medical examination, (2) for keeping a medical record and (3) for sharing of and access to this record.

9.2. Consent and the HPCSA

a. HPCSA rules on consent in general

i. The HPCSA requires consent for health investigations and treatment during clinical care, for performing health screening or testing to detect genetic predispositions or early signs of debilitating or life-threatening conditions, for the release of ICD-10 coding to the medical scheme and/or to the other health professionals, for the sharing of information with members of a healthcare team providing a health service to a patient and for disclosure to third parties, including the employee's employer.

ii. The HPCSA does not require express consent to share relevant personal information with other practitioners to enable a specific treatment, once the patient has consented to treatment.

iii. The HPCSA does not require patient consent to hand over medical records, in the event that a medical practice is taken over by another practitioner (the guideline only refers to the case where the health practitioner in private practice passes away).

iv. The HPCSA guideline on patient records states that the conditions in the POPI Act should be complied with and read in conjunction with Ethical Booklet 4- Seeking patients' informed consent: The ethical considerations, Ethical Booklet 5- Confidentiality: Protecting and providing information, and other rules and regulations of the HPCSA.

v. On further disclosure of health information, in general, the HPCSA will hold an OMP to the rule: '*If you decide to disclose confidential information you must be prepared to explain and justify your decision'*.

b. HPCSA on consent to perform an occupational medical examination.
The HPCSA does not have an express requirement to obtain employee/patient-consent for the occupational medical examination.

c. HPCSA on the recording of an occupational medical examination's findings in a medical record.
The HPCSA does not have an express requirement to obtain employee/patient-consent for the recording of health information in the medical record.

d. HPCSA on sharing health information or the medical record.

i. The HPCSA requires that the sharing of information with members of a healthcare team providing a health service to a patient (including inter-council, as would be the case when sharing with a professional nurse), is subject to the patient's consent to disclosure to the other healthcare practitioner.

ii. The HPCSA requires that, whenever the OMP writes a report to the employer, informed consent should first be given by the employee.

iii. The HPCSA rules are silent on the giving of access to medical records to a new OMP in a practice or appointed by an employer, except that the cut-off standard is set at compliance with the conditions in the POPI Act.

9.3. Consent in the POPI Act .

a. Consent to process health information in the medical record.

i. The medical record may be recorded and kept by the OMP without patient consent as this a legal requirement for the medical practitioner.
ii. Occupational medical records at an on-site clinic, as prescribed by the OHS Act and MHS Act, may be recorded and kept without patient consent as this a legal requirement for the employer, as Responsible Party.
iii. Processing health information in an occupational health setting may be done without patient consent where this is necessary in terms of the employee's employment contract and where the holding of a medical record is an obligation imposed by law on the responsible party (as per OHS Act and MHS Act).
iv. Primary care medical records are also permissible without patient consent as this record protects a legitimate interest of the patient, as data subject.

b. Notification when processing health information in the medical record.
The POPI Act requires that the Responsible Party must ensure that every employee, whose data are processed, has received the prescribed notification.

c. Sharing health information with others.

i. If the patient/employee consents to the sharing, then it is permissible.
ii. As the POPI Act dictates that, where other legislation provides for conditions that are more extensive, these extensive conditions prevail, the HPCSA's consent requirements regarding members of a healthcare team and the employer apply.
iii. As to the access to medical records for a new OMP in a practice or appointed by an employer the POPI Act makes sharing permissible without express consent (see FAQ).

10. Accountability for occupational medical records

10.1. Statutory rules for accountability

a. The PAI Act regulates access to any information held by a party and defines duties for an Information Officer.
b. The POPI Act regulates the protection of personal information, including health information. This act defines duties for the Responsible Party, the Information Officer, the operator and the person with delegated authority.
c. The National Health Act regulates the lifecycle of a medical record held at a health establishment and defines the duties of a person in charge of such establishment.
d. The Health Professions Act defines the rules of conduct for practitioners registered with the HPCSA, including the practitioner's accountability for medical records.

10.2. The Responsible Party

a. The person who determines the purpose of and means for the processing of health information is the Responsible Party and is the overall responsible person for the life cycle of the

occupational medical records.

b. The Responsible Party must ensure that all conditions for the lawful processing of health information are complied with.
c. Where OMPs contract their occupational health services to employers, it is important that the Responsible Party, for the resulting occupational medical records, is identified.
    i. At an on-site occupational health service, the employer, owning the on-site occupational health service, is likely to be the Responsible Party for the medical records.
    ii. At an off-site occupational health service, where the OMP operates a private occupational health service, the OMP is the Responsible Party for the medical records.

10.3. Operator and person with delegated authority

a. An 'operator' is a person who processes health information for the Responsible Party in terms of contract or mandate, without coming under direct authority of the Responsible Party.
    i. This could, for instance, be an OMP offering on-site occupational health services under a service level agreement with an employer.
    ii. This could be cloud-based company contracted to the OMP's private practice for the storing of medical records.
b. A person with 'delegated authority' is a person contracted or mandated to process personal information for the Responsible Party and who works under direct authority of the Responsible Party.
    i. This could, for instance, be a professional nurse or OMP offering on-site occupational health services under an employment contract with an employer, or a data capturer or an administrative clerk.
    ii. It could also be the practice nurse in a private OMP practice.
c. The Responsible Party must ensure that an 'operator', 'person with delegated authority, or anyone processing health information on behalf of a Responsible Party does so with the knowledge or authorization of the Responsible Party.
d. It is thus important for the OMP, contracted to offer occupational health services to an employer, to identify that OMP's designation and corresponding duties in respect of occupational medical records and the processing of health information.
e. The operator and the person with delegated authority must comply with all the Responsible Party's processing requirements, must limit processing to the extent of the authority given by the Responsible Party and are bound by the statutory duty of confidentiality at all times.

