MEDDOCS Open Access Publisher

ISSN 2639-4391

Annals of Epidemiology and Public Health

Open Access | Review Article

Fortifying the Digital Clinic: A Comprehensive Guide to Cybersecurity in the Modern Dental Office

***Bita Parnian*[1]*; *Omid Panahi*[2]**

[1]*Tehran University of Medical Sciences, School of Public Health, Tehran, Iran.*

[2]*Department of Healthcare Management, University of the People, California, USA.*

***Corresponding Author(s): Bita Parnian**

Tehran University of Medical Sciences, School of Public Health, Tehran, Iran.

Email: bita.p.afsharian@gmail.com

Received: Mar 21, 2026

Accepted: Apr 03, 2026

Published Online: Apr 10, 2026

Journal: Annals of Epidemiology and Public Health

Publisher: MedDocs Publishers LLC

Online edition: http://meddocsonline.org/

Keywords: Cybersecurity; Dental pactice; HIPAA Compliance; Ransomware; Data breach; Protected health information (PHI); Risk assessment; Encryption; Multi-factor authentication.

Abstract

As dental practices undergo rapid digital transformation, the integration of electronic health records, digital imaging, cloud-based software, and connected devices has exponentially increased the risk of cyberattacks. The healthcare sector now accounts for nearly one-third of all data breaches, with dental offices emerging as prime targets due to the high value of patient data and often limited security resources. This comprehensive article explores the multifaceted landscape of cybersecurity in modern dentistry. It examines the specific threat landscape facing dental practices, the stringent regulatory frameworks such as HIPAA and GDPR, essential technical and administrative safeguards, the critical role of human factors, and future trends including AI-driven threats. By synthesizing current research and industry best practices, this paper provides a roadmap for dental professionals to protect patient data, ensure regulatory compliance, and maintain operational resilience in an increasingly hostile digital environment.

Introduction

The modern dental office bears little resemblance to its counterpart of just two decades ago. Paper charts have been replaced by Electronic Health Records (EHRs), film radiographs have given way to digital sensors and Cone-Beam Computed Tomography (CBCT), and appointment books have evolved into sophisticated cloud-based practice management systems. While these technological advances have undeniably enhanced diagnostic capabilities, treatment outcomes, and practice efficiency, they have also introduced a new and formidable challenge: cybersecurity [1-23].

Dental practices are now data-rich environments, storing extensive repositories of Protected Health Information (PHI), including personal identifiers, medical histories, insurance details, billing information, and radiographic images. This data is exceptionally valuable on the black market often 50 times more valuable than financial information alone because of its permanence and potential for identity theft and insurance fraud. Cybercriminals have taken notice [24-29].

Contrary to the assumption that attackers target only large hospitals or financial institutions, small and medium-sized healthcare practices, including dental offices, have become preferred targets. They are perceived as low-hanging fruit: they possess valuable data but often lack dedicated IT security staff, robust defenses, and comprehensive response plans. The statistics are sobering: the healthcare sector accounts for 32% of all recorded data breaches, nearly double the rate of the financial and manufacturing sectors, and reports of healthcare data breaches increased by 89% between 2019 and 2023 [30-42]. The average cost of a healthcare data breach reached $9.8 million in 2024.

Cite this article: Bita P, Omid P. Fortifying the Digital Clinic: A Comprehensive Guide to Cybersecurity in the Modern Dental Office. A Epidemiol Public Health. 2026; 9(1): 1133.

This article provides a comprehensive examination of cybersecurity in the dental office. It aims to equip dental professionals from solo practitioners to multi-location group practices—with the knowledge necessary to understand their risks, meet their legal obligations, and implement effective protection strategies [43].

The cyber threat landscape in dentistry

Understanding the specific threats facing dental practices is the first step toward effective defense. Cybercriminals employ a variety of tactics, many of which are increasingly sophisticated and tailored to exploit the unique vulnerabilities of healthcare settings [44-50].

Why dental practices are attractive targets

Dental practices occupy a dangerous intersection of high-value data and structural vulnerability, creating what experts call a "triangle of vulnerability".

- High Value of Health Data: Medical records contain permanently sensitive information names, addresses, Social Security numbers, medical histories, and insurance credentials. This data can be used for years to commit fraud, file false insurance claims, or steal identities.
- Limited Security Resources: Most dental practices operate as small businesses. They rarely employ dedicated IT security professionals, operate with constrained security budgets, and often run outdated hardware or unsupported software, creating known vulnerabilities.
- Operational Dependency: Modern dental practices are entirely dependent on their digital systems. A ransomware attack that encrypts patient records and imaging software can halt all clinical operations, forcing cancellations and revenue loss while compromising patient care [51].

