MEDICAL RECORDS AMENDMENT

Introduction

Good clinical records are a prerequisite for delivering high-quality, evidence-based healthcare, particularly where a number of different clinicians are contributing simultaneously to patient care. Everyone involved in a patient's clinical management should have access to the information they need – otherwise, duplication of work, delays and mistakes are inevitable.

Records may be held electronically or manually, or a mixture of both. Some healthcare professionals – for example physiotherapists, occupational therapists, speech therapists and psychologists – often maintain separate departmental records, sometimes (but not always) copying important information relevant to others into the main hospital record. But in any event, a patient's clinical record is never a single document. Increasingly, GPs hold their records in computerised form and many hospitals hold a mixture of electronic and paper records. These should be cross- referenced with other files that may exist in various departments.

The information contained in clinical records may also be required for a range of non- clinical uses described below. Clinical records contain sensitive personal data and keeping them secure from prying eyes or inadvertent disclosure is a legal – as well as a professional – responsibility.

1. Why keep clinical records?

The main purpose of any clinical record is to provide continuity of care, but medical records are also used for other purposes:

- Administrative and managerial decision-making.
- Meeting current legal requirements, including enabling patients to access their records.
- Assisting in clinical audit.
- Supporting improvements in clinical effectiveness through research.
- Providing the necessary factual base for responding to complaints and clinical negligence claims.

In general, clinical records that contain sufficient information to secure continuity of care will also contain the information required for all other purposes. In the event of a complaint, clinical negligence claim or disciplinary proceedings, the doctor's defence will largely depend upon the evidence available in the clinical records. If essential information is missing, found to be inaccurate or indecipherable, cases may be lost when they could otherwise have been won. Where possible, information used for non-clinical purposes should be anonymised.

2. What are Clinical records?

Clinical records include a wide variety of documents generated on, or on behalf of, all the health professionals involved in patient care. This includes:

i. Handwritten clinical notes
ii. Computerised/electronic clinical records
iii. All personal correspondence (including letters, faxes, text messages and emails) relating to clinical matters, including correspondence sent between hospital and practice
iv. Scanned records
v. Laboratory results
vi. X-ray films and other imaging records
vii. Photographs
viii. Videos and audio recordings
ix. Print out from monitoring equipment, particularly in anaesthetics and obstetrics A&E and ICU
x. Consent forms.

3. What makes good Clinical records?

Good clinical records will contain all the information one clinician needs to take over where another left off – or, to put it another way, to allow a clinician to reconstruct a consultation or patient contact without relying on memory. This will include:

i. History – relevant to the condition including any positive and negative answers to direct questions
ii. Examination of the patient
iii. All systems examined
iv. All-important findings, both positive and negative, with details of any objective measurement such as blood pressure, peak flow, etc
v. Differential diagnosis
vi. Investigations – details of any investigations arranged
vii. Referral – details of any referral made
viii. Information – information given to the patient concerning risks and benefits of proposed treatments
ix. Consent – details of consent given to proposed investigations, treatments or procedures
x. Treatment – details of the main doses of drugs, total amount prescribed, any other treatment organised with batch number and expiry date of any medications personally administered
xi. Follow-up – arrangements for follow-up tests, future appointments and referrals made
xii. Progress – any further consultations, the patient's current condition, side effects, complications, etc.

That may seem like a daunting list, but it is all important information that someone would have to remember if it is not recorded – and both doctors' and patients' memories are

fallible. Many follow-up consultations will be with different members of the team, who will be totally reliant on the clinical records and therefore will need as much information as possible.

4. Presentation of Medical records?

Content is important, but so is presentation. If the records are unclear, inaccurate or written in such a way that they're difficult to follow, the content might as well not be there; worse than that, it could cause errors and misunderstandings. Good notes therefore have the following attributes:

i. Clear – both legible and understandable when handwritten. Each entry should be legibly signed with the date and time.
ii. Objective – clinical records should be factual and free from subjective comments about patients or their relatives. Always assume that patients will read their clinical records at some stage.
iii. Contemporaneous – clinical records should be written up at the time of, or as soon as possible after, an event to ensure accuracy. Retrospective entries should be clearly dated, timed and signed, together with an explanation of why it is being written retrospectively.
iv. Attributable – if information has been given to you by someone other than the patient, then you should record who provided the information as well as what they said.
v. Original – sometimes it is necessary to amend or alter medical records, for example if a factual error has been made. Any correction must be clearly shown as an alteration, complete with the date the amendment was made and the name of the person who made it so there can be no allegation that the alteration was an attempt to deceive anyone into thinking that it is part of the original record. (See Box 1)

