URF PUBLISHERS
connect with research world

International Journal of Aging and Geriatric Medicine

https://urfpublishers.com/journal/gerontology-geriatric-medicine

Vol: 2 & Iss: 2

Review

Digital Dentistry in Geriatric Patients: Clinical and Legal Perspectives

Maria Teresa Lo Conte[1,2]* and Salvatore Grieco[3]

[1]Junior Researcher Research Centre of European Private Law (ReCEPL) Suor Orsola Benincasa University, Naples, Italy

[2]Ph.D.(s) Tor Vergata University of Rome, Rome, Italy

[3]Dentist Student international Level II Master's degree in Global Aesthetic Medicine, Naples, Italy

Citation: Lo Conte MT, Grieco S. Digital Dentistry in Geriatric Patients: Clinical and Legal Perspectives. *Int J Aging Geriatr Med 2026*, 2(2), 155-160.

Received: 08 April, 2026; **Accepted:** 23 April, 2026; **Published:** 27 April, 2026

***Corresponding author:** Maria Teresa Lo Conte, Research Centre of European Private Law (ReCEPL) Suor Orsola Benincasa University, Naples, Italy / Tor Vergata University of Rome, Rome, Italy

ABSTRACT

The rapid aging of the global population, combined with the digital transformation of dental practice, is reshaping the management of clinical information in contemporary dentistry. In particular, geriatric dentistry is increasingly characterized by the production and processing of complex digital data, including radiographic imaging, intraoral scans, and three-dimensional models, which extend beyond traditional clinical records in both volume and identifiability.

Adopting an interdisciplinary approach (medical and legal), this review explores the evolving nature of dental data as a sensitive biometric resource in the context of geriatric patients. Particular focus is placed on the intersection between digital dentistry and data protection frameworks, especially the General Data Protection Regulation (GDPR), which enforces rigorous standards for the processing, storage, and sharing of health-related data. The European Framework, including the Artificial Intelligence Act (AI Act) and the European Health Data Space (EHDS), is also analysed. Current evidence highlights how the integration of digital technologies, cloud-based systems, and artificial intelligence can amplify both the clinical potential and the legal risks associated with data management. These challenges are further exacerbated in elderly patients, whose vulnerability raises critical issues regarding informed consent and data governance.

This paper synthesises existing literature to emphasise the need for a balanced approach that integrates technological innovation with robust legal safeguards to promote a more secure, transparent and patient-centred model of care in the digital era.

Keywords: Digital dentistry, Dental care, Elderly patients, Biometrics data, GDPR, AI Act EHDS

1. Introduction

The aging of the global population represents one of the most significant challenges for contemporary healthcare systems, leading to a substantial increase in the number of elderly patients requiring complex and continuous dental care. In this context, geriatric dentistry plays a crucial role in maintaining oral health, masticatory function, and overall quality of life. However, the management of elderly patients is often complicated by the

presence of comorbidities, polypharmacy, and cognitive decline, which may impair decision-making capacity and the validity of informed consent[1].

In addition, frailty and functional decline have been shown to significantly impact oral health status and treatment needs in older adults, further emphasizing the importance of continuous monitoring and personalized care strategies[2]. This need for continuous monitoring aligns closely with the capabilities offered by digital dentistry technologies.

Numerous recent studies have highlighted how dentistry has simultaneously undergone a profound digital transformation[3,4]. The widespread adoption of technologies such as intraoral scanners, three-dimensional imaging, electronic health records, and digital platforms has significantly reshaped clinical practice. Consequently, dental data can no longer be considered merely as traditional clinical notes, but rather as complex, high-resolution digital information that is potentially identifiable and easily shareable[5,6].

This increasing digitalization raises critical issues regarding the protection of personal data. Within the European context, the General Data Protection Regulation (GDPR) strictly regulates the processing of health-related data, classified as special categories of personal data[7,8]. In dentistry, such data include not only clinical and anamnestic information but also radiographic images, photographs, and three-dimensional models obtained through intraoral scanning, which may exhibit unique features and raise questions about their potential classification as biometric data[4,5].

These challenges become even more relevant in geriatric patients[1], who represent a particularly vulnerable population from both clinical and legal perspectives. Difficulties in providing fully informed consent, combined with the growing circulation of data through digital systems, cloud platforms, and artificial intelligence tools, increase the risk of misuse, unauthorized access, and breaches of confidentiality[1,3,8].

