The impact of digital transformation on data security, privacy and confidentiality: Human rights, legal and ethical considerations

Johan Hartshorne[1]

Keywords: Confidentiality, consent, data security, dental practice, digital transformation, electronic communication, ethics, law, legal, rights, privacy.

Executive summary

Importance

- Privacy and confidentiality are foundational principles in healthcare, essential for fostering trust between patients and healthcare providers.
- Digital technology, privacy, and confidentiality are linked through the shared goal of ensuring that information is handled responsibly, securely, and ethically.

Key points

- Patient consent is central to confidentiality.
- Privacy and confidentiality are essential for successful doctor-patient relationships, improved health outcomes and personalized care.
- Managing privacy and confidentiality of patient information is crucial for maintaining patient trust and complying with legal and ethical standards.

Practice implications

- Dental practitioners must be familiar and comply with legal frameworks and ethical guidelines to ensure patient privacy and confidentiality.
- Patients should be informed about how their data will be collected, processed, and shared with third-party providers.
- Informed consent must be obtained before processing and sharing personal information.
- Ensure confidentiality and secure storage of patient records.
- Implement robust data security measures to prevent unauthorized access.
- Practitioners are responsible for ensuring that dental assistants, receptionists and other staff respect confidentiality of patient personal information in the performance of their duties.
- Staff training on data protection protocols and adherence to professional guidelines to enhance the security and confidentiality of patient information is critical.

[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

Background

Digital technology and innovations from the "Internet of Medical Things (IoMT)" have become an integral part of healthcare,[1-3] including dentistry,[4-6] transforming the way data is captured, stored, processed, used, and communicated. The digital transformation is rapidly changing the way how health professionals manage

their practices, network, acquire knowledge and learn, plan treatment, deliver services, and communicate with patients, health care professionals (i.e., medical and dental specialists, dental laboratories), and other third parties (i.e., Medical Aid Funders, Corporate Managers, Dental Supply Companies).[5,6]

Rapid integration of digital technologies that have transformed operational efficiency, accuracy, and communication in modern day dental practices include: (i) electronic health records (EHR's) and cloud-based platforms that offer real time access and data sharing for streamlining practice management tasks like patient record-keeping, appointment scheduling, and billing[7,8] and centralized data storage of patient records;[4] (ii) digital imaging [e.g., intraoral scanners (IOS) for impression taking and 3D cone beam computed tomography (CBCT) scanners to facilitate effective treatment planning and communication;[4,9] (iii) computer-aided design (CAD) / computer-aided manufacturing (CAM) and 3D printers to enhance in-house treatment delivery and optimization of workflow efficiency;[4,7] and (iv) artificial intelligence (AI), interactive digital tools (virtual and assisted reality) that engage patients in their oral health management, motivating them to maintain good oral hygiene practices and habits, and automated clinical decision support (i.e., clear aligners and smile design), and robotics (guided surgery).[7] The use of digital workflow and various 3D-based technologies has become synonymous with modern dental practices.[10]

Simultaneously there has been a global explosion in the access to, and use of social media (SM) networks (e.g., Facebook, X, WhatsApp, LinkedIn); content sharing platforms (e.g., YouTube, Instagram); and electronic communication platforms (i.e., videoconferencing, personal and professional blogs, email, SMS, electronic journals, internet discussion forums). As a result, the way health professionals acquire, communicate, share, publish, marketing, and discuss information have changed.[11]

In addition, remote consultations and monitoring (tele-dentistry), is increasing access to care, combined with integrated smart technologies and wearable devices to facilitate remote monitoring, offering a vast array of personalized treatment options and advantages, increasing access to healthcare, and reshaping patient care and dental practices.[4,7,12]

The digital revolution and transformation is poised to re-shape the dentistry landscape redefining dental care delivery, accessibility, operational efficiency, patient outcomes, practitioner experiences, and dramatically changing the patient–dentist interaction and experience.[1,2,3,7,9,13,14,15] Data has become the new currency for driving operational efficiency and accuracy, personalized treatment planning, and improved oral health outcomes, as the *'Internet of Things' has evolved to the 'Intelligence of Things'.*[7]