BOX 1: guidelines on correcting medical records

1. Records shall not be erased or destroyed but shall be amended if incorrect.
2. Correction fluids shall not be used. The original entry shall remain visible.
3. Deletions or alterations shall be made by scoring out with a single line followed by:
    a. Signature (plus name in capitals) and counter signature, if appropriate.
    b. Date and time of correct entry.
    c. Reason for amendment.
4. Corrections shall be made as close to the original recording as possible.
5. Alterations to prescriptions shall not be permissible. A prescription that is no longer appropriate shall be discontinued and a new prescription shall be written.

5. Abbreviations

i) Abbreviations are commonly used in clinical records but can be misinterpreted and lead to mistakes in diagnosis or management. So the rule is, when in doubt, write it out – in full. Be aware, too, that patients may, if they access their notes, misinterpret innocuous abbreviations such as SOB (shortness of breath), which most lay people would interpret as an insulting reference to their origins (See Box 2 for the rules on abbreviations).

ii) Sarcastic and derogatory abbreviations have no place in clinical records – they are gratuitously offensive and sure to destroy any therapeutic relationship once found out.

BOX 2: Use of abbreviations

1. Abbreviations shall not be used.
2. In the event that abbreviations are utilized, only abbreviations which are universally understood should be used.
3. In the event that abbreviations are used, they shall be written in higher case (capital) BLOCK letters and not in a cursive script and/or in lower case.
4. In the event that abbreviations are used, on each side of each page the full term shall be used, followed by the abbreviation in brackets. Thereafter the abbreviation may be used on that page.
5. Abbreviations shall not be used on documentation which is used for transfer, discharge or external referral letters.
6. Abbreviations shall not be used on consent forms, death certificates, incident report forms and communications sent from the hospital.

Note: Drug names shall not be abbreviated.

6. Common Problems

All of the following can compromise patient safety or lead to medicolegal problems:

i. Not recording negative findings
ii. Not recording substance of discussions about the risks and benefits of proposed treatments
iii. Not recording drug allergies or adverse reactions
iv. Not recording the results of investigations and tests
v. Illegible entries
vi. Not reading the notes when seeing a patient
vii. Making derogatory comments
viii. Altering notes after the event
ix. Wrong patient/wrong notes.

Box 3: Medical records guidance on identifying patients

"Before the healthcare professional makes an entry in the patient's healthcare record, s/he shall establish that the record belongs to the patient being attended.

"This shall be done by verifying with the patient and by cross-referencing the patient's wrist band with the healthcare record."

7. Confidentiality of records

Confidentiality may seem a very straightforward principle, but translating principle into practice can be problematic. There are all sorts of situations where it is difficult to know if patient information should be shared or not – with the guardian, for example, or social workers. Confidentiality is usually referred to as an ethical issue. It is, but it is also a legal principle

i. Healthcare workers are usually bound by a confidentiality clause in their contracts.
ii. There is a common-law duty to preserve professional confidence.
iii. There are requirements under the Statutory Instrument 41 of 2004 Section 23 to keep personal data, including medical records, secure.
iv. It is a condition of registration to abide by Medical Council guidance, which includes a requirement to respect patient confidentiality.

The duty of confidentiality goes beyond undertaking not to divulge confidential information; it includes a responsibility to make sure that written patient information is kept securely. Confidential information about patients should be sent under private and confidential cover, with appropriate measures to ensure that it does not go astray.

Patients should 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. Patient information leaflets are a convenient way of notifying patients about this, but they are not sufficient in themselves. Bear in mind that few patients will bother to read the leaflets, and some may not be able to read them. It is especially important to inform patients – and to let them know that they have the right to withhold consent – if one intends to use their personal information for purposes other than their immediate care, or to share it with non-medical agents such as social workers. Confidentiality is not an absolute principle, and there are circumstances where it is permissible to disclose a patient's medical records to a third party.