In light of these considerations, this review aims to critically analyze dental data in its digital dimension as sensitive biometric information within the field of geriatric dentistry. The objective is to examine the ethical and legal implications arising from the application of the GDPR, the AI Act, the EHDS and the MDR, in order to identify strategies for a compliant and responsible clinical practice in the digital era.

2. Digital Dentistry and Data Generation

The field of dentistry has undergone a profound digital transformation over the past decade, reshaping diagnostic and therapeutic workflows. In geriatric dentistry, this evolution is particularly relevant, as elderly patients often require precise, continuous monitoring and treatment planning[3,4].

Technologies commonly used include intraoral scanners, three-dimensional imaging, CBCT, and CAD/CAM systems[3,4,5]. Intraoral scanners produce high-resolution 3D models of the oral cavity, capturing details such as tooth morphology, soft tissue contours, and occlusal relationships. CBCT provides volumetric imaging of the maxillofacial region, enabling accurate assessment of bone quality and anatomical structures. CAD/CAM systems generate digital models for prosthetic planning, surgical guides, and restorative design. Together, these technologies produce complex datasets that go well beyond traditional clinical notes[5,6].

Types of data generated include:

- 3D surface models of teeth and soft tissues.
- Volumetric CBCT images.
- CAD/CAM restorative plans.
- Annotated digital records integrated into electronic health systems.
- Longitudinal datasets obtained from repeated scans over time[6].

Such data are inherently high-resolution, potentially identifiable, and easily shareable. For example, an intraoral scan can serve both clinical purposes (diagnosis, treatment planning) and research or telemedicine applications, yet it may contain unique patterns that could identify an individual patient[3,5].

Data circulation is facilitated by cloud-based storage and telemedicine platforms, enabling real-time collaboration among clinicians, specialists, and even researchers[6,7].

Artificial intelligence algorithms can process these multidimensional datasets to support diagnostic accuracy, predictive modeling, and treatment optimization[3].

While these advances improve clinical precision, they also introduce vulnerabilities, including unauthorized access, potential misuse, and risks of data loss or corruption[3,8].

From a clinical perspective, digital tools are increasingly applied in geriatric populations. For instance, intraoral scanners have been successfully used in nursing home residents to perform diagnostic assessments and support telemedicine-based care, demonstrating good accuracy for structural conditions such as missing teeth and restorations[6].

Moreover, longitudinal approaches have long been employed in elderly cohorts to monitor oral health changes over time, including tooth loss and periapical pathology, highlighting the importance of repeated assessments in geriatric dentistry[10].

In digital dentistry, repeated intraoral scans can be superimposed to enable highly precise longitudinal monitoring of dental structures, allowing clinicians to detect subtle morphological changes and disease progression over time[11].

3. Nature and Circulation of Dental Data

3.1. Clinical and technological perspective

The progressive digitalization of dentistry has led to an exponential increase in the volume, complexity, and granularity of dental data. In geriatric dentistry, digital datasets generated through intraoral scanners, CBCT, and CAD/CAM systems are high-resolution, multimodal, and longitudinally reproducible. These datasets support diagnosis, treatment planning, and long-term monitoring of dental structures, enabling clinicians to detect subtle morphological changes, tooth loss, and disease progression over time[3,5,10].

The circulation of dental data is increasingly facilitated by cloud-based infrastructures and integrated digital platforms, allowing real-time sharing among clinicians, specialists, laboratories, and researchers. While this interconnected environment enhances clinical efficiency and interdisciplinary collaboration, it may reduce direct control over data access and management[6,7].

Artificial intelligence (AI) further extends potential applications by enabling predictive modeling, automated diagnostic support, and personalized treatment optimization. However, secondary uses of data beyond their original clinical purpose raise concerns regarding data governance, transparency, and clinical responsibility[3].

Recent advances in prosthodontics demonstrate how predictive analytics and personalized digital workflows can transform clinical datasets into individualized treatment strategies, enhancing both diagnostic precision and patient-centered care[12]. This exemplifies how digital dentistry in geriatric populations can leverage high-resolution data not only for routine monitoring but also to anticipate clinical outcomes and optimize personalized interventions[11].