Common types of cyberattacks

Several types of attacks are particularly prevalent and damaging in the dental sector.

- Ransomware: This is among the most feared threats. Malicious software encrypts the practice's data, rendering it inaccessible, and attackers demand a ransom typically in cryptocurrency for the decryption key. Ransomware has evolved into "double extortion" schemes, where attackers not only encrypt data but also steal it, threatening to publish sensitive patient information if the ransom is not paid. In some cases, attackers have even directly extorted patients, demanding small payments to prevent the release of their personal data. The official guidance from cybersecurity authorities worldwide is clear: never pay the ransom, as payment does not guarantee recovery and only fuels further criminal activity [52].
- Phishing and Social Engineering: Phishing remains one of the most common and effective attack vectors, responsible for the majority of successful breaches. Attackers send deceptive emails, text messages, or phone calls that appear legitimate, tricking employees into revealing login credentials or downloading malware [53]. With the rise of artificial intelligence, phishing campaigns have become significantly more sophisticated. AI-generated phishing emails are nearly indistinguishable from genuine communications, and studies show that more than half of healthcare professionals cannot reliably identify fraudulent emails. AI allows attackers to launch personalized campaigns at massive scale, increasing their success rate dramatically.
- Data Breaches: Data breaches can result from various causes, including software vulnerabilities, weak passwords, successful phishing attacks, or even accidental insider actions. Once attackers gain access, they exfiltrate sensitive patient information, which can then be sold on the dark web or used for fraud. The consequences are severe. For example, in December 2023, a pediatric dental surgery center experienced a data breach compromising names, Social Security numbers, and medical records, resulting in a class-action lawsuit settlement offering affected individuals up to $8,050 in compensation. In another case, a major dental insurer suffered a ransomware attack affecting nearly nine million patients, with stolen data ultimately released online when the company refused to pay the $10 million ransom [54].
- Insider Threats: Not all threats originate externally. Insider threats whether intentional or accidental—pose significant risks. Employees may unknowingly expose the network to malware by falling victim to phishing, improperly configure systems allowing unauthorized access, or in rare cases, act maliciously by stealing data for personal gain. A dental surgery receptionist was sentenced to 2 to 6 years in prison in 2018 for abusing system access to steal the identifiable health information of 653 patients [55].

Regulatory and legal framework

Dental practices operate within a complex web of legal and regulatory requirements designed to protect patient data. Compliance is not optional it is a legal obligation with significant penalties for failure [56].

HIPAA: The Cornerstone of U.S. Dental Compliance

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) sets the national standards for protecting PHI. Most dental practices qualify as HIPAA Covered Entities because they transmit health information electronically for transactions such as insurance claims, eligibility checks, and authorizations [57].

HIPAA comprises three primary rules relevant to dental practices:

- The Privacy Rule: This rule requires dentists to implement appropriate safeguards to protect the privacy of PHI and places conditions on its use and disclosure. It mandates that patients receive a Notice of Privacy Practices (NPP) explaining how their information may be used. Incidental disclosures such as calling a patient's name in the waiting room must be minimized to the extent reasonable. The Privacy Rule also requires the appointment of a HIPAA Privacy Officer [58].
- The Security Rule: This rule specifically addresses electronic PHI (ePHI) and is organized into three categories of safeguards:
- Administrative Safeguards: These include conducting regular risk assessments, designating a Security Officer, implementing security awareness training, and maintaining written policies and procedures [59].
- Physical Safeguards: These concern the security of computer systems and their environment, including facility access

controls, workstation security, and proper disposal of media containing ePHI.

- Technical Safeguards: These address the technology used to protect ePHI, including access controls, audit controls, integrity controls, and transmission security (encryption).
- The Breach Notification Rule: If unsecured PHI is impermissibly disclosed, this rule requires dentists to notify affected individuals within 60 days of breach discovery. The Department of Health and Human Services' Office for Civil Rights (OCR) must also be notified immediately for breaches affecting 500 or more individuals, and annually for smaller breaches. For large breaches, local media notification is also required [60].