10.4. Information Officer

a. The PAI Act and the POPI Act define that every organisation has an Information Officer by default and that it is compulsory for Information Officers to register with the Information Regulator.
b. The Information Officer's responsibilities relate to all information processed by the Responsible Party and, with respect to health information, include, the duty to ensure that:

i. A compliance framework is developed, implemented, monitored and maintained.
ii. A personal information impact assessment is done to ensure lawful processing.
iii. A manual is developed, monitored, maintained and made available.
iv. A system is in place to process requests for information.
v. Internal awareness sessions are conducted regarding the legal- and good governance management of personal information.
vi. There is encouragement of compliance with the conditions for the lawful processing of personal information (e.g., develop policy and procedure for the handling of medical records).
vii. There is appropriate management of requests for access to medical records or to correct personal information in medical records.
viii. Working with the Information Regulator.

c. At an employer who is a juristic person (e.g., Close Corporation, Pty (Ltd)), the Information Officer is the Chief Executive Officer, Managing Director or equivalent; it may also be any person duly authorised by the above.
d. A private OMP operating as natural person, is the Information Officer of the practice or may authorise another person; in a partnership-practice, the Information Officer is any partner or any person duly authorised by the partnership.
e. OMP's appointed by employers should identify who the employer's Information Officer is.
f. A Guidance Note On Information Officers And Deputy Information Officers is available at https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf.

10.5. Person in charge of a health establishment

a. An on-site occupational health clinic or the private practice of an OMP is a 'health establishment'.
b. The National Health Act requires the designation of a person in charge of each health establishment.
c. This person in charge must ensure that,

i. For every patient using the health services at the establishment, an appropriate medical record is created and maintained, containing the prescribed information.
ii. Control measures are in place preventing unauthorised access to medical records and to the storage facility.
iii. The confidentiality of patient information is assured.
iv. Only authorised health care providers have access to medical records for purposes of treatment.
v. Any disclosure of information contained in the medical records is only permitted if any of the following conditions prevail:
- The employee consents to that disclosure in writing.
- A court order requires that disclosure.
- Any law requires that disclosure.
- Non-disclosure of the information represents a serious threat to public health.

d. OMP's appointed by employers should identify who the employer's person in charge of the on-site clinic and its records is.
e. Whilst some duties of the Information Officer and those of the person in charge of a health establishment may coincide, it is advisable that these appointments are kept separate; an important consideration is that the Information Officer's duties concern all information held by the Responsible Party (see FAQ for a list), whereas the person in charge of a health establishment's accountability for personal information is limited to the medical records.

10.6. Health Professions Act and the duties of the OMP with respect to medical records

a. With respect to medical records, the rules of conduct for practitioners registered under the Health Professions Act and the HPCSA guidelines on the keeping of patient medical records, determine that the OMP must, at all times act in the best interests of patients, respect patient confidentiality and privacy and keep accurate patient records.
b. This means that, ultimately, the OMP, as registered person, may be held accountable for the standard of medical record control.

10.7. The OMP in private practice

c. OMPs in private practice are the practice's Responsible Party, their own Information Officer and assume the responsibility of the person in charge of the health establishment. The OMP may appoint a staff member to be the person in charge of medical records and a deputy Information Officer.
d. With respect to personal information held by the practice, the OMP must set up the required controls for compliance. Considering that a medical practice holds a large volume of personal information other than patient's health information, these (overall) controls are outside the scope of this guideline (see FAQ).
e. With respect to the medical records, the OMP must ensure that the following is in place:

i. A practice policy and appropriate procedures for the lifecycle of medical records.
ii. Training of all employees or locums who access or handle medical records.
iii. Privacy arrangements with employees and locums (agreement or clause in the contract).
iv. The mandatory notification to employees as data subjects.
v. The applicable written consents.
vi. A Processor's Supplier Data Protection Agreement with contractors, for IT, data storage, archiving of medical records etc (i.e., where another person is designated as permissible processor of health data).
vii. A security risk assessment, security safeguards and compliance verification.
viii. The appropriate handling of requests from patient/employees/data subjects.
ix. The appropriate handling of requests for access to or copies of health information or records.
x. The practice's Promotion of Access to Information Manual.

11. Ownership of occupational medical records

11.1. Healthcare records generally belong to the person who creates or pays for them: employers who set up an occupational health service and pay for the cost of the medical records are the owners of such medical records.

11.2. Employees have rights concerning the information contained in their occupational medical records, but they do not normally own the actual documents or electronic files. The exception is where the employee would have paid for records or images.

11.3. Records owned by the employer should be retained by the employer and copies must be made available to an employee (or the employee's medical practitioner or representative) on request by the employee.

11.4. When contracting for services with an employer, the OMP is advised to discuss and enter into an arrangement as to the ownership of medical records, both at the employer's workplace and at the OMP's surgery.

12. Quality requirements for medical records

Quality medical records are comprehensive, contemporaneous, have integrity, are attributable, accessible and securely stored.

12.1. Quality medical records must be comprehensive.

a. In general

i. A medical record must contain all the significant information needed by current and future healthcare providers in order to be sufficiently informed about the patient's history, clinical assessments, tests, treatment and all relevant reports.

ii. An entry should be made in the medical record on each occasion that a patient is seen by a doctor and any communication related to a patient's clinical condition and care belongs in the healthcare record.

iii. The HPCSA has compiled a general content requirement for a medical record, as a minimum to meet the comprehensiveness requirement (see FAQ).

b. The Occupational Health and Safety Act and the Mine Health and Safety Act specify risk-based significant health information to be recorded and retained in the medical record.

12.2. Quality medical records must be contemporaneous.

a. Records must be made at the time of each patient interaction or as soon as possible thereafter.

b. Late entries and addenda must be noted as such ["Addendum to entry made on [date and time]"], and reasons for such belated entries must be recorded.

12.3. Quality medical records must have integrity.

a. Check the patient/employee's identity.
b. Clear, legible in non-erasable ink.
c. Accurate.
d. Find a balance between brevity and comprehensibility; the briefer, the more open to misinterpretation.
e. Stick to facts and objective findings.
f. Use 'quotation' mark when documenting hearsay and identify the source.
g. Unambiguous + avoid using abbreviations that may not be understood in the context of multidisciplinary care.
h. No derogatory language.
i. An entry must never be deleted or obliterated, even if erroneous or misleading: all corrections must be made using a single black line to cross out the error, add the amendment , signature , name (in block capitals), date and time.
j. Tests recorded on thermal paper must be preserved by making a non-effacing copy.
k. Pages must be in the correct order, all pages must identify the patient and information must be filed chronologically in the correct section.
l. Integrity requires a constant process of review and verification at the point of care (in occupational health, this may include confirming name, designation, workplace, workplace exposures, changes to history or chronic conditions or management thereof etc.); if anything in the records seems unusual or illogical, check its validity.

12.4. Quality medical records are attributable.

a. Any person making an entry in a medical record must be identifiable.
b. When multiple healthcare professionals are responsible for a patient medical record, each entry must be dated and timed; the HPCSA defines this standard as: the record must be signed in full with the name of healthcare professional in block letters and the contact details.

