The evolving electronic dental record: Revisiting clinical-, digital-, medico-legal integrity, and information governance considerations

Johan Hartshorne[1]

Keywords: electronic dental record, clinical integrity, digital integrity, medico-legal integrity, information governance, record keeping, regulatory framework

Executive summary

Clinical significance/ Importance:

- Electronic health records (EHRs) are integral to oral healthcare, with increasing emphasis on interoperability and integration between dental and medical information.
- The quality of a dental record has implications extending beyond clinical continuity. It influences patient safety, informed decision-making, interdisciplinary communication, quality assurance, data protection, professional accountability and medico-legal defensibility.
- The purpose of this review is to revisit the impact of technology, innovation, and regulatory frameworks on evolving electronic dental records (EDR's) from a clinical-, digital-, medico-legal integrity, and information governance perspective.

Key findings

- EDR's should satisfy six characteristics: accurate, contemporaneous, comprehensive, traceable, secure and clinically meaningful.
- Digitalisation creates substantial opportunities but also introduces risks involving cybersecurity, unauthorised access, data integrity, interoperability, automated documentation and AI-generated content.
- Digital images or files should not exist as disconnected "islands" outside the patient's clinical EDR.
- AI-generated information should never be accepted automatically without appropriate professional review and practitioner verification.
- The responsible practitioner must verify clinically material AI-generated information before it becomes part of the clinical record or informs patient care.
- The depth of documentation recorded in EDR's should be proportionate to: the clinical complexity of the case/treatment.
- Cybersecurity should be seen as continuous information governance, rather than a one-time IT installation.
- The privacy principle should be: collect what is clinically justified, use it for a defined legitimate purpose, protect it throughout its lifecycle and disclose only what is

[1] Johan Hartshorne

B.Sc., B.Ch.D., M.Ch.D., M.P.A., Ph.D. (Stell), FFPH.RCP (UK)

General Dental Practitioner

Intercare Medical and Dental Centre, Tyger Valley, Bellville, South Africa, 7530

Email: johan.laptop@intercare.co.za

appropriately authorised or legally required.
- A signed consent document is important evidence, but not synonymous with informed consent.

Practice implications

- Dental practitioners should regard the patient record as a clinical and ethical stewardship responsibility, rather than as administrative paperwork.
- A contemporaneous EDR should be structured around the patient's clinical journey, supported by reliable digital infrastructure and maintained according to applicable professional, privacy and medico-legal requirements.
- An EDR is not a static form – it is dynamic and should be updated and backed-up on a regular basis.

Background

The new era of electronic health record's (EHR's) and the development and integration of digital imaging, digital workflows, artificial intelligence (AI), practice management technologies (i.e., block chain technology) and software, have revolutionized information management and patient care in health care, including dentistry.[1] Contemporary dentistry increasingly generates complex longitudinal datasets comprising clinical findings, artificial intelligence (AI)-assisted diagnostic and treatment outputs, treatment planning digital images, CAD/CAM workflows, digital laboratory prescriptions, patient and interprofessional communications. The implementation of these technologies in dental practice have facilitated comprehensive documentation, improved clinical efficiency, and enhanced patient safety through better recordkeeping and clinical decision support.[2] Despite its advantages, electronic dental records (EDR's) and advanced technology adoption in dentistry has introduced new challenges and concerns affecting clinical, digital, medico-legal integrity, and information governance in the dental practice setting.[3,4] In addition, despite the widespread adoption of digital and AI technologies, the quality and completeness, and interoperability of personal dental data still lag behind medical systems.[5]

An EHR is a longitudinal clinical, personal and professional record of a patient. Its fundamental purpose remains unchanged: to document the patient's health status, clinical assessment, diagnostic reasoning, treatment, communication/response, consent, outcomes and ongoing care, irrespective of the medium in which the information is recorded.[6] The HPCSA requires EHR's to be aligned with the following ethical integrity principles:[6]

- Contemporaneous (current, modern);
- Accurate, complete and comprehensive (correct, factual, precise);
- Clear, legible, and unambiguous (understandable);
- Attributable (patient, provider responsible, traceable, auditable);
- Accessible (available, retrievable, obtainable);
- Securely stored (protected from unauthorised access, loss or alteration);

While remaining clinically meaningful.

The primary purposes of a dental record is: to remind the practitioner what was found, decided, and done; to promote continuity of care; and to provide evidence of the standard of care the patient has received. It also recognises clinical audit, teaching, research, administration and litigation as secondary uses.[6] The FDI World Dental Federation 2025 Consensus statement on Integrated Electronic Health Records recognises EHRs as increasingly important for clinical care, communication, research, public health and data-driven healthcare. It also identifies the integration of oral and medical health information as an important component of person-centred care.[7] Integrated electronic health records offer clinical benefits by allowing dentists to access a richer patient history, such as lab results and medication records, to inform safer and more effective treatment planning.[8] However, interoperability challenges due to lack of linkage between EDR systems and electronic medical record systems often results in incomplete or inaccurate medical histories in EDRs, which are typically patient-reported.[9]

The HPCSA's 'Ethical Guidelines on the Keeping of Patient Records remains the central professional standard and forms part of the standards against which professional conduct is evaluated.[6] What has changed with keeping of patient records is the complexity, volume and potential significance of the information being generated. The central question that this review addresses is therefore no longer simply: "Have I kept adequate notes?" but: "Does my record accurately reconstruct the patient's clinical journey, support safe future care, demonstrate ethically sound decision-making and remain trustworthy and secure if independently scrutinised?"