Collectively, these characteristics underline a fundamental duality: dental data are highly valuable resources but also carry inherent risks, particularly in elderly populations, where prolonged monitoring and sensitive information require careful handling[7,8].

3.2. Legal perspective

3.2.1. Data protection in the dental sector through the use of digital tools in light of EU legislation: The General Data Protection Regulation (EU) 2016/679, which came into force on 25 May 2018, constitutes the fundamental regulatory framework for the protection of personal data within the European Union (and, given the Brussels effect under Article 3 of the GDPR, also beyond the Union's borders), establishing a regulatory framework of particular relevance to the healthcare sector. Understanding its fundamental provisions is essential for any assessment of legal risks, ethical challenges and the vulnerabilities of data subjects/patients, given that the adoption of medical devices such as intraoral scanners in clinical dentistry generates three-dimensional digital models - personal data - which must comply with the provisions of the GDPR[13].

Central to this discussion is the concept of 'special categories of personal data' within the meaning of Article 9(1), which encompasses both 'data concerning health' within the meaning of Article 4(15) of the GDPR and 'biometric data for the purpose of uniquely identifying a natural person' within the meaning of Article 4(14) of the GDPR: the processing of which is prohibited in principle[14], unless specific conditions for lawfulness set out in Article 9(2) of the GDPR are met. This dual classification is based on a clear premise: the dental morphology acquired by medical devices enables individual identification with accuracy rates that can reach 100%[15-17] , meaning that the relevant data is fully classified as personal data insofar as it constitutes information relating to an identifiable natural person within the meaning of Article 4(1) of the GDPR.

The definition of health data[18], set out in Article 4(15) of the GDPR, is deliberately broad: it includes all personal data relating to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about their health status. Recital 35 of the GDPR further specifies that this includes data derived from medical examinations or from 'a medical device', a formulation that can include intraoral scanners classified under the EU Medical Devices Regulation 2017/745[19]. The European Data Protection Board, in its Guidelines 03/2020 on the processing of health data for scientific research[20], confirmed that health data warrant enhanced protection precisely because their misuse can lead to discrimination, social stigma and material harm to individuals.

As mentioned, the processing of these special categories is prohibited in principle, except for a closed list of exceptions set out in Article 9(2), of which the most relevant to digital dentistry are: the patient's explicit consent, freely given, specific, informed and unambiguous, in accordance with Article 9(2)(a); the necessity for the purposes of preventive or occupational medicine, medical diagnosis or the provision of healthcare, in accordance with Article 9(2)(h), in conjunction with the obligations of professional secrecy referred to in Article 9(3); and the necessity for scientific research purposes, in accordance with Article 9(2)(j), subject to the safeguards provided for in Article 89(1) of the GDPR, including pseudonymisation and data minimisation.

The processing of data must comply with the six principles set out in Article 5(1) of the GDPR, each of which has specific operational implications for the digital dental workflow. The principle of lawfulness, fairness and transparency (Article 5(1)(a)) requires that patients be informed, in clear and plain language, of the identity of the data controller, the purposes of the processing, the legal basis on which it is based, any recipients or categories of recipients, and the existence of their rights, including the right of access under Article 15 of the GDPR, the right to rectification pursuant to Article 16 of the GDPR, the right to erasure pursuant to Article 17 of the GDPR, and the right to data portability pursuant to Article 20 of the GDPR. As noted in the legal literature[21], the obligation of transparency referred to in Recital 58 requires that the information be adapted to the specific capacities of the data subject, a requirement of particular relevance for geriatric patients.

It should also be noted that the principle of purpose limitation (Article 5(1)(b) of the GDPR) prohibits the reuse of scan data for purposes incompatible with those for which it was originally collected, meaning that data collected for clinical processing cannot subsequently be used for training AI models, commercial analysis or research without a new legal basis. The principle of data minimisation (Article 5(1)(c) of the GDPR) requires that only data that is adequate, relevant and limited to what is necessary in relation to the purposes of the processing be collected. The principle of accuracy (Article 5(1)(d) of the GDPR) imposes an obligation to ensure that personal data is kept up to date, which, in the dental context, extends to the correlation between scan data and the patient's evolving oral health status. The principle of storage limitation (Article 5(1)(e) of the GDPR) requires that data be stored in an identifiable form for no longer than is necessary for the stated purposes, raising unresolved issues regarding the retention periods of 3D scan files on cloud-based platforms, where the persistence of data may exceed clinical necessity. Finally, the principle of integrity and confidentiality (Article 5(1)(f) of the GDPR) requires that personal data be processed in a manner that ensures appropriate protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