12.5. Quality medical record management requires that records are accessible.

a. The medical record must be readily available whenever a patient is seen in a healthcare setting or facility.
b. Information must be stored in a manner that allows easy access to all important information.
c. Considering the long retention (and use) requirements of occupational health date, the average medical record may contain a considerable amount of data. Critical information and special needs should be prominent and this may sometimes require that allergies, impacting chronic illness, high risk work exposures etc. are extracted and highlighted on a summary sheet and/or the cover.

12.6. Quality medical record management requires that records are securely stored.

a. The HPCSA and the National Health Act require that the person in charge of a health establishment must set up control measures to prevent unauthorised access to records, to the

storage facility and to any system by which records are kept.

b. The POPI Act's requirements regarding medical records are more onerous:

   i. Accountability for the integrity, confidentiality and security measures to prevent loss, damage, unauthorised access and destruction of medical records vests with the Responsible Party.
   ii. The overall standard is that appropriate, reasonable technical and organisational measures must be in place, with due regard to generally accepted information security practices and procedures applicable in the health industry and defined by professional rules and regulations.
   iii. In practice, the Responsible Party must
      - Perform a risk assessment of risks to medical records. Besides unauthorised access, the risk assessment must include theft, physical risks (such as fire, floods, vermin- See FAQ) and, for electronic records, hard- and software failures.
      - Establish and maintain appropriate safeguards against these risks.
      - Regularly verify that the safeguards are effectively implemented and updated.

c. Every occupational health service should have a record management policy in place, which is regularly reviewed and updated to keep pace with technological advances and legislative requirements.

d. Where OMPs work for employer's who are the Responsible Party, the OMP should advise and assist the employer with such a record management policy.

13. Confidentiality of medical records

13.1. Besides the ethical obligation, common, constitutional, statutory and contract law define the right of confidentiality.

13.2. Confidentiality is central to the trust between practitioners and patients: patients have a right to expect that information about them will be held in confidence by healthcare practitioners.

13.3. The HPCSA determines that, where healthcare practitioners are asked to provide information about patients, they should :

   a. Seek the consent of patients to disclosure of information wherever possible, whether or not the patients can be identified from the disclosure.
   b. Anonymise data where unidentifiable data will serve the purpose.
   c. Keep disclosures to the minimum necessary.

13.4. Healthcare practitioners must always be prepared to justify their decisions to disclose.

13.5. The obligation of confidentiality includes a responsibility to make sure that all medical records are kept securely.

a. Medical records must not be left where other people may have casual access to them.
b. Information about patients must be sent under private and confidential cover, with appropriate security measures.
c. Patients must be informed about the kind of information being held about them, how and why it might be shared, and with whom it might be shared.

14. Access to occupational medical records

14.1. Background

a. Medical records must be kept securely to prevent unauthorised access, damage or loss.
b. Access to medical records must be controlled and the Responsible Party for the medical records will always be required to justify any disclosure.
c. In many instances, the occupational medicine practitioner may also be held accountable for any breaches of confidentiality.

14.2. Authorised access in general.

a. Patients have a right to access to their medical records.
b. Information from the medical record may be made available to a third party with the written authorisation of the patient, including:

    i. Medical information made available to union, legal and other employee representatives; access should be only to information that is relevant to the enquiry.
    ii. Access rights emanating from the PAI Act: the patient or someone authorised to act on behalf of the patient can request access to "*any information that is held by another person and that is required for the exercise or protection of any rights*". This includes access to medical records. Either the patient or someone authorised to act on the patient's behalf, can request access; ordinarily the request itself is made in writing and should be responded to within 30 calendar days.

c. There is a right to the record holder to refuse access if the disclosure to the patient or the person requesting access on the patient's behalf might cause serious harm to his or her physical or mental health, or well-being. The PAI Act sets out detailed conditions in this regard:

    i. The Information Officer who is of the opinion that disclosure might result in serious harm to the relevant person, must consult with a healthcare practitioner nominated by the relevant person.
    ii. If the nominated healthcare practitioner, after viewing the records, agrees that disclosure would be likely to cause serious harm to the relevant person as outlined above, the Information Officer may still allow access to the records if satisfied that adequate counselling arrangements have been made "to limit, alleviate or avoid" such harm.

iii. The appointed counsellor must be given access to the record before access is allowed to the requester.

14.3. Authorisation for access to medical records directly from the OMP's practice.

a. Patients have a right to access to their medical records.
b. The OMP is the Responsible Party, Information Officer and the person in charge of the health establishment.
c. The POPI Act's stipulation that the most onerous of access controls must always be applied, necessitates that the OMP may only authorise access if the requirements of the National Health Act are met.
d. Where the person in charge of medical records is not the OMP in person (e.g., the practice manager), the OMP must ensure that a standard operating procedure for comprehensive occupational medical record management is in place.
e. It would be wise to include a requirement that final authorisation for any access to and release of any medical record or data may only be given by the OMP.

14.4. Authorisation for access to medical records held by an employer's on-site occupational clinic.

a. Patients have a right to access to their medical records.
b. The employer is the Responsible Party and has appointed an Information Officer and a person in charge of the health establishment.
c. The POPI Act's stipulation that the most onerous of access controls must always be applied necessitates that the employer may only authorise access if the requirements of the National Health Act are met.
d. An employer's access to medical records is *per se* also limited to authorised access and it is the person in charge of medical records who must prevent unauthorised access.
e. The person in charge may not necessarily be the occupational medicine practitioner and the employer should define who this person in charge is in a written appointment. The employer should formulate a standard operating procedure for comprehensive occupational medical record management; it would be wise to include a requirement that the occupational medicine practitioner appointed by the employer has the ultimate authority to authorise access to and release of any medical record or data.