Contemporaneous integrated EDR's can be conceptualised around four interconnected domains: clinical integrity, digital integrity, information governance and medico-legal integrity. (Figure 1) These domains should not operate independently, but rather complementary. Clinical integrity generates defensible documentation; digital integrity protects the evidence; information governance provides management and regulatory guidance; medico-legal integrity ensures that



Figure 1: The interconnected domains of a contemporaneous integrated EDR

the record remains credible when decisions are challenged. Thus, the central principle becomes: A contemporaneous EDR must be clinically useful, ethically trustworthy, digitally secure and legally defensible – without compromising the patients' rights to privacy, participation in decision-making and access to information.

Purpose

The purpose of this review is to revisit the impact of technology, innovation, and regulatory frameworks on evolving electronic dental records (EDR's) from a clinical, digital, medico-legal, and information governance perspective.

Clinical integrity

EDR's must accurately communicate the patient's clinical condition and the practitioner's assessment, diagnosis, risks, clinical reasoning and treatment rationale, intervention/ treatment, outcome, and continuity.[6]

Patient identification and baseline information

EDR's should contain reliable patient identifiers and sufficient demographic, contact and emergency information to ensure accurate identification.

The medical and dental history should be updated when clinically relevant rather than treated as a static form. Changes in medication, systemic disease, allergies, pregnancy status, anticoagulant therapy, immunosuppression and other risk factors that may materially alter treatment decisions should be updated in the patients' medical status.

Comprehensive clinical assessment

The record should allow another appropriately qualified practitioner to reconstruct the clinical assessment. Where relevant, this includes:

- presenting complaint and patient's expectations;
- relevant history;
- clinical examination and diagnostic findings;
- periodontal and dental status;
- relevant extraoral and intraoral findings;
- radiographic and other imaging findings;
- photographs and digital scans;
- differential diagnosis;
- risk assessment; and
- diagnosis and prognosis.

Importantly, normal or negative findings should be documented where they influence clinical reasoning.

Clinical reasoning and treatment planning

One of the most important requirements of an EDR is documentation of clinical reasoning. Clinical reasoning should be documented contemporaneously where it materially informs diagnosis, treatment selection, risk assessment, consent or follow-up.[5] It should not be retrospectively reconstructed merely to justify a decision after an adverse event or complaint.

The EDR should answer:

- What was found?
- What does it mean clinically?

- What treatment options were considered?
- What are the expected benefits, limitations and risks?
- What alternatives, including no treatment, were discussed?
- Why was the selected approach appropriate?
- What monitoring or review is required?

This is particularly important in implant dentistry, periodontics, orthodontics, aesthetic dentistry, complex restorative treatment, and complex maxillo-facial and oral reconstructive surgical procedures where treatment may be elective, staged or dependent upon patient-specific risk factors.

Proportional documentation

The depth of documentation recorded in EDR's should be proportionate to: the clinical complexity of the case/ treatment; treatment risk, irreversibility, patient vulnerability, uncertainty of outcomes or complications, and its medico-legal significance.[10] In addition, documentation should sufficiently preserve clinical meaning, continuity and accountability. Thus, longitudinal contemporaneous clinical records, including radiographs and notes, are essential for demonstrating the clinical decision-making process, which supports the premise that documentation depth should reflect complexity and risk.[10]

Communication of essential patient information

EDR's form an essential part of communicating clinically significant patient information to:

- patients and caregivers;
- medical practitioners;
- specialists;
- laboratories (pathology and dental);
- other dental practitioners;
- insurers or funders where relevant; and
- multidisciplinary teams.

Telephone conversations, electronic messages and telehealth interactions may become clinically significant evidence and should be incorporated when they influence diagnosis, treatment, consent, advice or follow-up.[11,12] The record should document what was communicated, to whom, when, by whom and what action resulted.