This latter principle is operationalised by Article 32 of the GDPR, which requires the controller and the processor to implement measures ensuring a level of security appropriate

to the risk, explicitly citing pseudonymisation, encryption, the ability to ensure the ongoing confidentiality of processing systems, the ability to restore the availability of data in a timely manner, and the periodic testing and evaluation of the effectiveness of security measures.

Furthermore, the regulatory landscape has continued to evolve: the recent Regulation (EU) 2025/327 on the European Health Data Space (EHDS)[22,23] has established a framework dedicated to both the primary[24] and secondary use of electronic health data, including images relevant to the dental sector. Under the EHDS, such data[25] is classified as 'personal electronic health data' within the meaning of Article 2(2)(a) EHDS, and the healthcare professional (i.e. the person carrying out activities in the healthcare sector[26]) has free access to the relevant and necessary personal electronic health data of natural persons under their care through the access services for healthcare professionals (i.e. the LaMiaSalute@EU platform pursuant to Article 23 EHDS) (Article 11(2) EHDS), bearing in mind also that, where necessary to safeguard the vital interests of the data subject, the healthcare professional may be granted access to the electronic health data subject to the access restriction imposed by the patient (Article 11(5) EHDS).

It should also be noted that when operations are carried out by devices implemented using AI[27], the provisions of the AI Act (Regulation (EU) 2024/1689)[28] also apply, which - by providing for a risk-based approach – classifies AI systems on the basis of their intrinsic risk[29]. Among these, artificial intelligence systems that fall within the definition of a device under Regulation (EU) 2017/745 (MDR)[16] are considered, for example, to be high-risk systems. This definition also includes software that the manufacturer intends to be used on humans, either autonomously or in combination with other devices, for one or more specific medical purposes. In this case, doctors are classified as deployers (i.e. professional users of AI tools) and are subject to certain obligations laid down by the AI Act.

At the same time, when scan data originally collected for clinical treatment is subsequently reused for training artificial intelligence[30] a separate legal basis is required. Also the French data protection authority (CNIL) has clarified that the reuse of health data for the development of AI models constitutes a change of purpose that requires independent justification; in this specific case, reference may be made either to the legal basis of the patient's explicit consent pursuant to Article 9(2)(a) of the GDPR, or, in the case of AI systems adopted by the National Health Service (NHS), to the ground of substantial public interest pursuant to Article 9(2)(g) of the GDPR.

The interplay between the GDPR, the EHDS, the MDR and the AI Act defines the multi-layered regulatory framework within which digital dentistry professionals must operate: a framework in which compliance is not a static outcome, but a continuous and dynamic obligation requiring constant legal and technical vigilance.

3.2.2. Risks and liabilities relating to digital dentistry data: From the perspective of liability, whilst it is beyond dispute that the dentist acts as the data controller (i.e. the entity that determines certain key aspects of the processing, namely the reasons and purposes thereof, pursuant to Articles 4(1)(7), 24 and 25 of the GDPR)[31], it is the role of data processor that raises the most concerns: CAD/CAM centres and providers of dedicated cloud platforms (such as 3Shape and Dentsply Sirona) inevitably act as data processors since, being a separate entity from the controller, they process personal data on the controller's behalf (Articles 4(1)(8) and 28 of the GDPR)[32]. However, this latter role entails significant issues, as the controller/processor relationship is not particularly straightforward; on the contrary, suppliers' transparency regarding data security measures and cloud hosting locations remains poor, exposing professional controllers to risks that they could, in fact, neither foresee nor control.