Penalties for non-compliance

The financial consequences of HIPAA violations can be devastating. Fines range from $100 to $50,000 per violation, with a maximum annual penalty of $1.5 million per violation category. Real-world examples abound:

- In 2015, an Indiana dentist was fined $12,000 for abandoning thousands of patient records in boxes found by a dumpster.
- In 2019, Elite Dental Associates in Texas agreed to a $10,000 settlement for impermissibly disclosing patients' ePHI on a review website.
- In 2022, three dental practices reached settlements totaling $142,500 for noncompliance with patients' access rights, disclosing PHI on social media, and impermissibly using PHI for marketing.
- A 2023 Illinois dental office paid $80,000 for inadequate Privacy Rule training following a PHI disclosure.

International considerations: GDPR and beyond

For practices operating in the European Union or handling data of EU residents, the General Data Protection Regulation (GDPR) applies. GDPR classifies health data as a "special category" requiring reinforced protection. Key requirements include maintaining a Record of Processing Activities (ROPA), ensuring data minimization, and demonstrating accountability through documented compliance measures. Some U.S. states, such as California with its CCPA and Illinois with its Personal Information Protection Act, have enacted additional privacy laws that may impose stricter requirements than HIPAA, requiring practices to navigate overlapping regulatory frameworks [61].

Technical safeguards: Building a secure infrastructure

Effective cybersecurity requires a multi-layered defense strategy. Technical safeguards form the core of this approach, protecting data at rest, in transit, and during processing [62].

Access controls and authentication

Controlling who can access ePHI is fundamental. HIPAA requires unique user identification so that each individual accessing systems can be tracked [63].

- Strong Passwords: All passwords should be unique, complex, and regularly updated. Shared logins are unacceptable and create audit trail gaps.
- Multi-Factor Authentication (MFA): MFA requires two or more verification steps to access sensitive systems, combining something the user knows (password) with something they have (a smartphone app or hardware token) or something they are (biometric). MFA is especially critical for remote access, email accounts containing ePHI, and cloud services. Even if a password is compromised, MFA dramatically reduces the risk of unauthorized access.
- Role-Based Access Control: Staff should only have access to the minimum necessary ePHI required to perform their job functions. A front desk scheduler does not need access to clinical treatment notes, just as a hygienist may not need billing information [64].

Encryption

Encryption is the most reliable method to protect ePHI from unauthorized access. While technically "addressable" under HIPAA (meaning practices can adopt an alternative if equally effective), encryption has become the de facto standard [65].

- Data at Rest: All data stored on computers, servers, mobile devices, and external drives should be encrypted. This protects information if devices are lost or stolen.
- Data in Transit: Emails containing ePHI, file transfers, and communications between offices must be encrypted. Unencrypted email is not permitted for transmitting PHI, nor is standard SMS text messaging.

Network security

Protecting the practice's network perimeter prevents unauthorized entry and contains potential breaches.

- Firewalls: Robust firewalls act as the first line of defense, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.
- Software Updates and Patch Management: All software including operating systems, practice management software, and imaging applications must be kept current with the latest security patches. Outdated, unsupported systems (such as Windows 7) create known vulnerabilities that attackers actively exploit [66].
- Secure Wi-Fi: Practice Wi-Fi networks should be secured with strong encryption (WPA2 or WPA3) and hidden from public view. Guest networks should be completely separate from the network handling ePHI.
- Endpoint Detection and Response (EDR): Beyond traditional antivirus, EDR solutions continuously monitor devices (computers, servers, imaging systems) for suspicious activity, enabling rapid detection and response to threats [67].

Data backup and recovery

Regular, tested backups are the ultimate safety net against ransomware and data loss.

- The 3-2-1 Rule: Maintain at least three copies of data, on two different media types, with one copy stored off-site (preferably in encrypted cloud storage).
- Automated Backups: Backups should be scheduled automatically to ensure consistency and eliminate human error.
- Regular Testing: Backups are worthless if they cannot be restored. Practices must regularly test their restoration process to ensure data can be recovered quickly in an emergency.

The human factor: Training and culture

Technology alone cannot secure a dental practice. The human element remains the weakest link, with an estimated 70% of successful cyberattacks traced to human error. A robust cybersecurity program must therefore prioritize workforce training and cultivate a culture of security awareness.

HIPAA training requirements

HIPAA explicitly requires covered entities to train all workforce members on privacy and security policies and procedures. This applies to everyone dentists, hygienists, assistants, front desk staff, billing personnel, and even part-time or temporary workers. Training must be provided:

- To all new hires within a reasonable period (typically 30 days).
- Annually as refresher training for all staff.
- Whenever material changes in policies or procedures occur.