Use of ambient AI scribes for documentation of communication's between patient and provider

It is reported that capturing complete, accurate, and consistent patient records may be burden on dental practitioners, suggesting that this may act as a barrier to the quality of patient interactions.[9] In addition, poorly designed EHR interfaces cause significant workflow disruptions, leading to challenges such as task-switching, excessive navigation, and fragmented information, which directly relates to the burden of documentation.[13] Workflow disruptions often necessitate workarounds like duplicating documentation and using external tools, which increases the risk of data entry errors and prolongs documentation times, directly impacting clinical integrity. It is suggested that AI scribes using ambient voice technology (AVT) transforms spontaneous conversations between the clinician and patient into structured documentation, which is assembled into structured notes aligned with standard Subjective, Objective, Assessment, and Plan or procedure-note formats, thereby enhancing documentation quality.[5]

Thus, AI scribes may enhance the completeness, accuracy, and consistency of patient records while simultaneously reducing the time practitioners spend on clinical documentation.[9] However, it is noted that this effect is inconsistent, and curiously, some implementation studies showed an increase in note length despite a decrease in the proportion of text typed by clinicians.[14] It is also emphasized that clinicians retain full responsibility for the final EDR produced by AI systems, underscoring the necessity of reviewing and editing draft notes.[14] Clinical integrity concerns related to the potential for clinically significant errors, inaccuracies, omissions, and hallucinations observed in AI-generated documentation, especially with dental terminology, therefore necessitates moving evaluation beyond surface measures toward assessing clinical significance.[14]

The scarcity of complete and consistent documentation, particularly concerning social determinants of health in EDRs, leads to poorly performing AI tools, emphasizing the need for robust documentation for effective clinical integrity and policy use.[9] More standardized documentation of consent, procedures, and postoperative instructions achieved through ambient AI scribes may reduce variation and improve medicolegal defensibility at the practice level, supporting clinical integrity.[5] Ambient AI scribes provides an enhanced patient-centered care approach that support clinical integrity by allowing clinicians to focus more fully on patients and engage in more meaningful discussions about diagnosis, risk, and treatment options, aligning with patient-centered care principles.[5]

"The Medico-Legal Test"

Before closing a significant clinical episode, ask seven critical questions:

1. What did I know?
2. What did I find?
3. What did I conclude?
4. What options did I consider?
5. What did I explain to the patient?
6. What did the patient decide?
7. What did I do and what follow-up did I arrange?

If the EDR answers these questions contemporaneously,

it becomes considerably more useful both clinically and medico-legally.

Digital integrity

EDR's should not simply reproduce poor paper documentation in digital form. EDR's must preserve the authenticity, privacy, accessibility, availability, traceability, back-up, cybersecurity, interoperability, data integrity and AI governance of patient-related digital images or documents throughout its lifecycle. A contemporaneous integrated EDR should provide the following to preserve digital integrity:

- individual user authentication;
- role-based access;
- audit trails;
- secure backups;
- encryption where appropriate;
- controlled data export and transfer;
- protection against unauthorised alteration;
- reliable image and document storage;
- documented downtime procedures;
- disaster recovery;
- interoperability where clinically appropriate.

The HPCSA[6] and General Dental Council (UK)[15] similarly emphasises that records should remain complete, accurate, secure and accessible, tracible, with electronic information appropriately protected and backed up.

Cybersecurity should therefore be regarded as a clinical safety issue, not merely an IT responsibility. Healthcare systems are increasingly exposed to cyberattack, and South African healthcare has experienced significant ransomware-related disruption.[16]

Centralized EDR's versus Blockchain enabled EDR's

Centralized EDRs systems face critical vulnerabilities, such as data breaches and single points of failure, which compromise patient privacy and regulatory compliance.[17] The introduction of blockchain technology is being explored as a secure alternative to centralized EDR's to improve data security, transparency, and interoperability in the administration of dental records.[17] Blockchain enabled EDR systems could help ensure trust among dental professionals by providing an immutable history of patient care, insurance reimbursements, and diagnostic data, thereby maintaining data integrity.[17]

Digital images and EDR sharing

Digital images includes extra- and intraoral photographs, radiographs, CBCT, facial photographs, digital impressions (intra-oral scanning), CAD/CAM digital workflow files, and laboratory communications. Digital images are clinical records and should be integrated and managed accordingly within EDR's.[18]

The EDR should establish, where relevant:

- date and purpose of image acquisition;
- patient-identification;
- anatomical site;
- clinical indication;
- interpretation or significance;
- relationship to diagnosis and treatment; and
- storage location and traceability.

Digital files or images should not exist as disconnected "islands" outside the patient's clinical EDR. In addition, sharing digital images demands robust safeguards for patient privacy.[19]

Artificial Intelligence (AI) generated information

CentrThe introduction of AI technology into the dental practice setting has raised new documentation challenges.[20] The HPCSA's Booklet[20] provides an important and timely foundation for guiding the ethical use of AI in SA healthcare.[21]

Where AI contributes to diagnosis, image interpretation, risk assessment, treatment planning, clinical documentation or patient communication, the practitioner remains responsible for the clinical decision. AI-generated content should be treated as an assistive (augmentive) output rather than an authoritative clinical record.[22] The responsible practitioner must verify clinically material AI-generated information before it becomes part of the clinical record or informs patient care. The record should remain attributable to the practitioner responsible for the clinical decision. AI-generated information should never be accepted automatically without appropriate professional review and practitioner verification of the clinical interpretation and final clinical decision.[22] Recent literature in dentistry highlights privacy, data security, bias, transparency, accountability and human oversight as central requirements for responsible clinical AI.[22,23,24] Furthermore, patient information should not be entered into external AI systems unless the processing is lawful, appropriately governed and consistent with applicable confidentiality and data-protection requirements.