14.5. Permissible legal access without patient authorisation.

Access to occupational medical records by a third party is legally permissible without the written authorisation of the patient or legal representative if:

a. The third party is another healthcare or supplementary health-care professional to whom the patient is referred:
    i. Only the relevant patient information must be made available.
    ii. Patients should be informed that they have a right to require that certain information is withheld.
    iii. In most cases, this will be with the patient's consent. If consent is refused, disclosure

should be made only where the safety of other parties is manifestly at stake.

b. The third party is the occupational health care staff (nurses, doctors, clinic administrators).

   i. Access within the team should be on a need-to-know basis, depending on the role of the personnel in the patient's care.
   ii. Considering that the HPCSA requires that the sharing of information with members of a healthcare team requires consent to disclosure to another healthcare practitioner, including professionals beyond the HPCSA, an OMP must obtain consent. This consent would be in line with that obtained to, for instance, issue a medical report of fitness to the employer.
   iii. For an employer, it may be sufficient to include the following in the mandatory Notification:
      - Access to health data within the occupational health team is on a need-to-know basis and governed by an employment agreement.
      - Employee/patients have a right to require that certain information is withheld.
      - Employees can object to access by team members.

c. A court orders the records to be handed to the third party.
d. If the non-disclosure would represent a serious threat to public health.
e. Where a statutory obligation to disclose certain medical facts, or records exists:

   i. The Compensation for Occupational Injuries and Diseases Act requires that the treating practitioner reports the diagnosis of an occupational disease or the description of an occupational injury and the treatment thereof to the Compensation Commissioner. The statutory forms in terms of this Act require that prescribed medical information is divulged, without which compensation will not be finalised.
   ii. Reporting of occupational diseases in terms of the Section 25 of the Occupational Health and Safety Act.
   iii. Information entered on death certificates.

14.6. Special access

The HPCSA also permits access in the following special cases:

a. Where the third party is a health care practitioner who is being sued by a patient and needs access to the records to support a defence.
b. Where the third party is a health care practitioner who has had disciplinary proceedings instituted by the HPCSA and requires access to the records for defence purposes.
c. In both these instances, access to the records is declared permissible under the rules promulgated under the Health Professions Act; but the more onerous restrictions of the National Health Act must apply, and the Responsible Party must thus seek patient consent to give access to the records.

14.7. Sharing information with management

a. Statistical information which does not allow the identification of individual employees may be released without restriction.
b. Specific medical information about an employee should be revealed to management only with

written patient consent.

c. A possible exception to this rule is in cases where an occupational disease exists or where an individual's medical condition constitutes a hazard to that employee, fellow workers or the public. In such a case every effort should be made to obtain patient consent. If consent is not obtained, the medical practitioner may have no choice but to reveal the employee's condition to management in the interests of safety; it is advised that peer counsel, consultation with the HPCSA and with a legal advisor competent in these matters is first sought prior to divulging information without patient consent.

14.8. Access to sick certificates

a. Sick certificates are a legal requirement for an employee to provide evidence of a supervening impossibility to perform work or to attend work. The onus on providing an employer with such a certificate sits with the employee. The Basic Conditions of Employment Act requires that the certificate must state that the employee was unable to work for the duration of the employee's absence on account of sickness or injury. Where the certificate includes the diagnosis, the employee's submission of the document to the employer implies consent to divulge the information to the employer and its relevant management structures.

b. Section 90 of the Basic Conditions of Employment Act defines that it is a criminal offence for any person to disclose information acquired while exercising or performing any power or duty in terms of the Act; the record of any medical examination is specifically listed with the duty to keep it confidential.

c. Sick certificates should therefore be guarded and not left to lie around in the sight of others.

14.9. Access to medical record during audits

a. Clinical audits based on physical inspection of medical records require the employee to consent to such access; alternatively, the patient information provided must be anonymised.

b. Disclosure of information should in all cases be limited to the relevant parts of the medical record.

14.10. Access to occupational medical records by inspectors of the Department of Employment and Labour

a. Inspectors may be required to investigate occupational health and safety compliance, work injuries or occupational diseases and, for this purpose, information in the occupational medical record may be relevant and requested.

b. The OHS Act includes a number of statutory references to such access to medical records:

   i. At the employer's workplace, an inspector may enter any premises, question any person, require that a record is produced to the inspector, examine, make a copy or seize the record and require an explanation of any entry in the record.

   ii. The records of the hearing conservation program, asbestos-, ergonomic-, lead-, hazardous

chemical- and hazardous biological agent- health surveillance may not be made available to an inspector unless the employee consents.

iii. Records of health surveillance for hazardous chemical agent exposure may only be made available to an occupational health practitioner.

iv. Commercial diving regulations, construction regulation, environmental regulations for workplaces (thermal exposure) are silent on access to the occupational medical records.

c. When dealing with personal information, the POPI Act is supreme and applies to the exclusion of any provision of any other legislation that may be inconsistent with an object, or a specific provision, of the POPI Act. Moreover, in respect of the medical record, the National Health Act provides for conditions for the lawful processing of personal information that are more extensive than those in the OHS Act and in the POPI Act, and therefore these extensive conditions are law.

d. Therefore, Inspectors requesting access to an occupational medical record at an employer's workplace cannot base this on an OHS Act right or requirement, but must seek to obtain the employee's consent for such access. Alternatively, the inspector may apply for a court order.

14.11. Access to occupational medical records by inspectors of the Department of Mineral Resources and Energy.

a. Inspectors may be required to investigate occupational health and safety compliance, work injuries or occupational diseases and, for this purpose, information in the occupational medical record may be relevant and requested.

b. The Mine Health and Safety Act ('MHS Act') includes a number of statutory references to such access to medical records:

i. The Mine must appoint an OMP in charge of medical surveillance.

ii. An employee's medical record must be kept confidential and may be made available only in accordance with the ethics of medical practice, if required by law or court order or if the employee has consented, in writing, to the release of that information.

iii. The legislated powers of an inspector, include that, at a mine, the inspector may enter the medical archive, may require any person who has control over a record to produce that record to the inspector, may require an explanation of any entry and may examine, make a copy or extract from the record.

iv. At the OMP's private practice and at any other place outside the Mine, an inspector requires a warrant to enter.

c. In respect of access to a medical record, the National Health Act and the duty to keep the medical record confidential defined in the MHS Act provide for conditions for the lawful processing of personal information that are the most extensive and thus, the applicable law.

d. Therefore, Inspectors requesting access to an occupational medical record at a mine cannot base this on a statutory requirement but must seek to obtain the employee's consent for such access. Alternatively, the inspector may apply for a court order.

e. Note that:

i. An inspector may inspect arrangements made by the employer for medical surveillance of

employees.

ii. An inspector may be accompanied by any other person reasonably required to assist the inspector; this means that a colleague OMP may assist with inspection of the medical record if the above conditions (court order, consent) have been met.