Key training content

Effective training goes beyond reciting regulations. It must be practical, relatable, and specific to the dental environment.

- Recognizing Phishing: Staff must learn to identify suspicious emails, including those generated by AI, and know how to report them. They should verify unusual requests for information or money through a separate communication channel.
- Protecting PHI in Daily Tasks: Training should address real-world scenarios: discussing treatment plans discreetly at the front desk, managing patient records in open operatories, handling appointment reminders without disclosing details, and properly disposing of paper records.
- Secure Device Use: Staff should understand the importance of locking workstations when away, using privacy screens, and never sharing passwords.
- Incident Reporting: Every team member must know how to recognize and report a potential security incident immediately, without fear of reprisal [68].

Building a culture of cybersecurity

Training is most effective when it is part of a broader organizational culture that values security.

- Designate Champions: Appoint a HIPAA Privacy Officer and Security Officer who serve as go-to experts for questions and concerns.
- Ongoing Reinforcement: Use posters, team meeting reminders, and spot checks to keep security top-of-mind throughout the year, not just during annual training.
- Encourage Open Communication: Create an environment where employees feel comfortable reporting mistakes or asking questions without fear of blame.

Documentation is essential

If it wasn't documented, it didn't happen. Practices must maintain meticulous records of all training sessions, including dates, attendees, and topics covered. Employee signed acknowledgments must be retained—typically for at least six years—to demonstrate compliance during an audit or investigation.

Administrative safeguards: Policies and risk management

Behind every technical control and training program must lie a foundation of sound administrative practices [69].

The HIPAA Risk Assessment

The HIPAA Security Rule requires every covered entity to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. This is not a one-time task; it must be updated annually and whenever significant changes occur, such as new software implementation, facility changes, or changes in staff. A proper risk assessment identifies where PHI resides, how it is accessed, who has access, and the security of those systems.

Written policies and procedures

Practices must maintain written HIPAA policies and procedures that are tailored to their specific operations. These documents should address all aspects of privacy and security, from workstation use to breach response.

Business associate agreements (BAAs)

Dental practices rely heavily on third-party vendors—IT providers, billing services, cloud software companies, and even finance companies offering patient payment plans. These are Business Associates under HIPAA, and practices must have signed BAAs with each vendor that may encounter PHI. The BAA contractually obligates the vendor to protect the data and provides liability protection for the practice.

Incident response plan

Every practice must have a documented, tested incident response plan that outlines exactly what steps to take when a breach occurs: who to notify, how to contain the incident, how to preserve evidence, how to communicate with affected patients, and how to recover operations.

Conclusion: The path forward

Cybersecurity in the modern dental office is not merely an IT issue it is a patient safety issue, a regulatory compliance issue, and a business continuity issue. The digital transformation that has brought tremendous benefits to dentistry has also introduced profound risks that must be managed with intention and expertise.

The threats are real and growing. Cybercriminals view dental practices as attractive, vulnerable targets, and they are leveraging increasingly sophisticated tools, including artificial intelligence, to enhance their attacks. Meanwhile, regulators are actively enforcing compliance, with substantial fines and legal actions becoming more common.

Yet, as daunting as the landscape may appear, effective protection is achievable. It does not require becoming a security expert overnight. It does require commitment: commitment to conducting regular risk assessments, to implementing foundational technical safeguards like MFA and encryption, to training staff consistently, and to maintaining diligent documentation.

Most importantly, it requires a shift in mindset from viewing cybersecurity as an optional burden to recognizing it as an integral component of quality patient care. Patients entrust dental professionals not only with their oral health but with their most personal information. Protecting that trust is both a legal obligation and an ethical imperative.