7.1 Disclosure with patient consent

The first and most obvious exception is disclosure with the patient's consent. Insurance companies, employers and people involved in legal proceedings frequently request information about patients. Any disclosure must be with, and limited to, the authority provided by the patient. If this is not forthcoming, no information may be provided.

7.2 Disclosure without patient consent

Information can be disclosed without a patient's consent in two instances – if the disclosure is required by law or if the disclosure is in the public interest. This is the case whether the patient has explicitly refused consent or is incapable of giving consent.

7.3 Legal Practitioners

Legal practitioners often ask for medical information. If the legal practitioner is acting for the patient, then before disclosing confidential information, a valid signed and dated mandate should be provided.

7.4 Members of the clinical team

Patient care is usually team based and access to patient information is crucial for patient safety and continuity of care. Most patients are aware that information about them needs to be shared among the healthcare professionals delivering care, but they may not know that they have a right to ask for certain information to be withheld. They should be informed of this (via leaflets, notices and verbally) and, if they ask for information about them to be kept confidential, this should be respected. The only exception is if withholding information from staff would place others at risk of death or serious harm.

The sharing of information within the team should be on a need-to-know basis, depending on the role the member of staff has in the patient's care.

7.5 Court orders

Doctors should comply with a court or tribunal's order to disclose health records. Even if they have concerns about disclosing the records, they should still comply with the order and attach a covering letter to the judge describing their concerns. Generally, compliance with a court order should be considered mandatory, but in exceptional circumstances, if you have concerns, it may be appropriate to seek advice from a legal practitioner of Council. The mere threat of a court order is not sufficient authority to disclose.

Box 4: Exceptions to the rule of confidentiality

"In certain limited circumstances, disclosure of patient information may be required by law. These circumstances are not limited to but may include:

a) when ordered by a judicial officer in a court of law, or by a tribunal or body established by an Act of Parliament, or

b) where mandated by infectious disease regulations.

In these instances, you should inform patients of the disclosure and the reasons for it."

7.6 Child protection

In any case involving the welfare of a child, the child's best interests are paramount. This may require disclosure of some content of the medical record – or details from it – to a social worker and/or the guardian. As a matter of good practice, you should always explain to the parents that you have a duty to refer your concerns to non-medical professionals and, where possible, obtain their consent to disclosure, except in rare circumstances, where to do so would put the child at increased risk.

7.7 Where allowing access might be permissible

Situations can arise in which it is justifiable to disclose a patient's medical records to a person other than the patient. In some cases, you might have a statutory duty to share certain information – such as reporting notifiable diseases, reports to the cancer registry, etc – but in these cases it is unlikely that you will also need to provide access to the medical records themselves.

7.8 Relatives

The only relatives who have a right to request access to a patient's records are those with parental responsibility for a minor under the age of 18.

If the patient lacks capacity to consent to disclosure of his or her medical records, and those records are held by a public body, a family member may apply for access. Records held by a private organisation should only be disclosed if the holder of the records is satisfied that it would be in the patient's interests to do so – to a legal practitioner, for example, where the patient's family is pursuing a personal injury claim on his or her behalf – or to comply with a court order.

If a patient has died, the rule of confidentiality still stands, but if the records relate to publicly funded care, certain categories of people, including next of kin, can apply for access to the medical records. If the medical records are held by a private organisation, the medical records should only be disclosed with the consent of the next of kin or the executors of the deceased's estate (see Box 5).

Box 5: Next of kin

A person's next of kin is determined in the following order:

a) Spouse
b) Child or children
c) Parents or surviving parent
d) Brothers and sisters
e) Nephews and nieces.

7.9 The guardian

In general, the guardians have no more right of access to confidential information than anybody else, except in the following circumstances:

i. The patient has given consent to the release of information.
ii. In compliance with a court order.
iii. The public interest as guided by the Public Health Act.

7.10 Public interest justification to breach confidentiality

The public interest justification for disclosure usually turns on the threat of serious harm to others. This includes information held in a personal record that is "required for the purpose of preventing, detecting or investigating offences or prosecuting offenders" or "to prevent injury or other damage to the health of a person or serious loss of or damage to property". For doctors – who have a professional duty to protect the confidentiality of their patients – it would not be ethical to comply with any request for disclosure of sensitive personal information unless withholding the information would potentially have profound adverse consequences. The Medical and Dental Practitioners Council of Zimbabwe sets out the considerations that public bodies should take into account when deciding whether to withhold or disclose sensitive medical information.