14.12. Access to occupational medical records by a health officer or inspectors appointed in terms of the National Health Act

a. A health officer is a person employed by the national health department, a province or a municipality, and appointed by the Minister of Health or a member of the Executive Council or the mayor of a municipal council.
b. The chief executive officer of the Office of Health Standards Compliance Board appoints health inspectors.
c. A health officer and a health inspector may enter any health establishment, at any reasonable time and, amongst other, require the person in charge the health establishment to produce any medical record held; the record may be inspected, copied or removed. A health officer or an inspector who removes a medical record must issue a receipt for it to the person in charge of the premises or health establishment, and return it as soon as practicable after achieving the purpose for which it was removed.

15. Retention of occupational medical records

15.1. Purpose of retention of medical records

a. Further the diagnosis or ongoing clinical management of the patient.
b. Continuity of medical care: the medical record facilitates continuity of care from one visit to the next, and especially in cases where more than one practitioner (medical or nursing) is taking care of the patient.
c. Baseline and follow-up of health status: occupational disease often occur years after exposure, and health surveillance records are an essential part of the ongoing health-care programme for the working individual.
d. Health information and data management: medical records may constitute useful research and epidemiological data.
e. Legal and compensation: Compensation claims and litigation actions require precise records. Records need to be kept for many years after exposure if there is a possibility of occupational disease.
f. The HPCSA lists the following reasons for the retention of documents and materials:

    i. Conduct clinical audits.
    ii. Promote teaching and research.
    iii. Be used for administrative or other purposes.
    iv. Be kept as direct evidence in litigation or for occupational disease or injury compensation purposes.
    v. Be used as research data.

vi. Be kept for historical purposes.
vii. Promote good clinical and laboratory practices.
viii. Make case reviews possible.
ix. Serve as the basis for accreditation.

15.2. Statutory requirements and restriction on the retention of patient medical records

a. The POPI Act

i. Records must not be retained longer than is necessary for the purpose for which the information was collected or processed, unless:
- The retention of the record is required or authorised by law (e.g., OHS Act).
- The Responsible Party reasonably requires the record for lawful purposes related to its functions or activities (e.g., the above HPCSA purpose and retention rules).
- Retention of the record is required by a contract between the parties.

ii. Records of personal information may be retained for longer periods for historical, statistical or research purposes if the Responsible Party has established appropriate safeguards against the records being used for any other purposes.
iii. A health professional (who uses the data 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.

b. The HPCSA determines that:

i. When statutory obligations prescribe the minimum period for which patient medical records should be kept, a practitioner must comply with these obligations.
ii. Patient medical records should ideally be stored indefinitely particularly if this can be done using an electronic format.
iii. If this is not practical, a patient medical record should be stored for at least a minimum of six (6) years as from the date that a patient medical record has become dormant (dormancy commences at the time when a patient was last treated by a healthcare practitioner); but for certain health conditions that take a long period to manifest, the records should be kept for a sufficient period to allow 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.
iv. In principle, a balance must be reached between the costs of long-term retention of records and the risk to a practitioners' defence in a matter of litigation or complaint. The value of the record for academic and research purposes, and the risks of late complications occurring, are additional considerations.

15.3. Methods of record retention

a. Hard copy records

i. Hard copies are the most acceptable form of records, especially for legal and compensational purposes.
ii. Hard copies are bulky, expensive to archive and awkward for research purposes.
iii. Hard records can easily be damaged by water, fire and insects and appropriate controls

must be in place for floods, fires, insects and vermin etc.

iv. Hard copy protection systems must ensure security and protection from environmental risks (See FAQ)

b. Microfilm records are effective and space-efficient but unwieldy for frequent retrieval and therefore not practical for records in daily use. Microfilm records are good for long-term storage of inactive records and are acceptable for legal purposes.

c. Electronic records

i. Computer records are easy for daily use, practical for management reporting, data recording and for research purposes.
ii. Electronic records are vulnerable to operator error, hardware failure and computer viruses.
iii. A main-frame computer or cloud with reliable details of date of storage may be as effective in a legal setting as a paper or microfilm record.
iv. Electronic records should be regularly backed up and the back-up system should be kept at a secure off-site location.
v. Only technology that is designed to record information once only may be used: old information must not be able to be overwritten or removed.
vi. All electronic records must be encrypted and protected by a password to prevent unauthorised access.
vii. Effective safeguards against unauthorised use or retransmission of confidential patient information must be assured and the right of patients to privacy, security and confidentiality must be protected at all times: the OMP must be satisfied that there are appropriate arrangements for the security of personal information when it is stored, sent or received by electronic means.
viii. The HPCSA advises that health care practitioners should take appropriate authoritative professional advice on how to keep information secure before connecting to a network and that they should record the fact that they have taken such advice.

15.4. Use of the internet, websites and social media in occupational medicine

The British Medical Association, the British General Medical Council and the European Council of Medical Orders have issued guidelines in respect of tele-medicine, including the use of the internet, websites and social media by medical practitioners:

Data can only be used in the interest of patients and without affecting the right to information privacy.

a. Networks must be secured, regularly verified for security leaks and must be accessible only when due access controls are applied.
b. Practitioners must use strong security passwords.
c. Adequate computer anti-virus software must be in use.
d. Computers must be closed at the end of professional activities.
e. Software support suppliers must be required to enter into contractual confidentiality agreements.

f. Computers with patient data must be solely used for professional purposes.

15.5. Occupational medicine practitioner's websites

The professional website of an occupational medicine practitioner should include a disclaimer confirming that personal data of patients will not be disclosed, and that patient confidentiality will be guaranteed at all times.

15.6. Statutory retention periods for occupational medical records

Purpose or Occupational risk exposure	Retention period after last entry
Primary medical care with no occupational exposure	6 -25 years
Fitness for work	10 years
Exposure to Lead	40 years
Exposure to Radiation	40 years
Exposure to Hazardous chemical substances	30 years
Exposure to Noise	40 years
Exposure to Hazardous biological agents	40 years
Mineworkers	40 years
Divers	6 years
Exposure to Asbestos	40 years (6 years)*
Injury-on-duty (IOD) treatment	10 years after treatment
Occupational diseases	40 years
Mining OH records	40 years

* Commercial Driving Regulation, 2022

- Employer to retain 'Regulation 7 medical surveillance' records for 40 years.
- Commercial diving school to retain 'Regulation 7 medical surveillance' records for 6 years

16. Disposal of occupational medical records

16.1. Policy and procedure

a. POPI Act

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

b. The person in charge of the occupational health unit and the occupational medicine practitioner must document a policy for disposal of records, defining the standards for record retention and the procedures for dealing with records which may be due for disposal.
c. Records earmarked for disposal must be evaluated and certified suitable for disposal by the designated authoritative person defined in the policy.
d. The authority to dispose must be documented and signed by the designated person.
e. Electronic records are subject to the Electronic Communications and Transactions Act, which requires that personal information shall be deleted or destroyed when it becomes obsolete.