The GDPR does, in fact, impose genuine obligations of proactive responsibility: one example is Article 25 of the GDPR, which requires data protection by design and by default, obliging data controllers to implement appropriate technical and organisational measures when determining the means of processing and at the time of processing itself. In the present case, this is particularly significant given that part of the legal literature[33] has questioned the function of dental images, noting also that they entail a high risk of re-identification, rendering pseudonymisation techniques alone insufficient to protect patients' privacy. At the same time, the EDPB's Guidelines 4/2019 on Article 25[34] have clarified that this obligation of privacy by design and by default extends to the design of products and services, directly involving scanner manufacturers and their proprietary software ecosystems in the compliance architecture.

Furthermore, the obligation to carry out a data protection impact assessment pursuant to Article 35 of the GDPR remains in force prior to processing operations that could pose a high risk to the rights and freedoms of natural persons. Digital devices meets at least three of the nine high-risk criteria identified in the Article 29 Working Party's DPIA Guidelines[35], which require a DPIA to be carried out when such tools are adopted: processing of sensitive data (biometric and health data), data relating to vulnerable individuals (patients, particularly elderly patients) and the use of innovative technologies (3D scanning, cloud-based storage and AI-assisted analysis). It should be noted that the DPIA must contain, as a minimum, a systematic description of the envisaged processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing, an assessment of the risks to the rights and freedoms of data subjects, and the measures envisaged to address such risks (Article 35(7) GDPR). Where the DPIA indicates that the processing would result in a high risk in the absence of mitigation measures, the controller must consult the supervisory authority in accordance with Article 36 of the GDPR before proceeding with the processing in question.

These obligations are not abstract: in the event of a data breach (a security incident leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data), the GDPR imposes strict obligations to notify breaches in accordance with Articles 33 and 34. The data controller must notify the competent supervisory authority without undue delay and, where possible, within 72 hours of becoming aware of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons (Article 33(1) GDPR); where the breach is likely to result in a high risk, the controller must also communicate the breach to the data subjects without undue delay (Article 34(1) GDPR). The dental sector is no stranger to this; indeed, the Absolute Dental

cyberattack in May 2025 affected approximately 1.22 million patients across Nevada.

Finally, the consequences of non-compliance with the GDPR are severe[36]: Article 83(5) provides for administrative fines of up to €20 million or 4% of total global annual turnover, whichever is higher, for breaches of the fundamental principles of processing, the conditions for consent or the rights of data subjects. The Westend Dental case, in which a dental group was fined $350.000 for misrepresenting the nature and scope of a ransomware attack, demonstrates that supervisory authorities are increasingly willing to penalise not only the breach itself, but also the failure to communicate it transparently.

Geriatric patients occupy a position of heightened vulnerability within the digital dental data ecosystem. This vulnerability is in fact decision-making, informational and structural in nature, yet current legal frameworks address it only indirectly. Furthermore, Recital 75 of the GDPR is the only provision that refers to 'vulnerable natural persons'[37], and the Article 29 Working Party has explicitly identified the elderly, vulnerable patients and people with mental health conditions as groups requiring greater protection[38].

4. Informed Consent in Elderly Patients

Elderly patients often present with comorbidities, polypharmacy, and cognitive or functional decline, which can significantly affect their capacity to make informed decisions about dental care[1,2]. Frailty is particularly associated with diminished cognitive reserve and reduced ability to process complex information, making standard consent procedures insufficient in many cases[2].

In clinical practice, these challenges translate into several specific considerations:

- **Assessment of decision-making capacity:** Clinicians must evaluate whether the patient can understand proposed procedures, weigh risks and benefits, and communicate a clear choice.
- **Enhanced communication strategies:** Use simplified language, visual aids, and repeated explanations to ensure comprehension.
- **Family or caregiver involvement:** When cognitive limitations exist, involve legal representatives or caregivers to support patient autonomy while ensuring safety.
- **Complexity of digital data:** Digital outputs - including 3D visualizations from intraoral scanners, CBCT, and digital treatment plans - may be difficult for patients to interpret without guidance. These tools can improve understanding if effectively communicated but may also overwhelm frail patients or inadvertently create misunderstandings about procedures[3,4].

In geriatric dentistry, clinicians carry a critical responsibility: ensuring that informed consent is a patient-centered process, adapted to the cognitive and functional abilities of the elderly. While digital tools enhance diagnostic precision and treatment planning, they require careful mediation by the clinician to translate complex data into accessible, actionable information.