Box 6: Sensitive medical information

"Particular procedures must be followed in respect of medical information where the head of the body is of the opinion that its disclosure to the person concerned may be prejudicial to his or her health or emotional well-being.

In these circumstances, if requested to do so by the person concerned, the public body shall instead release the record to an appropriate health professional nominated by the requester.

"The head has discretion to consider release of personal information to a third party only in exceptional circumstances where, on balance, he or she is of the opinion that the public interest in disclosure outweighs the right to privacy of the individual concerned, or where release of the information would benefit the individual."

7.11 Publishing case reports, photographs and recordings

The patient's consent is also required before individual case histories, photographs or recordings can be published in media that the public has access to, even if they have been anonymised.
The Medical and Dental Practitioners Council of Zimbabwe also recommends obtaining patients' express consent before using their case histories or photographs for education and training. (See Box 7.)

Box 7: Taking visual images for teaching

"Audio, visual or photographic recordings of a patient, or a relative of a patient, in which that person is identifiable should only be undertaken with their express consent. These recordings should be kept confidential as part of the patient's record."

8. Security

When it comes to protecting privacy, medical records are the public's top concern, The key to safeguarding your patients' confidential information is a sensible records management policy, incorporating strong security controls with clear policies governing access to and use of information contained in the records. There should also be policies setting out the circumstances in which certain information may and may not be disclosed and protocols for dealing with requests for access.

9. Records management

Good records management makes everybody's life easier and facilitates continuity of care, reducing the risk of adverse incidents through misplaced or untraceable records. Many patient safety incidents have been attributed to lost and misplaced files, reports placed in the wrong records, mix-ups with patients' names and poor flagging up of crucial information such as drug allergies.

For the sake of efficiency and patient safety, every practice should have a records management policy in place, and this should be regularly reviewed and updated to keep pace with technological advances and legislative requirements.

THIS MUST BE A CONDITION OF REGISTRTION OF ANY HEALTH INSTITUTION TO HAVE A RECORD MANAGEMENT POLICY

10. Retention of medical records

- Doctors should keep records for 10 years from the date of last entry.
- All medical records at an institution should be kept indefinitely. However, an institution can keep records for a minimum of 10 years from the date of last entry and thereafter they should be sent to the National Archives.
- Doctors who cease to practice medicine must transfer the records to another person taking over the practice.

11. Disposal of records

Clinical records may be transferred to the National Archives rather than be destroyed, if they are of archival value.

If records are to be destroyed, paper records should be shredded or incinerated. CDs, DVDs, hard disks and other forms of electronic storage should be overwritten with

random data or physically destroyed. Be wary of selling or donating second- hand computers – "deleted" information can often still be recovered from a computer's hard drive.

If you use an outside contractor to dispose of patient-identifiable information, it is crucial that you have a confidentiality agreement in place and that the contractor provides you with certification that the files have been destroyed.

You should keep a register of all healthcare records that have been destroyed or otherwise disposed of. The register should include the reference number (if any), the patient's name, address and date of birth, the start and end dates of the record's contents, the date of disposal and the name and signature of the person carrying out or arranging for the disposal.

12. Transferring records

If a patient transfers to another doctor, you should forward a copy of the patient's records to the new doctor, while retaining the original for your own records. These should be disposed of at the end of the retention period in your records management policy.

13. Research

If you are conducting your own research or audit based on your patients' medical records, it is acceptable to do so without the patient's consent, although as a matter of courtesy you should inform the patients concerned if it is feasible.

For studies involving outside researchers, any patient information you provide should be anonymised. If it is necessary to include information that could be used to identify individual patients, you must first secure the patient's express consent.

Box 8: Educational research

"Education and training of health professionals is essential to the provision of safe and effective healthcare. When patient information is to be used for education and training purposes, you should anonymise it as far as possible.

Where anonymisation is not possible or appropriate, you should make patients aware that their identifiable information may be disclosed for such purposes. They should have the opportunity to object to disclosure of their information and any such objection must be respected."