While these technologies improve practice delivery efficiency and patient experience, they also create vulnerabilities related to data security resulting in significant challenges regarding privacy and confidentiality of patient information.[5,16,17,18] The use of digital technologies pose significant risks to data security due to the following factors: (i) cyberattacks, hacking, and data breaches of sensitive patient information; (ii) unauthorized access to electronic health records (EHRs) and digital databases; (iii) data sharing and interoperability of collaborative platforms inadvertently exposing patient data; and (iv) tele-dentistry and remote planning and care increasing the risk of data interception through insecure networks. These risks can lead to the exposure of personal and health information, potentially causing identity theft, financial loss, damage to reputation, and subsequent loss of patient trust, raising serious human rights, ethical and legal consequences and challenges.[13]

Abovementioned vulnerabilities and concerns require that practitioners have to adopt robust data security protocols, procedures, authorizations, and safeguards to protect the integrity, availability of, access to, and communication of sensitive patient information. Healthcare professionals and their staff must be educated regarding the lawful processing of personal information, respect the rights of patients, and limit the consequences of careless handling of data.[18] It has also been suggested that: "*often the biggest liability in any system is the individuals using it.*" [17]

Purpose

The purpose of this review is to: (i) explore the impact of digital transformation in dentistry on data security, patient privacy and confidentiality; (ii) enhance practitioners understanding of data security, privacy, and confidentiality, including the human rights, legal and ethical considerations thereof; and (iii) to probe current key strategies for the handling of sensitive patient data or information.

The definition and relevance of privacy and confidentiality

Raw data consists of unprocessed facts or figures that by themselves may not identify an individual. [e.g., 32 (age); #16 (Upper right first molar); and BI=5.5% (Bleeding index)] When data is linked to unique personal identifiers such as

a name, ID number, or contact information, it becomes personal information. (e.g., John Doe, Age: 32, Patient ID: 123456, Cell: 084 667 8092). When personal information is linked to certain data types such as health records, treatment records, financial details, or biometric data (e.g., "John Doe has periodontal disease"), then it becomes sensitive personal information). Data concerning a patient's state of health, diagnosis, prognosis, medical and dental treatment has a particularly sensitive nature and is therefore private and confidential.

Privacy and confidentiality and are among the oldest and most important safeguards that human rights, ethical, and legal frameworks globally offer to patients. Confidentiality and privacy are related but distinct concepts, especially in contexts like healthcare, law, and data protection.

- ***Privacy***

Privacy pertains to people and refers to the rights of the patient. Privacy is the patient's right to have their health and personal information stored securely and not revealed without proper authorization, and we speak of a 'loss of privacy'.

Privacy refers to an individual's right to control access to their personal information and to make decisions about what, when, and how much information about themselves is shared with others. Privacy is a broader concept than confidentiality, encompassing individuals' autonomy over their personal data, physical space, and lifestyle choices. Privacy is also a state of being free from public attention. In the context of personal data, privacy laws (such as POPIA in South Africa) aim to give individuals control over how their information is collected, stored, processed, and shared by health care practitioners.

- ***Confidentiality***

Confidentiality pertains to information and refers to the duty of the provider to prevent 'breach of confidentiality' through controlled release of personal information, disclosing it only with the patient's consent or under legally mandated circumstances. Confidentiality is the obligation of professionals and other health workers not to disclose information about people to unauthorised third parties, especially when it involves sensitive or personal details shared in a trusted relationship.

Confidentiality is an ethical and often legal obligation for professionals to protect information shared by clients, patients, or colleagues, ensuring it is only used or shared as agreed upon. Confidentiality is about keeping information private once it's shared within a trusted relationship; it's a duty or obligation to protect the information shared. Breaching confidentiality can lead to emotional harm, loss of trust, and reluctance to seek care, particularly in cases involving sensitive issues such as mental health or infectious diseases.