5. Conclusion

We can state that innovations in this field represent not only a technological evolution, but a profound paradigm shift that imposes new and rigorous responsibilities[39].

Within a complex regulatory framework, compliance with the GDPR and sector-specific rules is not a static requirement but a continuous process demanding ongoing assessments, advanced security measures, and a risk-oriented design approach.

At the same time, innovation shifts the focus both toward the development of reliable systems and the centrality of clinical judgment: dentists must ensure human oversight, communicate clearly about the use of AI, and maintain patient trust by explaining that technology acts as a "digital collaborator" rather than replacing professional expertise. The adoption of AI cannot be improvised either; staff must receive proper and accredited training to understand algorithmic limitations, avoid biases, and ensure cybersecurity, in line with AI literacy requirements under Article 4 of the AI Act.

In this context, safeguarding digital devices data and complying with the European regulatory framework become essential conditions for a dental practice that is safe, transparent, and genuinely patient-centred.

6. Declarations

6.1. Ethics approval and consent to participate

This study was conducted in accordance with all applicable ethical standards.

6.2. Consent for publication

All participants provided informed consent for the publication of the collected data in anonymized and aggregated form.

6.3. Availability of data and materials

The materials used and analyzed during the current study are available from the corresponding author on reasonable request.

6.4. Competing interests

The authors declare that they have no competing interests related to the content of this manuscript.

6.5. Funding

This study received no external funding.

6.6. Authors' contributions

All authors made a substantial contribution to the conception, design, data collection, data analysis, drafting, or critical revision of the manuscript. Specifically:

- **Ph.D.(c) Maria Teresa Lo Conte:** conception, design, data collection, data analysis, drafting, critical revision of the manuscript. She writes §3.2, §3.2.1, §3.2.2, §5.
- **Dr. Salvatore Grieco:** design, data collection, data analysis, drafting. He writes §1, §2, §3.1, §4.

Translation activities were also carried out with the support of AI tools, followed by human revision to ensure accuracy, terminological consistency.

All authors read and approved the final version of the manuscript.

6.7. Acknowledgements

Not applicable.