16.2. Destruction of records

a. Paper records must be shredded or incinerated.
b. Electronic records may be overwritten or physically destroyed.
c. If destruction is outsourced to a contractor, a written confidentiality agreement must be entered into, and the final destruction must be certified in writing.
d. All destroyed records must be entered in a register, detailing the employee's company reference number, name, address, date of birth, the start and end dates of the records, the date of disposal and the name and signature of the person carrying out or arranging for the disposal.

16.3. Medical records of the employer who ceases activities

a. Employers governed by the Occupational Health and Safety Act

   i. If a medical record is within its statutory retention period and the employer ceases activities, the OMP or the person in charge of the medical records shall hand it over (or forward by registered post) to the relevant provincial director of the Department of Labour.
   ii. The records must include specific data listed in the relevant Regulations of the Occupational Health and Safety Act.

b. Employers governed by the Mine Health and Safety Act: Section 13(8) requires that an employer must retain medical records until the Mine closes and, when a Mine closes, the occupational medicine practitioner or the person in charge of the medical records must deliver the records to the Medical Inspector of the Department of Mineral Resources

17. Frequently asked questions

A. What are the HPCSA's minimum requirements for recording a consultation?

1. Patient medical records must be contemporaneous:

    a. This means that they must be made at the time of each patient interaction or as soon as possible thereafter.
    b. Late entries and addenda must be noted as such and reasons for such belated entries must be given.

2. Patient medical records must have integrity:

    a. They must be accurate, complete and comprehensive.
    b. They must be clear and legible.
    c. They should be kept in non-erasable ink and erasure fluid should not be used.
    d. They must be unambiguous (especially relating to the use of abbreviations).
    e. They may not be tampered with.
    f. They may not contain derogatory or similar language.
    g. They must be regularly checked.
    h. They must be in order and all pages in a written document must identify the patient to which those notes refer.

3. Patient medical records must be attributable:

    a. Any person making an entry in a patient medical record must be identifiable.
    b. When multiple healthcare professionals are responsible for a patient medical record (particularly in the case of hospital records), each entry must be dated and timed. When such an entry is made in writing (or when an electronic record will not identify the practitioner), the record must be signed in full (or by electronic means in the case of an electronic medical record).
    c. The name of the healthcare professional must be recorded alongside the signature in block letters including the practitioner's contact details.

4. Patient medical records must be accessible:

    a. The patient medical record must be readily available whenever a patient is seen in a healthcare setting or facility.
    b. Information in the patient medical record must be stored in a manner that allows easy access to all important information.
    c. Critical information related to allergies, significant idiosyncrasies and special needs should be prominently recorded to reduce the risk that these will be overlooked.

5. Patient medical records must be securely stored:

    a. The person in charge of a health establishment in possession of a user's medical 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.

6. The patient medical record should, where appropriate, consist of:

   a. All relevant clinical findings, including (but not limited to):

      i. Who is making the notation in the patient medical record (this is particularly important when multiple healthcare professionals are responsible for a patient health care record).
      ii. The times of consultation and other clinical interactions.
      iii. The full clinical history.
      iv. The clinical examination.
      v. The differential diagnosis.
      vi. The information and advice given to the patient.
      vii. The clinical decisions made and when and who made such decisions.
      viii. The decisions and actions agreed to and when these were agreed to.
      ix. When required the written affirmation of such agreements (consent forms).
      x. The treatment administered (including detailed operation or invasive intervention notes when such a procedure has taken place).
      xi. The drugs and doses of drugs given.
      xii. The investigations ordered and their results and dates when ordered and when results have been received.
      xiii. Future appointments and referrals made.
      xiv. Any other documentation relevant to a patient's health.

   b. The interactions that need to be recorded in a patient medical record include (but are not limited to):

      i. The face-to-face discussions between the patient and a health practitioner.
      ii. Progress notes when a patient is seen for review regarding a specific episode of care (e.g. while a patient is in hospital or when a particular condition requires follow-up).
      iii. Any virtual, telephonic or similar discussions and/or consultations with the patient and their relatives.
      iv. Discussions with colleagues related to the patient.
      v. All correspondence related to the care of a patient.

   c. The compulsory elements of a patient medical record are:

      i. The personal (identifying) particulars of a patient.
      ii. The full biopsychosocial history of a patient, including allergies and idiosyncrasies.
      iii. The time, date and place of consultation.
      iv. The assessment of the patient.
      v. The proposed management of the patient.
      vi. The medication and dosage prescribed.
      vii. Details of referrals to specialists and other healthcare professionals.
      viii. The patient's response to treatment, including adverse effects.
      ix. Investigations ordered and their results.

x. Details of the times that a patient was booked off work or similar activities and the relevant reasons.
xi. Written proof of informed consent when this is relevant.

B. How can a medical record be altered?

a. Medical records should preferably not be altered.
b. Strictly no information and no entry may be removed from a medical record.
c. An error or incorrect entry discovered in the record may be corrected by placing a line through it with ink and correcting it. The date of change must be entered, and the correction must be signed in full.
d. The original record must remain intact and fully legible. Erasing ink or removing sections of the record is forbidden.
e. Additional entries added at a later date must be dated and signed in full.
f. The HPCSA requires that the reason for an amendment or error should also be specified on the record.

C. What to do if a request for access of records is received in terms of the Promotion of Access to Information Act 2000?

a. The Promotion of Access to Information Act 2000 gives patients access to their occupational medical records.
b. Either the patient or someone authorised to act on the patient's behalf, can request access; ordinarily the request is in writing and should be responded to within 30 calendar days.
c. Access to medical records must only be given with the patient's consent.
d. The only ground for refusing access is if disclosure might cause serious harm to the employee's physical or mental health, or well-being. The Act sets out detailed conditions in this section: the Information Officer must consult with a healthcare practitioner nominated by the employee. If the patient lacks the capacity for nomination, a person appointed by the court to manage the patient's affairs, must make the nomination.
e. An occupational medicine practitioner employed or contracted by an employer should be versant with that employer's procedure for access to records.