14. Summary

i. Records that secure continuity of care will also be adequate for evidential purposes, in the event of a complaint, claim or disciplinary action.

ii. Clinical records should be clear, objective, contemporaneous, tamper-proof and original.
iii. Abbreviations, if used, must be unambiguous and universally understood.
iv. Clinical records comprise handwritten and computerised notes, correspondence between health professionals, laboratory reports, x-ray and other imaging records, clinical photographs, videos and other recordings, and printouts from monitoring equipment.
v. Clinical records are sensitive personal data and must be kept securely to prevent damage and unauthorised access.
vi. Clinical records can usually be shared with other members of the clinical teams responsible for clinical management, unless the patient objects.
vii. Access to records or the information they contain is also permissible in other circumstances but the record holder must always be prepared to justify disclosure.
viii. All healthcare organisations holding clinical records must be registered with the Health Professions Authority.
ix. Where information from clinical records is required for audit and research purposes, anonymised data should be used wherever possible.
x. Any alteration to written medical records should be immediately apparent to avoid any accusation that there has been an attempt to mislead or deceive.
xi. Similarly, with electronic records, any entries should be made clear to identify any changes.
xii. Common problems are illegibility of handwritten notes, failing to date and sign them, inaccurate recording of information and insufficient detail.

15. Appendix 1: Environmental risks to note

Although most of us think of security in terms of safeguarding against unauthorised access, there is another important aspect – protecting records from physical damage. Paper records in particular can be easily damaged by moisture, water, fire and insects. And – unlike electronic records – it's not feasible to create up-to-date copies against the chance destruction of the originals. Your paper records are therefore not only vulnerable, but irreplaceable, so it's a good idea to carry out a risk assessment to identify ways in which you can reasonably safeguard their physical integrity. Below are some of the factors that should be considered in a risk assessment.

15.1 Fire

Install chemical fire extinguishers (do not use a sprinkler system as water can be even more damaging than fire). Smoke from fires elsewhere in the building can also do much damage, so make sure that doors are tight fitting and kept closed. Inflammable liquids kept on the premises should be properly stored, and as far away as possible from the records. Install smoke and fire alarms, preferably a system that connects directly to the local fire service.
Important paper documents should be kept in a fire-proof safe, but do not entrust your computer back-up drive to a fire-proof safe – it can melt. Instead, use secure off-site storage.

15.2 Water

Basements are not a good place for archiving records – it is better to use professional offsite archiving services if you don't have a suitable space for storing inactive files. If you are in a flood-prone area, store records above floor level. Think also about the risks from leaking roofs and plumbing problems. If you have sprinklers in areas that house computers, put waterproof covers on the computers before going home at night.

15.3 Gravity

Paper records can be very heavy, so get an engineer to check that the floor of your records room can carry the load.

15.4 Insects and vermin

Have regular inspections and control measures carried out by experts to keep damaging insects and rodents at bay.

15.5 Poor building maintenance

Dangerous wiring, gas leaks, plumbing problems, leaking roofs and damp walls can all cause damage to both paper and electronic records. A regular building maintenance programme can help to reduce the risk from these elements.

15.6 The risk of unauthorised access

Paper records should be kept in a room that can be securely locked when the practice is unattended. Limit the number of keys in circulation and keep a record of all key holders. If you use an electronic lock, only give the access code to staff who need it and change the code periodically.

Your records management policy and procedures should include protocols specifying the different roles of staff regarding access to records. Staff should be suitably trained so that they understand the legal and ethical principles of confidentiality and are aware of the need to keep records secure from unauthorised access.

Suitable safeguards for electronic records include firewalls, antivirus software, strong passwords, careful positioning of monitors so that information cannot be read by unauthorised people and setting access permissions on a need-to-know basis.

16. Appendix 2:

16.1 Legal considerations

It is up to everybody working in an organisation that holds records containing personal information to comply with the spirit of Section 57 of the Constitution i.e, respect the subject's privacy, keep the use of information to the minimum necessary and allow appropriate access.

Data controllers must:

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was initially given
4. Keep it safe and secure
5. Keep it accurate and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a copy of his/her personal data to any individual, on request.

Furthermore, personal information should not be transferred to a country or territory outside Zimbabwe unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (This does not apply if the patient has consented to information being sent.)