- ***Importance***

Privacy and confidentiality are foundational principles in healthcare, essential for fostering trust between patients and healthcare providers. These principles protect sensitive patient information from unauthorized access or disclosure, ensuring that individuals feel secure sharing personal details critical to their diagnosis and treatment. When patients trust that their personal and medical information will remain confidential and private, they are more likely to be open and honest to disclose accurate and complete details about their health, leading to better diagnosis and treatment.[19] This transparency allows healthcare providers to deliver effective care. The definition, context and goals of privacy and confidentiality are discussed in greater detail by Martin in the *'Handbook of Global Bioethics'*. [20]

Human rights, legal, and ethical framework for privacy and confidentiality

Privacy and confidentiality are world-wide rooted in human rights, legal frameworks, and ethical standards. Confidentiality of personal information in healthcare is protected by a combination of constitutional, common law, and statutory frameworks, that establish legal obligations for healthcare providers. These frameworks are designed to safeguard patients' rights to privacy, ensuring that their health information is kept confidential. Confidentiality is central to trust between healthcare practitioners and patient. "Without assurances about confidentiality, patients may be reluctant to give healthcare practitioners the information they need in order to provide good care."[19] Being registered under the Health Professions Act No. 56 of 1974, gives healthcare practitioners certain authority and privileges. In return, healthcare practitioners have a duty to meet the standards of competence, care and conduct set by the HPCSA and its Professional Boards.[19]

- ***Human rights (Rights##)***

Human rights principles are enshrined in the Constitution of the Republic of South Africa[21] which guarantees every persons right to privacy. This constitutional provision obligates healthcare providers to respect patient's rights, and

to safeguard patients' personal and medical information needed to maintain and improve healthcare for individual patients, ensuring that it is not disclosed without consent.[19] This constitutional right underpins confidentiality, especially regarding individuals' control over their personal data, and is fundamental to safeguarding human dignity and autonomy.

The HPCSA Ethical Guidelines on: *"Confidentiality: Protecting and Providing Information, set out a framework for respecting patient rights, while ensuring that information needed to maintain and improve healthcare for individual patients and society is disclosed to those who need it for such purposes."*[19] For instance - *"A healthcare practitioner (i.e., specialist) cannot treat a patient safely, nor provide continuity of care without having relevant information about the patient's condition or medical history."* The Department of Health (DoH) has committed to upholding, promoting and protecting patient rights through proclamation of a National Patients' Rights Charter as a common standard for achieving the realization of patient rights.[22]

Although confidentiality is strongly protected, the Constitution's limitations clause (Section 36) allows for lawful restrictions on rights, including the right to privacy, when necessary and reasonable in an open and democratic society. For example, confidentiality may be limited in cases involving public interest, national security, or lawful investigations. However, such limitations must be justified and proportionate, respecting individuals' fundamental rights.

- ***Legal framework***

The National Health Act (NHA)

Dental practitioners hold information about patients which are private and sensitive and protecting the confidentiality of this information is enshrined in law. The National Health Act (NHA)23 (Act No.61 of 2003) states that all patients have a right to confidentiality, and this is consistent with the right to privacy in the South African Constitution. This core statute is central to patient confidentiality in South Africa's healthcare sector. It mandates that healthcare providers keep patient information confidential, unless the patient consents, and may only share it with others under specific, lawful circumstances. Section 14 of the NHA explicitly requires that healthcare providers do not disclose any patient information without the patient's expressed consent, unless legally authorized or required to protect public health, or when necessary for the proper treatment of the patient.[17,19] According to the National Health Act (No.61 of 2003) dental practitioners may only disclose information regarding a patient in the following circumstances: (i) if it is done in terms of a statutory provision; (ii) an instruction of court; (iii) in the public interest; (iv) with the express consent of a patient; (v) with a written consent of a parent or guardian of a minor under the age of 12 years; (vi) or in the case of a deceased patient, with the written consent of the next of kin or the executor of the deceased estate.[19]

Patients therefor have a right to expect that information about them will be held in confidence by health care practitioners.[17,19] Patients also, have the right to access their health records, and healthcare providers must ensure this access is granted appropriately.[17,19] For healthcare information related to children, the Children's Act (Act No. 38 of 2005)[24] provides additional protections for the processing and sharing of personal information of minors.[25]