D. Can a relative of an employee request access to occupational medical records?

a. Relatives have no automatic right of access to adult patient's medical records.
b. If the patient does not have the mental capacity to give consent to disclosure, the relative can apply under the Promotion of Access to Information Act 2000. See FAQ "what to do if a request for access of records is received in terms of the Promotion of Access to Information Act 2000?" for dealing with such requests.

E. When must deceased patient's records/medical information be released?

a. Deceased patients have the same right to confidentiality.
b. Information may (legally) be released to third parties with the consent of the next of kin or the

executors or an inquest magistrate.

c. It remains an ethical duty of the record holder to consider the circumstances surrounding the request for information and the potential effect which disclosure may have on the deceased person's partner or family.

F. Must a patient's medical records/information be released when a court orders to do so?

a. Record holders must comply with court orders.
b. If there are concerns about the consequences of releasing information, the record holder should address these in writing to the judge or the registrar of court.
c. Note that the threat of a court order does not constitute an authority and there is no obligation to disclosure.

G. Must a patient's records/information be released to the Police if requested or ordered by the Police to do so?

The Police has no authority or right to medical record, other than in the following situations:

a. The patient has given written consent to release the information.
b. A court orders the release of information.
c. A judge or magistrate orders the release of information in terms of the Criminal Procedure Act, or
d. The public interest outweighs the right to confidentiality; this last situation warrants, peer-, legal- and maybe HPCSA consultation prior to release.

H. Must a patient's records/information be released to solicitors?

a. Solicitors could request information relating to a claim when acting for the patient or when acting for another party.
b. When acting for the patient, information should only be released if there is a written consent by the patient or a legally recognised proxy of the patient.
c. When acting for a third party, the solicitor's request can only be considered if it is made in terms of the Promotion of Access to Information Act 2000 and the following also applies:
    i. Either the patient has given written consent to the solicitor.
    ii. Either the patient is physically or mentally incapable of giving consent or requesting the information and giving access would be in the patient's interest.
    iii. Either the patient has deceased, and the solicitor has a written consent of the next of kin or the executor.
    iv. Either the information is already publicly available.

I. What is personal information?

Personal Information means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to:

a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
b. information relating to the education or the medical, financial, criminal or employment history of the person;
c. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
d. the biometric information of the person;
e. the personal opinions, views or preferences of the person;
f. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g. the views or opinions of another individual about the person; and
h. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

J. What types of information could be processed at an occupational health practice?

a. Internal records relating to the business
b. Personnel records
c. Client records
d. Medical records of patients
e. Supplier and service provider records
f. Technical records
g. Third party information
h. Environment and market information

K. What are the POPI Act's general conditions for the lawful processing of occupational medical records?

1. The POPI Act sets general conditions for the lawful processing of personal information and additional specific conditions for medical records.

2. In general, a Responsible Party is accountable for the life-cycle of all personal information and must ensure compliance with the 8 universal conditions:

a. Accountability.
b. Processing limitation.
c. Purpose specification.
d. Limitation on further processing.
e. Information quality.
f. Openness.
g. Security safeguards.
h. Data subject participation.

3. Accountability

   a. The Responsible Party is the overall responsible person for the life-cycle of the occupational medical records.
   b. 'Operators' are persons who process occupational health information for a Responsible Party but don't fall under the direct authority of the Responsible Party. A Responsible Party must enter into an agreement with an operator, setting the conditions for lawful processing by the operator.
   c. Persons with 'delegated authority' are contracted or mandated to process occupational health information whilst working under the direct authority of the Responsible Party. A Responsible Party must enter into an agreement with a person with a delegated authority in the form of an employment contract-clause or a specific written arrangement setting the conditions for lawful processing by the person.

4. Occupational medical records are subject to a number of limitations:

   a. The processing must be lawful and not infringe on the privacy of the data subject-employee.
   b. Records must only contain what is adequate and relevant.
   c. Employee's health information may only be processed if the processing complies with an obligation imposed by law on the Responsible Party (such as the OHSA or MHSA) or the processing protects a legitimate interest of the data subject (such as for a pregnant employee) or processing is necessary for pursuing the legitimate interests of the Responsible Party (such as recording drug- or alcohol testing) or the employee has consented.
   d. The Responsible Party must, at all times, be able to justify the lawfulness of the processing of the information in the occupational medical record.
   e. Unless legislation defines a duty on the part of the employer or Responsible Party, an employee is entitled to withdraw consent to the processing of health information.
   f. The collection of personal information on an employee must be direct from that employee, unless the employee has consented to collection from another source.
   g. Health information may be processed if it is necessary for the proper treatment or care of the data subject.
   h. Registered medical professionals and healthcare facilities may process health information where this is necessary for treatment and care or for the administration of facility or professional practice.
   i. Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations may process health information. The processing may only be done, subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.
   j. Employers may process health information if required by law, for pension regulations, collective agreements and for the reintegration of or support for workers in connection with sickness or work incapacity.
   k. These responsible parties, permitted to process health information who are not subject to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the information as confidential.

5. The occupational medical records must be processed with a specific purpose and the data subject must be aware of this purpose. Retention must be restricted to the statutory requirement or authorisation and identifiable data must be destroyed or deleted when retention is no longer authorised.

6. The further processing of information (i.e., sharing with other parties) is limited to the purpose for which it was collected unless the employee consents or there is a serious and imminent threat to public health or public safety or to the life or health of the data subject or it is necessary for the proper treatment or care of the data subject.

7. Further processing may also be done with

    a. Registered medical professionals and healthcare facilities where this is necessary for treatment and care or for the administration of facility or professional practice.
    b. Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.
    c. Employers if this required by law, or for pension regulations, collective agreements and for the reintegration of or support for workers in connection with sickness or work incapacity.

8. A Responsible Party must ensure that the personal information is complete, accurate, not misleading and updated where necessary.

9. Openness

    a. An employee whose data is processed must, prior to the data being collected, receive notification from the Responsible Party.
    b. The notification must include:

        i. What information is being collected, and any source other than directly from the employee.
        ii. The name and address of Responsible Party.
        iii. The purpose for which information is being collected.
        iv. Whether the employee may supply the information voluntarily or whether this is mandatory.
        v. The consequences of a failure on the part of the employee to provide the information.
        vi. Which law(s) authorise or require the collection of information.
        vii. Whether the Responsible Party intends to transfer information to 3rd country or international organisation (note that this may be through servers, drop box, clouds etc.)
        viii. The level of data protection which these third parties guarantee.
        ix. Any planned recipients or category of recipients of the information (such as HR, line management).
        x. The employee's right of access to and right to rectify personal information.
        xi. The employee's right to object to the processing of health information, the right to lodge a complaint with the information regulator and the contact details of the information regulator.