Information governance

EHR records must be aligned according to HPCSA,[6] POPIA[25] and PAIA[26] ethical and regulatory frameworks to preserve confidentiality, access request, information officer, operators/vendors obligations, breach responses, and retention/destruction protocols. HPCSA professional record-keeping obligation; POPIA privacy/data-processing obligations; and; PAIA access-to-records obligations are complementary protocols, not interchangeable ones. This moves patient data management from traditional 'record

keeping' to genuine 'information governance'.

The HPCSAs' PAIA and POPIA manual[27] was prepared in accordance with section 14 of the Promotion of Access to Information Act, 2000 ("PAIA") and to address the requirements of the Protection of Personal Information Act, 2013 "POPIA").[6, 27] The Promotion of Access to Information Act (PAIA) No. 2 of 2000 is South Africa's freedom of information law that gives effect to Section 32 of the Constitution, granting everyone the right of access to records held by the State or by private bodies.[26] The Protection of Personal Information Act (POPIA) is South Africa's data protection law (Act No. 4 of 2013) that safeguards the right to privacy by regulating how public and private bodies collect, use, store, and share personal information.[25] A checklist for POPIA compliance[28] is summarized in **Table 1**. The risks of non-compliance are stark, resulting in potential fines and reputational damage. On the other hand, robust compliance can result in reduced patient attributes, enhanced referrals, operational efficiency, and defensive marketing.[28]

In South Africa, health information constitutes special personal information under the Protection of Personal Information Act[25], requiring appropriate safeguards and lawful processing.

A modern practice should therefore establish:

- a defined information-governance policy;
- access controls;
- staff confidentiality obligations;
- secure communication procedures;
- appropriate retention and disposal policies;
- breach-response procedures;
- documented responsibilities for information governance;
- appropriate safeguards when information is transferred to external providers or cloud services.

POPIA defines processing broadly, encompassing collection, recording, storage, updating, dissemination, linking, erasure and destruction. The privacy principle should be: collect what is clinically justified, use it for a defined legitimate purpose, protect it throughout its lifecycle and disclose only what is appropriately authorised or legally required.

Privacy and confidentiality

Dental records contain highly sensitive health information. Robust data security measures are necessary to protect patient privacy and confidentiality within EDR's which is a key component of clinical- and digital integrity.[11] It is suggested that ethical considerations regarding digital equity, data privacy, and the risk of depersonalization require deeper analysis to balance innovation with patient safety and clinical integrity.[11] Practitioners must adopt strategies that align with clinical needs and regulatory standards, indicating that compliance with privacy and security regulations is critical for implementing modern communication tools, including electronic health records.[11]

Cybersecurity – Security measures on integrity and confidentiality of personal information

Common, systemic cybersecurity vulnerabilities found during a security assessment of a South African dental practice, include the use of default vendor passwords, unsegmented networks, outdated software, and shared staff credentials.[29] Encryption, access controls, backups and cybersecurity measures are essential elements of digital integrity.[29] However, POPIA section 19 goes further- South African dental practices carry a legal obligation under the Protection of Personal Information Act (POPIA) to implement appropriate, reasonable technical and organisational measures to protect personal information against loss, damage, unauthorised destruction, unlawful access or processing.[25] It must identify reasonably foreseeable risks, establish safeguards, regularly verify them and update them as risks evolve. This means cybersecurity should be presented as continuous information governance, rather than a one-time IT installation. It is emphasized that there is a critical need for comprehensive security measures, such as network segmentation, patch management, and multi-factor authentication, to prevent catastrophic ransomware attacks and ensure digital integrity of patient records.[29]

Cloud-based platforms and external software providers

This is particularly important for modern dental practices. Cloud-based EHRs, digital imaging platforms, practice-management systems, online booking systems, laboratory portals and AI-platforms may process patient information on behalf of the practice.

POPIA sections 20–21 impose obligations concerning operators processing information on behalf of a responsible party, including contractual security requirements and notification of suspected unauthorised access.[25]

Where external software providers, cloud-based platforms for EDR's, laboratories, digital imaging platforms or AI systems process patient information on behalf of the practice, appropriate contractual, security, confidentiality and data-governance arrangements should be established. Vendor selection should therefore be regarded as a clinical information-governance decision rather than solely a

procurement decision. The minimum standard requirements for digital information governance when using cloud-based, or external digital imaging platforms should include (**Table 1 & 2):**

- access control;
- unique user identification;
- strong authentication;
- role-based permissions;
- audit trails;
- secure backups;
- encryption appropriate to the risk;
- software and security updates;
- staff cybersecurity training;
- operator/vendor agreements;
- documented breach-response procedures;
- periodic security-risk assessment;
- tested disaster-recovery procedures.