16.2 Private practice

If you are in private practice, you are required to demonstrate that you have an appropriate data protection policy in place. This applies both for records held in your private place of work and for any private practice you may have within a public hospital. A designated member of staff will need to take on the further responsibility of ensuring that the practice as a whole is complying with the Acts.

16.3 Requests for access

Patients have a right to access their own records. One must comply with the request within 30 days. Before granting access, however, it is important to check the records to ensure that they do not include identifiable information about third parties, which should be edited out of any copy you make available to the patient. This does not generally include omitting letters or opinions contributed by colleagues, such as a letter from a consultant.

Those with parental responsibility for a child can also request access to that child's records.

Requests for access to the records of a patient who is mentally incapacitated must be decided on a case-by-case basis, bearing in mind that the interests of the patient are paramount.

You are permitted to withhold access to part or all of the record if there is a real possibility that viewing it would result in serious damage to the patient's physical, mental or emotional wellbeing. This would be a rare circumstance and such a decision should be based on sound clinical judgment. Your reasons for withholding the information should be clearly documented and you should indicate to the person requesting the record where omissions have been made. The patient has the right to ask Council to investigate the matter, so it is important that your reasons for denying access are defensible.

16.4 Correction of Records

You are under no obligation to erase or amend clinical information that has been fairly collected, relevant and accurate, and is not excessive for the purpose for which it was obtained. However, this raises the issues of confidentiality and consent; patients have the right to expect healthcare professionals to respect their wishes regarding disclosure of personal information. If the patient does not want certain information to be available to the healthcare team, you should agree to restrict access to it, but explain that this could compromise the patient's care.

17. Appendix 3 : Standards for Content of the healthcare record

17.1 Standard

The content of the healthcare record shall provide an accurate chronology of events and all significant consultations, assessments, observations, decisions, interventions and outcomes. The content of each record shall comply with clinical guidance provided by professional bodies and legal guidance.
This standard shall apply to both hard copy and electronic documentation.

17.2 Rationale

The healthcare record and its content form an essential part of care allowing communication between healthcare professionals and demonstrating that the practitioner's duty of care has been fulfilled.

17.3 Correct identification

The patient's name shall be on each side of each page where patient information is documented and each page shall have the correct unique patient identification number and/or label. This shall also apply to every screen on computerised systems.
There shall be no blank spaces or pages between entries.

Before the health care professional makes an entry in the patient's healthcare record, s/he shall establish that the record belongs to the patient being attended. This shall be done by verifying with the patient and by cross-referencing the patient's wrist band with the healthcare record.

17.4 Legibility

- All documentation shall be clear and legible.
- When prescribing, writing shall be in un-joined lower case text or block capitals.
- All entries shall be dated, timed and signed with a clear signature, printed name, title and bleep number (where relevant).
- All entries shall be in permanent black/blue ink.

17.5 Documenting date and time

- It shall always be clear from the patient record the time that an event occurred and the time that a record was made.

- The time (24-hour clock) and date (day/month/year) shall be noted against each clinical entry.
- All entries shall be accurate in relation to date (day/month/year) and time.

17.6 Author identification

- Each hospital site shall have an up-to-date signature bank of all clinical staff and non-clinical staff that may have occasion to write in the healthcare record.
- Identification stamp pens, which have the clinician's name printed on a stamp attached to the pen, shall be permissible.
- All signatures shall be accompanied by a printed name.

- Records shall provide information on physical, psychological and social factors that may affect the patient.

- The chronology of events and reasons for any decision made shall be recorded in the context of a thorough assessment of the patient including relevant history taking.
- Records shall provide accurate, correct, comprehensive and concise information concerning the condition and care of the patient or client and associated observations.

17.7 Information shall be factual

All entries in the record by healthcare professionals shall be made as soon as possible after each intervention and at least once every 24 hours during the working week for acute inpatient episodes. There shall be an entry in the record at least twice a week for rehabilitative care.
Every record entry (clinician related) shall identify the most senior clinician present at the time the entry was made.

The name of the primary clinician who is assuming overall responsibility for the patient's care shall be clearly identifiable in the healthcare record at all times. The name in the patient's record shall be the same clinician's name entered into the Patient Administration System (PAS). Should the primary clinician change during the course of treatment, this shall be noted on the healthcare record and on the PAS.
Input into all records shall be multidisciplinary.