The Protection of Personal Information Act (POPIA)

The Protection of Personal Information Act (POPIA), also referred to as the 'POPI Act' (POPIA, 2013)[26] is specifically designed to protect personal information and maintain confidentiality, and it aligns with the human rights principle that individuals have the right to control and protect their personal data. The POPI Act enforces the constitutional right to privacy and brings South African law in line with global standards for data protection and privacy. POPIA emphasizes that personal information must be processed lawfully and securely, respecting data subjects' rights to confidentiality and providing individuals with control over their data. POPIA also gives individuals enforceable rights, including the right to access and correct their information, the right to be informed about its use, and the right to withdraw consent.

According to the POPI Act, health practitioners and service providers are legally required to carefully manage data capture, storage processes, and disclosing and communicating personal information of a patient to other stakeholders (i.e., healthcare practitioners, laboratory technicians, referrals to specialists and medical schemes)

The purpose of the Act is to provide for the rights of persons regarding unsolicited electronic communication and automated decision-making, and to regulate the flow of personal information. POPIA ensures that patient information is handled responsibly, limiting unauthorized access and misuse. POPIA also grants patient's rights to access their information, correct inaccuracies, and seek recourse if their data is mishandled. Healthcare practitioners must follow these data protection principles, integrating POPIA's standards with those established by the National Health Act.

Dental practitioners have the following responsibilities regarding communication and safeguarding privacy and

disclosure of personal information:[26] (i) accountability for ensuring POPIA compliance; (ii) processing (using only that information that is required; (iii) personal information must only be collected for a specific purpose; (iv) further processing must be compatible with the original purpose of the collection of information; (v) steps must be taken to ensure that personal information records are complete, accurate and up to date; (vi) disclose only certain information to specific data subjects; (vii) ensure that appropriate, reasonable and organisational measures and safe-guards are implemented and maintained to prevent loss, damage or unauthorised destruction or unlawful use or access to personal information, and (viii) data subjects (patients) have the right to request personal information that a responsible party (dental practitioner) holds about them and in circumstances request access to such information. Dental practitioners are responsible for ensuring that receptionists, assistants and other staff respect confidentiality in the performance of their duties.

Ethical basis

Fundamental ethical principles

The ethical basis for confidentiality of personal information rests on key principles and core values, including respect for autonomy, trust, non-maleficence, beneficence, and fairness.[25] The principle of autonomy require professionals to keep patient information private, except in cases where disclosure is justified or legally required, or informed consent is obtained.[25] Individuals have the right to understand how their personal information will be used, to whom it may be disclosed, and the potential risks and benefits. Informed consent empowers individuals to make informed choices, furthering respect for autonomy.

Another important reason for maintaining confidentiality is to uphold the ethical duty of beneficence. Protecting confidentiality helps individuals feel safe and respected, promoting their mental, emotional, and social well-being. Without confidentiality, the fear of stigma, discrimination, or breach of privacy may deter individuals from seeking medical attention or providing truthful information, potentially resulting in harm. Unauthorized disclosure of personal information can result in significant harm, such as social stigma, emotional distress, financial loss, or discrimination. By maintaining confidentiality, individuals and institutions can avoid causing harm that could arise from breaches of privacy, thus respecting the well-being of others and adhering to a commitment to "do no harm."

Confidentiality is also rooted in the ethical principles of fairness and justice, which emphasize equal treatment and respect for all individuals' rights. Upholding confidentiality means respecting everyone's right to privacy equally, without discrimination. Fairness also requires that information collected from individuals is used responsibly and ethically, protecting against misuse that could unfairly disadvantage or discriminate against certain individuals or groups.

Confidentiality is fundamental to establishing and maintaining trust, particularly in sensitive relationships such as those with healthcare providers, legal professionals, and employers. People are more likely to share personal or sensitive information if they believe it will be kept confidential. These principles emphasize the importance of treating individuals with respect, protecting their personal data, and building ethical relationships. In ethical practice, confidentiality is seen not just as a legal requirement, but as a core value that upholds trust, fairness, and the dignity of those whose information is held in confidence.