References

1. Panahi DO, Dadkhah DS. La IA en la odontología moderna. 2025.
2. Panahi O, Eslamlou SF, Jabbarzadeh M. Digitale Zahnmedizin und künstliche Intelligenz. 2025.
3. Panahi O, Esmaili DF, Kargarnezhad DS. Intelligenza artificiale in odontoiatria. SAPIENZA Publishing; 2024.
4. Panahi DO, Dadkhah DS. L'IA dans la dentisterie modern. 2025.
5. Panahi O, Eslamlou SF, Jabbarzadeh M. Stomatologia cyfrowa i sztuczna inteligencja. 2025.
6. Panahi O, Eslamlou SF, Jabbarzadeh M. Odontoiatria digitale e intelligenza artificiale. 2025.
7. Panahi O, Eslamlou SF, Jabbarzadeh M. Dentisterie numérique et intelligence artificielle. 2025.
8. Panahi DO, Eslamlou DSF. Le péridontium: Structure, fonction et gestion clinique. 2025.
9. Panahi DO, Dadkhah DS. L'intelligenza artificiale nell'odontoiatria moderna. 2025.
10. Panahi O. Células madre de la pulpa dental. Ediciones Nuestro Conocimiento; 2021.
11. Panahi DO, Dadkhah DS. A IA na medicina dentária moderna. 2025.
12. Panahi DO. Cellule staminali della polpa dentaria. 2021.
13. Thamson K, Panahi O. Challenges and opportunities for implementing AI in clinical trials. J Bio Adv Sci Res. 2025; 1: 1-08.
14. Thamson K, Panahi O. Ethical considerations and future directions of AI in dental healthcare. J Bio Adv Sci Res. 2025.
15. Thamson K, Panahi O. Bridging the gap: AI, data science, and evidence-based dentistry. J Bio Adv Sci Res. 2025.
16. Thamson K, Panahi O. Bridging the gap: AI as a collaborative tool between clinicians and researchers. J Bio Adv Sci Res. 2025.
17. Panahi O, Dadkhah S. Transforming dental care: A comprehensive review of AI technologies. J Stoma Dent Res. 2025; 3: 1-5..
18. Panahi O. Predictive health in communities: Leveraging AI for early intervention and prevention. Ann Community Med Prim Health Care. 2025; 3: 1028.
19. Gholizadeh M, Panahi O. Research system in health management information systems. Sciencia Scripts Publishing. 2021.
20. Gholizadeh M, Panahi O. Sistema issledovaniy v informatsionnykh sistemakh upravleniya zdravookhraneniem. Sciencia Scripts Publishing. 2021.
21. Panahi O, Esmaili F, Kargarnezhad S. L'intelligence artificielle dans l'odontologie. Edition Notre Savoir Publishing; 2024.
22. Zarei S, Panahi DO, NimaBahador D. Antibacterial activity of aqueous extract of eucalyptus camaldulensis against Vibrio harveyi and Vibrio alginolyticus. Saarbrucken: LAP. 2019.
23. Panahi O, et al. Robotics in implant dentistry: Current status and future prospects. Sci Arch Dent Sci. 2025; 7: 55-60.
24. Samira MRS, Zarei P, Omid D. Eucalyptus camaldulensis extract as a preventive to the vibriosis. Scholars' Press; 2019.
25. Panahi O. Empowering dental public health: Leveraging artificial intelligence for improved oral healthcare access and outcomes. JOJ Pub Health. 2024; 9: 555754.
26. Panahi O. Sistema issledovaniy v informatsionnykh sistemakh upravleniya zdravookhraneniem. Sciencia Scripts Publishing 2021.
27. Panahi O. Smart implants: Integrating sensors and data analytics for enhanced patient care. Dental. 2025; 7: 22.
28. Panahi O. Forging a healthier future through responsible AI in families and communities. Arch Community Fam Med. 2025; 8: 21-30.
29. Omid P, Fatmanur KC. Nano technology. Regenerative Medicine and Tissue Bioengineering. 2023.
30. Panahi DO, Esmaili DF, Kargarnezhad DS. L'intelligence artificielle dans l'odontologie. Edition Notre Savoir Publishing. 2024.
31. Panahi O, Eslamlou SF. Periodontium: Structure, function and clinical management.
32. Panahi O. Health in the age of AI: A family and community focus. Arch Community Fam Med. 2025; 8: 11-20.
33. Panahi O, Shahbazpour Z. Healthcare reimagined: AI and the future of clinical practice. Am J Biomed Sci Res. 2025; 27: AJBSR. MS.ID.003617.
34. Panahi O, Dadkhah S. AI in modern dentistry. 2025.
35. Panahi O. Robotic surgery powered by AI: Precision and automation in the operating room. SunText Rev Med Clin Res. 2025; 6: 225.
36. Panahi O. Smart materials and sensors: Integrating technology into dental restorations for real-time monitoring. J Dent Oral Health. 2025; 2.
37. Panahi DU. AD HOC-Netze: Anwendungen, Herausforderungen, zukünftige Wege. Verlag Unser Wissen. 2025.
38. Koyuncu B, Ugur B, Panahi P. Indoor location determination by using RFIDs. Int J Mobile Adhoc Netw. 2013; 3: 7-11.
39. Panahi U. Redes AD HOC: Aplicações, desafios, direcções futuras. Edições Nosso Conhecimento. 2025.
40. Panahi P, Dehghan M. Multipath video transmission over ad hoc networks using layer coding and video caches. In: Proc ICEE 2008 16th Iranian Conf Electrical Engineering. 2008: 50-55.
41. Panahi DU. HOC A networks: Applications, challenges, future directions. Scholars Press. 2025.
42. Panahi O, Esmaili F, Kargarnezhad S. Artificial intelligence in dentistry. Scholars Press Publishing. 2024.
43. Omid P. Relevance between gingival hyperplasia and leukemia. Int J Acad Res. 2011; 3: 493-499.
44. Panahi O. Secure IoT for healthcare. Eur J Innov Stud Sustain. 2025; 1: 1-5.
45. Panahi O. Deep learning in diagnostics. J Med Discov. 2025; 2.
46. Omid P. Artificial intelligence in oral implantology, its applications, impact and challenges. Adv Dent Oral Health. 2024; 17: 555966.
47. Panahi O. Teledentistry: Expanding access to oral healthcare. J Dent Sci Res Rev Rep. 2024: SRC/JDSR-203.
48. Omid P. Empowering dental public health: Leveraging artificial intelligence for improved oral healthcare access and outcomes. JOJ Pub Health. 2024; 9: 555754.
49. Thamson K, Panahi O. Bridging the gap: AI as a collaborative tool between clinicians and researchers. J Bio Adv Sci Res. 2025; 1: 1-8.