7. References

1. Ivashkov Y, Van Norman GA. Informed consent and the ethical management of the older patient. Anesthesiol Clin, 2009;27(3): 569-580.
2. Niesten D, van Mourik K, van der Sanden W. The impact of frailty on oral care behaviour of older people: a qualitative study. BMC Oral Health, 2013;13: 61.
3. Schwendicke F, Samek W, Krois J. Artificial intelligence in dentistry: chances and challenges. J Dent Res, 2020;99(7): 769-774.
4. Schleyer TK, Spallek H, Leon R, et al. Dental informatics: a cornerstone of dental practice. J Am Dent Assoc, 2001;132(5): 605-613.
5. Mangano F, Gandolfi A, Luongo G, et al. Intraoral scanners in dentistry: a review of the current literature. BMC Oral Health, 2017;17(1): 149.
6. Sonnenschein SK, Kim TS, Spies AN, et al. Remote assessment of dental records by using intraoral scan-based digital 3D models in an elderly patient population: an exploratory study. Int J Comput Dent, 2025;28(1): 21-34.
7. Voigt P, Von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, 2017.
8. Kruse CS, Goswamy R, Raval Y, et al. Challenges and opportunities of big data in healthcare: a systematic review. JMIR Med Inform, 2016;4(4): 38.
9. Paglia V. Sanità digitale e persone anziane. Sanità digitale - Regolamento EHDS (UE 2025/327) sullo spazio europeo dei dati sanitari. I Uso dei dati e assetti organizzativi. Morace Pinelli A (eds), 2025: 513-516.
10. Øzhayat EB, Gotfredsen K, Elverdam B, et al. Patient-generated aspects in oral rehabilitation decision making. II. Comparison of an individual systematic interview method and the Oral Health Impact Profile. Int J Prosthodont, 2010;23(5): 421-428.
11. Díaz-Flores García V, Freire Y, David Fernández S, et al. Suárez Intraoral scanning for monitoring dental wear and its risk factors: a prospective study. Healthcare (Basel), 2024;12(11): 1069.
12. Pandey A. The digital frontier: personalization and predictive analytics in modern prosthodontics. Int J Aging Geriatr Med, 2026;2(1): 76-78.
13. Gatt L, Montanari R, Caggiano IA. Privacy and Consent. A Legal and UX&HMI Approach, University Suor Orsola Press, 2021.
14. Jedlińska A, Jedliński M. 3D intraoral scan and diagnostic plaster model under the General Data Protection Regulation - Legal protection. Journal of Forensic and Legal Medicine, 2023;95: 102503.
15. Chen Z, Wang Y, Zhang X, et al. Digital dental biometrics for human identification based on automated 3D point cloud feature extraction and registration. Bioengineering, 2024;11(9): 873.
16. Mou H, Li J, Chen X, Zhang J. 3D-3D dentition superimposition for individual identification: A study of an Eastern Chinese population. Forensic Science International, 2024;318: 111057.
17. Reesu GV, Woodsend B, Mânica S, et al. Automated Identification from Dental Data (AutoIDD): A new development in digital forensics. Forensic Science International, 2020;309: 110218.
18. Gaeta MC. The protection of health data in compliance with the GDPR. EJPLT, 2020;1: 158-160.
19. European Commission. Medical Devices Regulation. Regulation (EU) 2017/745, 2017.
20. European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 2020.
21. Piasecki J, Chen J. Complying with the GDPR when vulnerable people use smart devices. International Data Privacy Law, 2022;12(2): 113-131.
22. European Commission. European Health Data Space Regulation (EHDS). Regulation (EU) 2025/327, 2025.
23. Caggiano IA. Interessi e norme nell'ecosistema europeo dei dati sanitari: la tecnoregolazione abilitativa e le sfide per l'efficacia. Sanità digitale - Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari. I Uso dei dati e assetti organizzativi. Morace Pinelli A (eds), 2025: 19-34.
24. Solinas C. Diritto alla salute del paziente e uso primario dei dati sanitari elettronici personali. EJPLT, 2025;2.
25. Ricciuto V. Base giuridica del trattamento del dato sanitario nel contesto dell'EHDS. Sanità digitale -Regolamento EHDS (UE 2025/327) sullo spazio europeo dei dati sanitari. I Uso dei dati e assetti organizzativi. Morace Pinelli A (eds), 2025: 9-18.
26. Article 3(f) of Directive (EU) 2011/24.
27. Ramnarayan BK, Luke AM, Vidya MA, et al. Artificial intelligence-driven dentistry: A systematic review of ethical and legal challenges. International Journal of Dentistry, 2026;1: 1870800.
28. European Commission. Artificial Intelligence Act. Regulation (EU) 2024/1689, 2024.
29. Gatt L, Lo Conte MT, Mazzarella ME. L'ambito di applicazione, soggettivo e oggettivo, dell'AI Act. U Ruffolo (ed.) AI Act - La regolamentazione europea dell'Intelligenza artificiale. Luiss University Press, 2025: 49-89.
30. Waithira N, Mukaka M, Kestelyn E, et al. Data sharing and reuse in clinical research: Are we there yet? A cross-sectional study on progress, challenges and opportunities in LMICs. PLOS Glob Public Health, 2024;4(11): 0003392.
31. European Data Protection Board. Guidelines 7/2020 on the concepts of controller and processor in the GDPR, 2020: 3-4.
32. European Data Protection Board. Guidelines 7/2020 on the concepts of controller and processor in the GDPR, 2020: 3-4.
33. Rischke R, Schmitt RH, Prescher D, et al. Federated learning in dentistry: Chances and challenges. Journal of Dental Research, 2022;101(13): 1558-1564.
34. European Data Protection Board. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2020.
35. WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679.
36. Salanitro U. La tutela risarcitoria tra GDPR e EHDS: appunti per una ricerca. Sanità digitale - Regolamento EHDS (UE 2025/327) sullo spazio europeo dei dati sanitari. I Uso dei dati e assetti organizzativi. Morace Pinelli A (eds), 2025: 381-390.
37. Malgieri G. Vulnerability and data protection law. Oxford University Press, 2023.
38. Malgieri G, Niklas J. Vulnerable data subjects. Computer Law & Security Review, 2020;37: 105415.
39. Rokhshad R, Ducret M, Chaurasia A, et al. Ethical considerations on artificial intelligence in dentistry: A framework and checklist. Journal of Dentistry, 2023:135: 104593.