HPCSA Ethical Guidelines

The Health Professions Council of South Africa (HPCSA) guidelines mandate that healthcare providers respect patient privacy and confidentiality as part of their professional conduct. Dental practitioners therefor have an ethical duty and responsibility to respect the privacy, confidentiality and dignity of patients.[25] This obligation promotes trust in the provider-patient relationship, enabling open communication essential for accurate diagnosis and effective treatment.[19]

The HPCSA Ethical Guidelines, are based upon international ethical codes, The South African Constitution (Act No.108 of 1996) and the National Health Act (Act No. 61 of 2003). It offers ethical guidance and directions to healthcare professionals code of conduct relating to: Core ethical values;[25] Confidentiality;[19] Informed consent;[27] Keeping of patient health records;[28] Use of social media platforms;[29] and Telehealth.[12] These guidelines reinforce the duty of confidentiality and require professionals to keep patient information private, except in cases where informed consent is given, disclosure is justified or legally required. [25,30]

Together, these constitutional, statutory, and ethical frameworks create a comprehensive legal basis for confidentiality of personal information in healthcare in South Africa. They emphasize that patient confidentiality is a fundamental right that healthcare providers are legally and ethically obligated to protect.

Key Strategies for protecting data security, privacy, and confidentiality

Protecting and maintaining data security, and respecting privacy and confidentiality is important for upholding the dentist-patient trust relationship, complying with legal obligations, and meeting professional ethical standards. The common denominator that connects digital technology, privacy, and confidentiality is the need for personal and medical data protection and responsible information management. To mitigate privacy and confidentiality risks, dental practices should adopt the following strategies. By implementing these practical steps, dental practices can uphold confidentiality, comply with legal and ethical standards, and enhance the quality of care and trust in their patient relationships.

- ***Comply with HPCSA Ethical Guidelines***

Dental practitioners have a duty and responsibility to respect the privacy, confidentiality, and dignity of patients. The HPCSA offers ethical guidance and directions in this regard.

- ***Compliance with POPI Act regulations***

Inform patients or provide them with a privacy policy that explains how their data is collected, stored, processed, shared, and protected. Ensure patients can access their records and request corrections as necessary.

- ***Patient communication protocols***

Confirm the identity of patients or authorized healthcare partners before sharing sensitive information. Use encrypted email, secure messaging systems, or patient portals for sharing sensitive information. Always obtain patient consent before sharing information with third parties (e.g., specialists, dental laboratories, insurance companies).

- ***Minimize exposure of patient information***

Ensure that computer screens are not visible to unauthorized persons, and use privacy screens when necessary. Share only the minimum necessary information required for a task or consultation. De-identify Information (Anonymise) data, when full identification is not needed.

- ***Protect patient privacy during patient consultations***

Consultations should be conducted in private settings where others cannot overhear confidential information. Dental staff should ensure that conversations about a patient's health or treatment do not take place in public areas like the reception area, where they can be overheard, or leave patients' records (paper or electronically) where they are vulnerable to disclosure, where they can be seen by other patients, unauthorised health care personnel or the public This helps to maintain a patient's sense of privacy and trust in the practice's commitment to confidentiality.

- ***Secure storage and access to patient records***

Data storage, secure access control, and data sharing are three key aspects that must be enhanced to ensure the security and privacy of patient information. Dental practices must ensure that patient records, including medical histories, treatment plans, and x-rays, are stored securely, whether in physical or digital form. Physical records should be kept in locked cabinets, and EHR's records should be protected with secure passwords, encryption, and access controls. Unauthorized access to these records should be strictly controlled, with only authorized staff members having access to sensitive patient information.

- ***Conduct regular information technology risk assessments and audits***

Conduct regular risk assessments and audits of digital records and data bases to identify vulnerabilities and to ensure adherence to confidentiality policies through internal and third-party audits, and update software and security protocols in response to evolving cyber threats. Have a clear protocol for reporting and managing data breaches or confidentiality violations.