Lawful processing health information – Is consent required

Health information is special personal information. Patient consent is not the sole legal basis for processing health information. Section 26 and section 27 of the POPIA Act provides circumstances in which a patients' information may lawfully be processed. Although patient consent remains fundamental to many clinical and ethical processes, lawful processing of personal and health information under POPIA depends on the applicable statutory processing condition and purpose.

This distinction is an important medico-legal principle. Thus, for healthcare professionals, processing of patients' health information may be permissible where necessary for appropriate treatment and care and within the statutory framework.

Data breaches — the POPIA notification requirement

All dental practice's should maintain a documented security-compromise response protocol addressing identification, containment, investigation, notification and remediation. POPIA section 22 requires notification to the Information Regulator and, subject to the statutory conditions, the affected data subject where there are reasonable grounds to believe personal information has been accessed or acquired by an unauthorised person.[25] Notification must occur as soon as reasonably possible after discovery, taking account of legitimate investigative needs. This information governance rule is highly relevant to an evolving EHR.

Record Retention, Access and Transfer

Retention requirements vary according to jurisdiction, professional rules, patient age, type of record and other applicable legislation. Practices should therefore maintain a written retention schedule rather than relying on informal custom.

In South Africa, practitioners should align their policy with applicable HPCSA requirements, POPIA (Section 14) and other relevant legislation and professional guidance.[25] The HPCSA specifically identifies record keeping as both an ethical and legal responsibility.[6] Patients should have appropriate mechanisms to access their information, and transfer to another practitioner should be undertaken securely and with appropriate authorisation.

The HPCSA recommends that patient health records ideally be retained indefinitely, particularly where electronic retention is practicable.[6] Where indefinite retention is not practical, the guideline specifies a minimum period of six years from the date the record becomes dormant, subject to longer periods applicable to specific categories of patients or records and to any statutory retention requirement. Practices should therefore maintain a documented retention schedule and apply the longest applicable mandatory period where different legal or professional requirements overlap.

Important medico-legal addition pertaining to record retention.

For a record relating to:

- an unresolved complaint;
- pending litigation;
- threatened litigation;
- regulatory investigation;
- serious adverse event; or an
- unresolved professional indemnity matter,

routine destruction should be suspended. This should be explicitly included in the practice policy.

Patient-rights to access records

HPCSA[6] explicitly recognises patient access to health records, while POPIA section 23 gives a data subject a right to request access to personal information held by the responsible party, subject to applicable grounds of refusal.[25] PAIA is also relevant, particularly to access to records held by private bodies where the statutory requirements apply. Section 50 provides a right of access to records of private bodies where the record is required for the exercise or protection of rights, subject to PAIA's requirements and grounds of refusal.

Patients have rights of access to information concerning themselves. In South Africa, access to patient information must be managed within the framework of the HPCSA ethical requirements, POPIA and, where applicable, PAIA. Practices should have a documented procedure for verifying identity and authority, receiving, processing and responding to

requests for access, while protecting third-party information and applying any lawful grounds for refusal.

Requests for access to records

For a dental practice operating as a private body, PAIA may also impose organisational information-governance obligations, including an appropriate PAIA manual and processes for requests, subject to the applicable statutory framework and exemptions. Therefore, dental practices operating as private bodies should ensure that their information-governance arrangements address applicable PAIA obligations, including appropriate procedures and documentation for requests for access to records and the maintenance of the required PAIA documentation.[26]

The Information Officer should be added

This is an important contemporaneous information governance component.

The Information Regulator's guidance confirms registration of Information Officers and provides for Deputy Information Officers where appropriate.

Thus the practice should identify its Information Officer and, where appropriate, Deputy Information Officer(s), with clearly defined responsibility for POPIA and PAIA compliance, information governance and regulatory engagement.

Medico-legal integrity

EDR's and documentation are essential tools in clinical dentistry, providing a comprehensive account of a patient's oral health status, treatment history, and diagnostic findings for informed treatment decisions and continuity of care.

The medico-legal significance thereof is that accurate documentation of informed consent, which includes clear information about treatments, potential risks, benefits, alternatives, and expected outcomes, protects both the patient's autonomy and the dentist's professional responsibility, especially in complex or surgical interventions where failure to obtain proper consent may result in legal claims.

Contemporaneous documentation

Clinical reasoning is an important medico-legal component of a health record. The record must provide contemporaneous evidence of professional decision-making (clinical reasoning) related to alternative treatment options, risk assessment, informed consent, communication, treatment and follow-up. (**Table 2**) In addition, documentation on records should be traceable, while corrections should be transparent. Clinical reasoning should be documented contemporaneously where it materially informs diagnosis, treatment selection, consent, risk assessment or follow-up. It should not be retrospectively reconstructed or altered merely to justify a decision after an adverse event or complaint.[6]

Table 1: POPIA compliance checkbox

Appoint Information Officer

Conduct mapping audit:

- ☐ What patient data is collected?
- ☐ Where is the data stored?
- ☐ Who has access to the data?
- ☐ What is the lawful purpose of having the data?