10. Security

    a. The Responsible Party must prevent loss of, damage to, unauthorised- access or -destruction of medical records.
    b. Risk-based safeguards must be established, maintained and regularly audited and updated. The standard of these safeguards must be based on information security practices and procedures applicable in healthcare services.
    c. The Responsible Party must enter into a written security contract with every operator.
    d. In the event that healthcare information has been accessed or acquired by an unauthorised person, the operator must inform the Responsible Party and this party must immediately notify the regulator and the data subject.
    e. Persons acting under the authority of the Responsible Party must only process information with the knowledge or authorisation of the Responsible Party, treat personal information confidential and not disclose unless required by law or in course of proper performance of duties.

11. Data subject participation

    a. Data subjects can request the Responsible Party for a record or description of the health information.
    b. A data subject may request to correct or delete certain data or request destruction or deletion of health information which may no longer be retained.

L. What are the duties of an OMP in private practice, where the OMP is the Responsible Party ito POPI Act and PAI Act?

1. Register the Information Officer and deputy with Information Regulator. Appoint deputy in writing, where applicable.

2. Compile an inventory of personal information held at the practice.

3. Identify who the operators are.

4. Identify who the persons with delegated authority are.

5. Processor's Supplier Data Protection Agreement with operators and contractors.

6. Privacy rules, notification and statement for employees with delegated authority; also data protection clause for employment contracts.

7. PAI Act manual.

8. Notification to patients.

9. Lifecycle risk assessment of personal data management.

10. Data Protection Policy.

11. Document Retention Policy.

12. Standard operating procedures

    a. Personal Information management controls
    b. Data subject requests (for info (aligned with PAIA manual), for amendment, for deletion)
    c. Personal Information security breach

13. Compliance inspection and verification records.

14. Patient consents.

O. Which protection mechanisms are suitable for the environmental risks to medical records?

1. Protection from fire risks

    a. Store medical records in a dedicated cupboard and room where there is no other storage of materials.
    b. Ensure that doors are tight-fitting and kept closed as smoke damage may be caused by fires elsewhere in the building.
    c. Flammable substances must be stored properly and as far away as possible from the records.
    d. Ensure that electrical installations in the record room are installed in accordance with the legal standard + that a certificate of compliance is issued + arrange for an annual audit by an electrician.
    e. Install chemical fire extinguishers. Preferably not Dry Powder, but gas-based systems (e.g., CO_2).
    f. Do not use a sprinkler system as water damages the records.
    g. Install smoke and fire alarms, preferably a system that connects directly to the local fire service.
    h. Important paper documents should be kept in a fire-proof safe.

2. Protection from water risks

    a. Check the water reticulations (potable water, flood water from rain and downpipes, sewer reticulation) and make sure that any rupture or blockage causing a flood will not inundate the record store.
    b. If you are in a flood-prone area, store records above floor level.
    c. Basements are not a good place for archiving records.
    d. Ensure that an annual inspection of all reticulations is done.

3. Gravity

    a. Paper records can be very heavy, and cupboards must be designed to hold the weight.

b. If there is a large archive, it may be necessary to contract an engineer to check that the floor of your records room can carry the load.

4. Insects and vermin

a. Ensure a regular inspection and application of control measures by experts to keep damaging insects and rodents away.

5. General building maintenance

a. A regular building inspection and maintenance programme (legal minimum = 2 yearly).
b. Items to inspect include

i. Building integrity and structure.
ii. Roofs, gutters, downpipes.
iii. Walls and dampness.
iv. Water, sewer, plumbing and stormwater reticulations
v. Electrical and gas reticulations and installations.

F. How are existing medical records accessed/ transferred if a new OMP is appointed by an employer?

1. The following principles apply:

a. Medical professionals may process health information where this is necessary for the proper treatment and care of the data subject, or for the administration of a professional practice.
b. Employers may process health information where this is necessary for the implementation of the provisions of laws, pension regulations, collective agreements and for the management of benefits in connection with sickness or work incapacity.
c. An OMP and an employer must keep occupational medical records, which are confidential and may be disclosed only if the employee consents in writing or a court order or any law requires that disclosure or non-disclosure of the information represents a serious threat to public health.
d. Where health data are transferred from one OMP to another, such further processing, must be compatible with the purpose for which the data were collected; in the case of an occupational medical record being transferred between two OMP's contracted by the same employer, this computability stems from the following:

i. The original data collection and the hand-over process have the same purpose; i.e., ensure there is a record of the occupational medical examinations, testing and relevant data.
ii. The health information has been collected from the examinations and tests done on the employee.
iii. The consequence of handing the information to the 'new' OMP is to ensure the continuity of occupational health and safety care and to fulfil the statutory duty of the employer to have an occupational medical record.

iv. The consequences of sharing the health record are managed through the obligation of confidentiality by virtue of the OMP's profession and registration.
v. The health information has been collected in the framework of occupational health and safety and within the statutory and contractual rights and obligations between the parties.

e. Prior to the opening of an occupational medical record, the Responsible Party (employer or OMP) must notify an employee of the category of recipients who may have access to the health data. This notification should include the fact that the employer may have to appoint an alternative OMP to the one who collected the original personal data in the medical record, as part of the employer's duty in terms of OHS Act or MHS Act.
f. The HPCSA defines that, should a practice (and the medical records) be taken over by another health practitioner, the patient medical records shall be handed to the new health care professional. The new health practitioner is obliged to take reasonable steps to inform all patients regarding the change in ownership and that the patient could remain with the new health care practitioner or could request that their patient medical records be transferred to another health care practitioner of their choice.

2. In practice, the following is advised:

a. The mandatory Notification iro health data to occupational health patients or employees should include the communication that

i. The employer may need to appoint occupational health practitioners, including an OMP, alternative to the one who collected the original personal data in the medical record, as part of the employer's duty in terms of OHS Act or MHS Act.
ii. Any such new appointment includes the OMP's obligation of confidentiality by virtue of profession and registration and the confidentiality of the records is therefore safeguarded.

b. Where such a notification is in place, there is no requirement to obtain the patient/employee's consent for the handover of the medical records.
c. Where there is no such notification, it could be argued that the employees must consent to the 'new' OMP accessing the medical records.