- ***Ensure secure tele-dentistry practices***

Use POPIA-compliant telehealth platforms with secure video conferencing and data transmission. Educate patients on securing their end of communication, such as using private networks and secure devices. The use of social media platforms for the purpose of Tele-Dentistry is not desirable.[29]

- ***Staff training and confidentiality protocols***

Dental practitioners are responsible for ongoing training for all staff including, dental assistants, receptionists, and administrative personnel to ensure that they respect confidentiality in the performance of their duties.[17,19] Training should cover topics like secure handling of information, respectful communication, and understanding the importance of confidentiality in upholding patient trust. Regularly remind staff to avoid discussing patient information in public areas or outside the practice. Signing confidentiality agreements should also be part of staff employment contracts.

- ***Sharing or publishing patient information on social media***

Dental practitioners are advised to err on the side of caution when using social media for sharing content online for marketing or educational purposes. If uncertain about whether it is ethically and legally permissible to share particular content via social media, it is best not to do so until advice has been obtained.[29] Always ensure that the recipient of the information is not able to identify the patient from the data disclosed. Dental practitioners must obtain the written consent of the patient before publishing information (e.g. case histories and photographs) about them in social media platforms.

Electronic communication by email or text messaging can raise special ethical and legal concerns about confidentiality and privacy, particularly when sensitive and personal information about a patient has to be communicated. A dental practitioner engaging in electronic communication holds the same ethical responsibilities to a patient as during other clinical encounters.31 It's essential to be vigilant about what is shared online to protect patient confidentiality.

Conclusions

The dental profession is undeniably in transformation, with dental practitioners increasingly relying on new digital technologies, social media, and electronic communication platforms to increase practice management and workflow efficiency, improved communication and sharing of health information, and to promote the patient experience. Electronic communication is indispensable in modern data exchange, but it must be carefully managed to uphold data privacy and confidentiality. By leveraging robust security measures and adhering to legal and ethical standards, dental practitioners and their staff can protect patient sensitive information and build trust in the digital ecosystem.

Privacy and confidentiality are foundational principles in healthcare, essential for fostering trust between patients and healthcare providers, encouraging open communication that leads to accurate diagnoses and effective treatment. These principles protect sensitive patient information from unauthorized access or disclosure, ensuring that individuals feel secure sharing personal details critical to their diagnosis and treatment. Protecting and maintaining data security, and respecting privacy and confidentiality is important for upholding the dentist-patient trust relationship, complying with legal obligations, and meeting professional ethical standards.

In South Africa, the Protection of Personal Information Act and the National Health Act provide a legal framework for safeguarding personal health data. These laws require healthcare providers to implement strict measures, such as secure data storage and obtaining informed consent for data sharing. Respecting the privacy rights and confidentiality of personal information of patients is both an ethical requirement as well as legally mandated. Both concepts are integral to healthcare, ensuring that sensitive information is handled with utmost care and respect for the patient's autonomy and dignity.

Digital transformation presents unique challenges in maintaining patient confidentiality and privacy. By implementing robust security measures, adhering to human rights, legal and ethical standards, and fostering a culture of privacy awareness, dental practices can safeguard patient information while leveraging the benefits of technological advancements.

Ultimately, maintaining confidentiality and privacy while responsibly managing disclosure fosters trust, upholds patients' rights, and ensures compliance with ethical and legal standards in healthcare. This trust is crucial for effective healthcare delivery, as it encourages patients to share information necessary for accurate diagnosis and treatment. As technology continues to evolve, it is vital for healthcare systems to adapt and prioritize these principles to maintain patient confidence and promote better health outcomes. By adhering to legal standards, securing patient data, obtaining informed consent, and using technology responsibly, dental professionals can protect patient privacy, uphold trust, and ensure that their practices remain ethical and compliant with both regulations and professional guidelines.

References

1. Schierz O, Hirsch C, Krey K-F, et al. Digital dentistry and its impact on oral health-related quality of life. J of Evid-Based Dent Prac, 2024; 24(1): Supplement, 101946, https://doi.org/10.1016/j.jebdp.2023.101946.