Core information governance documentation:

- ☐ Privacy policy
- ☐ PAIA and POPIA manual
- ☐ Subject access request protocol
- ☐ Data breach protocol

Review and secure 3rd party contracts:

- ☐ IT providers
- ☐ Cloud-based hosts
- ☐ Laboratories
- ☐ Accounting software

Technical and physical safeguards:

- ☐ Access control for practice administration software
- ☐ Encryption of data
- ☐ hysical security

Patient communications, use of patient information & consent :

- ☐ Treatment data
- ☐ Recall reminders via SMS /WhatsApp
- ☐ Use of photos and other digital images

Staff and training (annually):

- ☐ Identifying phishing email
- ☐ Secure data handling
- ☐ Understanding patient rights and data requests

AI generated information

The HPCSA requires health records to be attributable.6 The medico-legal implication thereof is strait forward: AI may generate information, however the practitioner generates the clinical record and is responsible for verification and clinical reasoning.

Informed Consent as a Process, Not a Form

A signed consent document is important evidence, but it should not be regarded as synonymous with informed consent. The record should demonstrate the consent process, including the nature and purpose of the proposed intervention, material risks, reasonable alternatives, expected limitations, the patient's questions and preferences and costs. For complex or elective treatment, documentation should also establish that expectations were discussed realistically.

The medico-legal value of documentation lies not simply in proving that a form was signed, but in demonstrating that meaningful communication and patient participation occurred.[6] Patients should receive information in a manner they can understand, and patients should have access to their medical records.

Informed consent should be documented as an ongoing communication process rather than reduced to the presence of a signed form. The record should demonstrate, where relevant, the information provided, material risks, reasonable alternatives, costs, patient questions, preferences and the decision reached.

That is particularly important for:

- implant dentistry;
- orthodontics;
- aesthetic dentistry;
- elective rehabilitation;
- periodontal surgery; and
- complex multidisciplinary care.

HPCSA Ethical Rule 27A also requires practitioners to provide adequate information about diagnosis, treatment options, alternatives, associated costs and other pertinent information to facilitate informed decision-making.[30]

Treatment Documentation: The "5 Rs" (Medico-Legal test)

Every significant treatment entry should ideally demonstrate five elements:

Record: What was actually done?

Reason: Why was it done?

Risk: What clinically relevant risk factors or complications were present?

Response: How did the patient respond?

Review: What follow-up, monitoring or further treatment was planned?

Entries should be contemporaneous, attributable to the person making them, dated and timed where appropriate, and sufficiently clear that another practitioner can understand the clinical sequence. South African Dental Association guidance similarly emphasises the importance of records being contemporaneous, clear and complete, including clinical findings, decisions, communication and actions.[31]

Corrections, Amendments and Late Entries

A critical medico-legal principle is that the original clinical record should remain traceable.[6] Corrections and amendments must preserve the original information and its auditability. Electronic systems should retain an audit trail identifying the author, date, time and nature of the amendment. Late entries must be identified as late entries and should include the reason for the delay. Original clinical information should never be deleted or overwritten merely to improve the appearance of the record. This is an important medico-legal safeguard.

Errors should be corrected transparently rather than deleted or concealed. Electronic systems should preserve audit trails showing who made a change and when. Late entries should be clearly identified as such and should not be backdated. If a complaint, adverse event, regulatory inquiry or litigation arises, the record should never be retrospectively altered to improve its appearance. Contemporary guidance emphasises that late amendments should retain their date and time and that records should not be altered in response to a malpractice claim or complaint.

Minimum practice standards for contemporary EDR's

Professional responsibility and medico-legal defensibility in dentistry are evaluated on a process-based standard, which includes the documentation of risk stratification, adherence to updated guidelines, and appropriate clinical reasoning, rather than on outcome-based judgments.[32]

Every dental practice should be able to answer "yes" to the questions in **Table 2.**

Conclusion

Contemporaneous EDR's represents a fundamental shift from record keeping/documentation to information stewardship. EDR's should be viewed as a trusted longitudinal representation of the patient–practitioner relationship: clinically useful, ethically trustworthy, digitally secure, ethically governed, and legally defensible—without compromising the patient's rights to privacy, participation and access to information. Its purpose is not primarily to protect the practitioner from litigation. Its first purpose is to support safe, continuous and patient-centred care. Its medico-legal value follows from the quality of that clinical and information

Domain	Contemporary question
Identity	Is the correct patient unambiguously identified?
History	Is the relevant medical/dental history current?
Examination	Are significant positive and negative findings documented?
Risk assessment	Are materially significant risks documented and stratified?
Diagnosis	Is the diagnosis and clinical reasoning evident?
Planning	Are options, alternatives and risks recorded?
Consent	Is meaningful informed consent documented?
Treatment	Is treatment contemporaneously and accurately recorded?
Communication	Are clinically significant communications documented?
Imaging	Are images identifiable, interpretable and securely stored?
Digital integrity	Is access controlled and the audit trail preserved?
AI	Is AI use appropriately governed and professionally verified?
Privacy	Is personal information securely processed and disclosed?
Corrections	Are amendments transparent and traceable?
Continuity	Could another practitioner safely continue care?
Medico-legal integrity	Could the record objectively reconstruct the clinical journey?

stewardship process. EDR's should enable: better clinical care, informed patients, medico-legal defensibility, digital resilience, and ethical stewardship.