17.8 Retrospective entries

Retrospective documentation shall be:

i. Dated.
ii. Timed.
iii. Signed (and counter-signed as appropriate).

The reason why the retrospective entry is being made shall be clearly stated.
It shall be clear that the entry is a retrospective entry.

17.9 Relevancy

Records shall be objective and shall describe what is observed.
If an incident has not been observed but is relevant to client care then this shall be clear, eg, patient states that..."

17.10 Verbal instructions

Instructions regarding patient care from a healthcare professional via the telephone shall be documented, dated, signed and counter-signed by the healthcare professional responsible for giving the instructions.
If no instructions were given, this shall also be documented.

17.11 Abnormal results

There shall be a note in the clinical record of any significant abnormal results found or communicated to the healthcare professional. This shall include a record of who has been informed, eg, healthcare professional's name. This note shall be made by the appropriate healthcare professional.

17.12 Medications

- Drugs shall only be administered and documented in the presence of clear unambiguous prescriptions and in accordance with hospital policies.
- Drug names shall never be abbreviated under any circumstances.
- Generic names ONLY shall be used for the drug chart.
- The choice of therapeutic agents used shall remain the responsibility of the clinician.

17.13 Language

- Records shall be written in English.
- Records shall be completed in terms that the patient and/or the healthcare professional can understand.
- Records shall be supported by explanations where this may not be possible.
- Records shall be phrased clearly and unambiguously.

17.14 Advice

Healthcare professionals advice on care, in any format (eg, verbal, leaflet), shall be documented in notes of advice given.

17.15 Patient alerts and allergies

Alerts and allergies shall be recorded on the inside of the cover of the healthcare record chart.
The information shall be signed and dated and there is an end date for the alert, if appropriate.

The hospital shall have a clear procedure regarding who should enter alerts into the healthcare record, when alerts should be entered and the procedure for removing alerts from the healthcare record. These procedures shall be adhered to.

17.16 Admission entry

The following minimum, general patient information shall be included in the record entry for acute medical admissions and may also be supplemented with additional specialty information:

i. Reason for clinical encounter.
ii. Presenting problem/complaint.
iii. History of presenting problem.
iv. Current diagnoses.
v. Patient Alerts/Allergies (this should also be recorded on the inside of the front cover).
vi. Past illnesses.
vii. Procedures and investigations.
viii. Medications and diets including nutritional supplements.
ix. Social circumstances.
x. Functional state (Self-care/baseline mobility/walking aids and appliances).
xi. Family history.
xii. Systems review.
xiii. Examination findings.
xiv. Results of investigations.
xv. Problem list.
xvi. Overall assessment.
xvii. Management plan.
xviii. Intended outcomes.
xix. Information given to patient

17.17 Follow-up entry

The following patient information shall be included in the follow-up entries for acute medical admissions:

i. Reason for clinical encounter.
ii. Review of case.
iii. Overall assessment including any change since previous encounter.
iv. Management care plan.
v. Information given to patient and carers.

18. Documenting consent in the healthcare record

Consent shall:

i. Be easily and clearly identifiable either on a consent form, which is retained as part of the clinical record, or in the case of verbal consent, documented within the clinical record.
ii. Contain no abbreviations.

iii. Clearly state the procedure/treatment/care involved and the risks and benefits of that procedure.
iv. Clearly identify the patient by name and healthcare record number.
v. Clearly identify who has granted or refused consent and/or their relationship to the patient in the case of parent/guardian.
vi. Have a documented record of what appropriate patient/client information or relevant discussions have been provided to the patient/guardian detailing the procedure/treatment/care, risks, benefits and/or alternative.
vii. Have a documented record of how this information has been provided (eg, patient/client information leaflets, verbally, etc).
viii. Be dated and signed by the healthcare professional obtaining the consent, including full name and grade.

Verbal consent shall be documented in the clinical record and shall clearly identify the witness, eg, by name and grade.

This standard shall apply to both hard copy and electronic documentation.

Sources: Ireland Medical Council Medical Records Guidelines.
Constitution of Zimbabwe Amendment(No.20)Act 2012

MEDICAL AND DENTAL PRACTITIONERS COUNCIL
REGISTRAR
2023 -01- 19
8 Harvey Brown Ave, Milton Park, Hre
P.O. Box CY818, Causeway
Telephone: 0242 792195

19/1/2023