2. Alawiye T. The Impact of Digital Technology on Healthcare Delivery and Patient Outcomes. E-Health Telecommunication Systems and Networks, 2024; 13: 13-22. https://doi.org/10.4236/etsn.2024.132002

3. Paul M, Maglaras L, Ferrag, MA, Almomani I. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express 2023; 9(4): 571–588. https://doi.org/10.1016/j.icte.2023.02.007

4. Khoury P. Embracing evolution: How dental leaders navigate the shift from traditional to digital practices. Dental Economics July

18, 2024. https://www.dentaleconomics.com/science-tech/article/55093146/embracing-evolution-how-dental-leaders-navigate-the-shift-from-traditional-to-digital-practices

5. Mariño RJ, Zaror C. Legal issues in digital oral health: a scoping Review. BMC Health Services Research, 2024; 24: 6 https://doi.org/10.1186/s12913-023-10476-w

6. Metty P, Leandros M, Mohamed AF, Iman A. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 2023; 9(4): 571-588 https://doi.org/10.1016/j.icte.2023.02.007.

7. Seif A, Jarry C R, Chauvel A M. The New 'Golden Age' of Dentistry: A Highly Desirable Profession with Unprecedented Global Opportunities in Industry Settings. J Calif Dent Assoc, 2024; 52(1): https://doi.org/10.1080/19424396.2024.2324979

8. Shojaei P, Vlahu-Gjorgievska E, Chow Y-W. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. Computers. 2024; 13(2): 41. https://doi.org/10.3390/computers13020041

9. Khurshid Z. Digital Dentistry: Transformation of Oral Health and Dental Education with Technology. Eur J Dent, 2023;17(4): 943-944. https://doi.org/10.1055/s-0043-1772674

10. Maart RD, Mulder, R. (2024). Ethical considerations for artificial intelligence in dentistry. S Afr Dent J , 2024; 79(5): 260- 262. https://dx.doi.org/10.17159/sadj.v79i05.18355

11. Sykes LM, Harryparsad A, Evans WG, Gani F. Social Media and Dentistry: Part 8: Ethical, legal, and professional concerns with the use of internet sites by health care professionals. S Afr Dent J 2017; 72(3): 132-136. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S0011-85162017000300009&lng=en.

12. Health Professions Council of South Africa. General ethical guidelines for good practice in Telehealth. Edited by The Committee for Human Rights, Ethics and Professional Practice of the HPCSA. Booklet 10, 2021. Accessed on the internet at: https://www.hpcsa.co.za/Uploads/professional_practice/ethics/Booklet_10_Telehealth_Dec_2021_v2.pdf

13. Alqahtani SAH. Enhancing dental practice: cutting-edge digital innovations. Braz J Oral Sci 2024; 23: e0240115. https://doi.org/10.20396/bjos.v23i00.8674785

14. Lelyana N. Strategic Analysis in the Application of Digital Technology in Dental Practice. J of Soc Interactions and Humanities (JSIH), 2023; 2(3): 253-274. https://journal.formosapublisher.org/index.php/jsih/article/view/6441/6871

15. Favaretto M, Shaw D, De Clercq E, et al.. Big data and digitalization in dentistry: A systematic review of the ethical Issues. Int J Environ Res Public Health. 2020; 17(7): 2495. https://doi.org/10.3390/ijerph17072495.

16. Naeem MM, Sarwar H, Hassan MT, et al. Exploring the ethical and privacy implications of artificial intelligence in dentistry. Int J of Health Sci, 2023; 7(S1): 904–915. https://doi.org/10.53730/ijhs.v7nS1.14294

17. Peters F. The POPI Act vs medical records. Family Medicine at TUKS, Faculty of Health Sciences, University of Pretoria. Accessed on November, 27, 2024 on the Internet at: https://www.up.ac.za/media/shared/62/CPD/CPD%202019/Presentations/peters-frank-prof-presentation-popi-act.zp173622.pdf

18. Buys M. Protecting personal information: Implications of the Protection of Personal Information (POPI) Act for healthcare professionals. S Afr Med J 2017; 107(11): 954-956. https://doi.org/10.7196/SAMJ.2017.v107i11.12542