Practitioners should ask of every record: "If another clinician had to care for this patient tomorrow—and if the record were independently examined five years from now—would it accurately explain what I knew, what I considered, what I discussed, what I decided, what I did, and why?" If the answer is yes, the dental record is functioning not merely as documentation, but as an instrument of clinical excellence, digital responsibility and medico-legal stewardship.

Mastering POPIA compliance builds the necessary infrastructure for the next generation of digital dentistry, anticipating the exponential growth of data volume and sensitivity due to AI diagnostic tools and interconnected health records. Your commitment to appropriate data protection and information governance will ultimately contribute towards patient safety, improved clinical outcomes and patient satisfaction, reduced medico-legal risk, while providing stronger transparency and trust.

Acknowledgement:

ChatGPT (OpenAI, San Francisco, CA, USA) was used during manuscript development to assist with conceptual structuring, section organisation, and language refinement. The tool was not used to generate original data, perform literature searches, or determine interpretations. All scientific content, analysis, referencing, and final editorial decisions were independently developed, reviewed, and approved by the author, who assumes full responsibility for the manuscript.

The conceptual figure was developed by the author through an iterative design process with the assistance of ChatGPT (OpenAI) as a visualisation and language-support tool. The author conceived the underlying scientific framework, directed figure development, critically evaluated and revised the visual illustration, and accepts full responsibility for the scientific content, clinical interpretation and final presentation.

References

1.McGrath C, Chau CWR Molina GF. Monitoring oral health remotely: ethical considerations when using AI among vulnerable populations. Front. Oral Health 2025; 6:1587630. https://doi.org/10.3389/froh.2025.1587630

2. Sravya K, Movva JB, Sinha R, et al. Electronic Health Records in Dentistry: A Systematic Review. Journal of Contemporary Clinical Practice. 2024;10(1):71-79.https://jccpractice.com/article/ electronic-health-records-in-dentristry-a-systematic-review-340/#:~:text=10.18683/jccp.2024.1091

3. Mari WA, Siddique M, Sharmam P. Balancing Technology and Trust: Ethical Framework for Digital Transformation in Dentistry. Sarvodaya International Journal of Medicine, 2026; 2(2): 121 – 128. https://doi.org/10.4103/SIJM.SIJM_23_26

4. Araidy S, Batshon G, Mirochnik R. Artificial Intelligence Applications in Dentistry: A Systematic Review. Oral, 2025; 5(4):90. https://doi.org/10.3390/oral5040090

5. Zhou KX, Ng QX, Wu TS, Gigliotti J. Ambient artificial intelligence scribes in dentistry: Benefits, barriers, and a burgeoning research agenda. JADA, 2026:https://doi.org/10.1016/j.adaj.2026.01.016.

6. Health Professions Council of South Africa (HPCSA). Ethical guidelines for good practice in the healthcare professions. Guidelines on the keeping of patient health records. Booklet 9. September 2022. https://www.sada.co.za/sites/default/files/content-files/HPCSA/HPCSA%20Ethical%20Guidelines/Booklet_9_Keeping_of_Patient_

Records_Review%20Draft_vSept_2022.pdf

7. FDI World Dental Federation, Integrated electronic health records: consensus statement 2025.FDI World Dental Federation. https://www.fdiworlddental.org/consensus-statement-integrated-electronic-health-records

8. Schwendicke F, Uribe SE, Walji M, et al. Electronic Health Records in Dentistry: Relevance, Challenges and Policy Directions. Int Dent J. 2025;75(6):103964. https://doi.org/10.1016/j.identj.2025.103964.

9. Pethani F, Dunn AG, Spallek H. Solutions to improve the quality and use of patient records. JADA, 2026; 157(7): 677-681. https://doi.org/10.1016/j.adaj.2025.08.010

10. Morgan A, Youngson C, McLean W. Medico-legal considerations in endodontics. Br Dent J 2025; 238: 573–579. https://doi.org/10.1038/s41415-025-8333-z

11. Ho JCY, Chai HH, Huang MZ, et al. Impact of Modern Communication in Transforming Dental Care. Dentistry Journal, 2025; 13(10):441. https://doi.org/10.3390/dj13100441

12. Kaushik R, Rapaka R. AI-driven evolution in teledentistry: A comprehensive overview of technology and clinical applications. Dentistry Review, 2025; 5(2): 100154. https://doi.org/10.1016/j.dentre.2025.100154.