50. Panahi O. Algorithmic medicine. J Med Discov. 2025; 2.

51. Panahi O. The future of healthcare: AI, public health and the digital revolution. MediClin Case Rep J. 2025; 3: 763-766.

52. Thamson K, Panahi O. Challenges and opportunities for implementing AI in clinical trials. J Bio Adv Sci Res. 2025; 1: 1-8.

53. Thamson K, Panahi O. Ethical considerations and future directions of AI in dental healthcare. J Bio Adv Sci Res. 2025; 1: 1-7.

54. Thamson K, Panahi O. Bridging the gap: AI, data science, and evidence-based dentistry. J Bio Adv Sci Res. 2025; 1: 1-13.

55. Panahi O, Ezzati A. AI in dental medicine: Current applications and future directions. Open Access J Clin Images. 2025; 2: 1-5.

56. Panahi O, Borhani S. Odontoiatria intelligente: Una guida completa all'intelligenza artificiale e alla robotica. 2026.

57. Panahi O, Borhani S. Inteligentna stomatologia: Kompleksowy przewodnik po sztucznej inteligencji i robotyce. 2026.

58. Panahi O, Borhani S. Medicina dentária inteligente: Um guia abrangente de IA e robótica. OmniScriptum Publishing Group. 2026.

59. Panahi O, Borhani S. La dentisterie intelligente: Un guide complet de l'IA et de la robotique. OmniScriptum Publishing Group. 2026.

60. Panahi O, Borhani S. Odontología inteligente: Una guía completa sobre IA y robótica. OmniScriptum Publishing Group. 2026.

61. Panahi O, Borhani S. Intelligente Zahnmedizin: Ein umfassender Leitfaden zu KI und Robotik. OmniScriptum Publishing Group. 2026.

62. Panahi O, Borhani S. Intelligent dentistry: A comprehensive guide to AI and robotics. 2026.

63. Panahi O. Predictive health in communities: Leveraging AI for early intervention and prevention. Ann Community Med Prim Health Care. 2025; 3: 1027.

64. Panahi O, Esmaili F, Kargarnezhad S. Inteligencia artificial en odontología. Mento Publishing. 2024.

65. Panahi O, Esmaili F, Kargarnezhad S. Künstliche Intelligenz in der Zahnmedizin. Unser Wissen Publishing; 2024.

66. Panahi DO. Stem cells of dental pulp.

67. Panahi O, Arab MS, Tamson KM. Gingival enlargement and relevance with leukemia. Int J Acad Res. 2011.

68. Panahi O, Eslamlou SF, Jabbarzadeh M. Odontología digital e inteligencia artificial. 2025.

69. Panahi DO, Dadkhah DS. Sztuczna inteligencja w nowoczesnej stomatologii. 2025.