19. Health Professions Council of South Africa. Confidentiality: Protecting and providing information – Guidelines for good practice in the healthcare professions. HPCSA, Booklet 5, December 2021. Accessed on the Internet at: https://www.hpcsa.co.za/Uploads/professional_practice/ethics/Booklet_5_Confidentiality_Protecting_and_Providing_Information_vDec_2021.pdf

20. Martin JF. Privacy and confidentiality. Ch.9; pp. 119-137. In: Handbook of Global Bioethics. Eds. HAMJ ten Have & B Gordijn. Springer Science and Business Media. Dordrecht, 2014. https://www.researchgate.net/profile/Francis-Masiye/publication/263007847_Handbook_of_Global_Bioethics/links/59099c12a6fdcc4961683ae3/Handbook-of-Global-Bioethics.pdf#page=137

21. South African Government. Constitution of the Republic of South Africa. Chap 2: Bill of Rights; Section 14: Privacy. Accessed on the Internet at: https://www.gov.za/documents/constitution/constitution-republic-south-africa-1996-04-feb-1997

22. Health Professions Council of South Africa (HPCSA B3 2023). National Patients' Right Charter. Guidelines for good practice in the health professions Booklet 3, September 2023. https://www.hpcsa.co.za/Content/upload/professional_practice/ethics/Booklet_3_Patients_Rights_Charter_vSept_2023.pdf

23. South African Government. National Health Act 61 of 2003. Accessed on the Internet at: https://www.gov.za/documents/acts/national-health-act-61-2003-23-jul-2004

24. South African Government. Children's Act No. 38 of 2005. Accessed on the Internet at: https://www.gov.za/sites/default/files/gcis_document/201409/a38-053.pdf

25. Health Professions Council of South Africa (HPCSA B1 2021) General ethical guidelines for the health care professions. Booklet 1. December 2021. Accessed on the Internet at: https://www.hpcsa.co.za/Uploads/professional_practice/ethics/Booklet_1_Guidelines_for_Good_Practice_vDec_2021.pdf

26. Government of South Africa. Protection of Personal Information Act No. 4 of 2013. Accessed on the Internet at: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

27. Health Professions Council of South Africa (HPCSA B4 2021). Seeking patients informed consent: The ethical considerations – Guidelines for good practice in the healthcare professions. HPCSA, Booklet 4, December 2021. Accessed on the Internet at: https://www.hpcsa.co.za/Uploads/professional_practice/ethics/Booklet_4_Informed_Consent_vDec_2021.pdf

28. Health Professions Council of South Africa (HPCSA B9 2022). Guidelines on keeping of patient health records. General ethical guidelines for good practice in Telehealth. Guidelines for good practice in healthcare professions. Edited by The Committee for Human Rights, Ethics and Professional Practice of the HPCSA. Booklet 9, 2022. Accessed on the internet at:https://www.hpcsa.co.za/Uploads/professional_practice/ethics/Booklet_9_Keeping_of_Patient_Records_Review%20Draft_vSept_2022.pdf

29. Health Professions Council of South Africa (HPCSA B16 2019). Ethical guidelines on social media. Edited by The Committee for Human Rights, Ethics and Professional Practice of the HPCSA. Booklet 16, 2019. Accessed on the internet at: https://www.hpcsa-blogs.co.za/wp-content/uploads/2019/09/HPCSA-Booklet-16-Ethical-Guidelines-on-Social-Media.pdf

30. Legalwise. The right to privacy and access to medical information. Accessed on November, 14, 2-24. Internet at: https://www.legalwise.co.za/help-yourself/legal-articles/right-privacy-and-access-medical-information#:~:text=Patients%20often%20approach%20their%20trusted,information%20without%20his%2Fher%20consent.

31. American Medical Association (AMA). AMA Code of Medical Ethics. Accessed on November 16, 2024, at: https://code-medical-ethics.ama-assn.org/sites/amacoedb/files/2022-08/2.3.1.pdf