13. Olakotan O, Samuriwo,R, Ismaila H, Atiku S. Usability Challenges in Electronic Health Records: Impact on Documentation Burden and Clinical Workflow: A Scoping Review. Journal of Evaluation in Clinical Practice, 2025; 31: e70189. https://doi.org/10.1111/jep.70189

14. O´Kane R, Stonehouse-Smith D, Shirazi M. et al. For the record: a narrative review of ambient voice technology in clinical documentation for dentistry and wider healthcare. Br Dent J 2026; 241: 385–393. https://doi.org/10.1038/s41415-026-9951-9

15. General Dental Council (GDC). Maintain and protect patients' information. In Standards for the dental team. 2013. Accessed on the internet at: https://standards.gdc-uk.org/pdf/Standards%20for%20the%20Dental%20Team.pdf

16. Cassim S, Chapanduka ZC. Cyberattack on the National Health Laboratory Service of South Africa - implications, response and recommendations. S Afr Med J. 2024;114(12):e2549. https://doi.org/10.7196/SAMJ.2024.v114i12.2549.

17. Abbas S, Talib MA, Moufti A, et al. Blockchain-Based EHR, EMR, and EDR Systems: A Review of Literature and Market Analysis," 2025 7th International Conference on Blockchain Computing and Applications (BCCA), Durbovnic, Croatia, 2025; 579-586, https://doi.org/10.1109/BCCA66705.2025.11229552.

18. Surdu A, Foia CI, Luchian I, et al. Telemedicine and Digital Tools in Dentistry: Enhancing Diagnosis and Remote Patient Care. Medicina, 2025; 61(5):826. https://doi.org/10.3390/medicina61050826

19. Brinz J, Eslamiamirabadi N, Salamati A, et al. Data sharing for responsible artificial intelligence in dentistry: a narrative review of legal frameworks and privacy-preserving techniques. Journal of Dentistry, 2025; 163: 106130. https://doi.org/10.1016/j.jdent.2025.106130.

20. Liu T-Y, Lee K-H, Mukundan A, Karmakar R, Dhiman H, Wang H-C. AI in Dentistry: Innovations, Ethical Considerations, and Integration Barriers. Bioengineering, 2025; 12(9):928. https://doi.org/10.3390/bioengineering12090928

21. Health Professions Council of South Africa (HPCSA) . Ethical guidelines on the use of AI. Booklet 20. Pretoria: HPCSA, September 2025. https://www.hpcsa-blogs.co.za/wp-content/uploads/2025/11/ETHICAL-GUIDELINES-USE-OF-AI.pdf

22. Makhubela KC. AI in dental practice: From diagnostic aid to practice partner – A strategic and ethical framework. SADJ, 2026; 61(4):230-232. https://www.scielo.org.za/pdf/sadj/v81n4/02.pdf

23. Khurshid Z, Osathanon T, Shire MA, et al. Artificial Intelligence in Dentistry: A Concise Review of Reporting Checklists and Guidelines. Int Dent J. 2026; 76(1):109322. https://doi.org/10.1016/j.identj.2025.109322.

24. Ramnarayan BK, Maniangat, LA, Shetty V, Prasad K. Artificial Intelligence–Driven Dentistry: A Systematic Review of Ethical and Legal Challenges, International Journal of Dentistry, 2026, 1870800, 8 pages, 2026. https://doi.org/10.1155/ijod/1870800

25. Protection of Personal Information Act (POPIA). Act No.4 of 2013. Government Gazette, Vol 581; No: 37067. Cape Town, 26 November, 2013, https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf / https://popia.co.za

26. The Promotion of Access to Information Act (PAIA) Act No. 2 of 2000 . Government Gazette Vol. 416; No.20852. Cape Town , 3 February 2000. https://www.gov.za/sites/default/files/gcis_document/201409/a2-000.pdf

27. Health Professions Council of South Africa (HPCSA). PAIA and POPIA Manual.July 2021. https://www.hpcsa.co.za/page/paia-popia

28. Makhubele KC. (POPIA) The data-driven practice: Transforming POPIA compliance from burden to strategic advantage. SADJ 2026; 81(3): 136-137. https://www.sada.co.za/sites/default/files/2026-06/SADJ%20April%202026%20LR_0.pdf#page=12

29. Sykes D. The Password Was 1234: What a single security assessment revealed about risks facing dental practices in South Africa -- and why changing one password won't fix it. International Dentistry - African Edition, 2026; 16(2): 30

30. Health Professions Council of South Africa (HPCSA). Ethical guidelines for good practice in the healthcare professions. Ethical and professional rules of the HPCSA. Booklet 2. September 2016. https://www.hpcsa-blogs.co.za/wp-content/uploads/2020/12/Ethics_Booklet-2.pdf

31. Govan P. Everything you need to know about dental records. S Afr Dent J. 2024; 79(10): 558–562. https://scielo.org.za/pdf/sadj/v79n10/10.pdf

32. Sciarra FM, Caivano G, Di Vita E, Palermiti M, Messina P, Cumbo EM, Caradonna L, Nigliaccio S, Fontana DA, Scardina A, et al. Infective Endocarditis, Antibiotic Resistance and Dentistry: Clinical and Medico-Legal Aspects. Oral, 2026; 6(1):20. https://doi.org/10.3390/oral6010020