

Do patients consent to the use of their panoramic radiographs for AI training? Ethical and clinical implications in dentistry

¿Dan los pacientes su consentimiento para el uso de sus radiografías panorámicas en el entrenamiento de la inteligencia artificial? Implicaciones éticas y clínicas en odontología

Youris Samón Mayán¹, Ana Rodríguez Yanes¹, Yivelin Fernández Queija¹ , Lourdes Hernández Cuétara¹  , Arlin Castro Diaz²

¹Universidad de Ciencias Médicas de La Habana, Facultad de Ciencias Médicas “Miguel Enríquez”, Departamento de Estomatología General Integral. La Habana, Cuba.

²Universidad Iberoamericana. Santo Domingo, República Dominicana.

Cite as

Samón Mayán Y, Rodríguez Yanes A, Fernández Queija Y, Hernández Cuétara L, Castro Diaz A. Do patients consent to the use of their panoramic radiographs for AI training? Ethical and clinical implications in dentistry. SAP Artificial Intelligence in Dentistry. 2025; 1:35. <https://doi.org/10.62486/aid202535>.

Publication History

Submitted: 14-05-2025

Revised: 03-07-2025

Accepted: 01-10-2025

Published: 02-10-2025

Corresponding Author

Lourdes Hernández Cuétara 

ABSTRACT

Artificial intelligence has become increasingly integrated into dental practice, particularly through the use of imaging data such as panoramic radiographs and three-dimensional scans. This study examines the ethical, legal, and clinical implications associated with the use of dental patient data for artificial intelligence training. A central issue identified is the distinction between primary clinical use and secondary algorithmic use of patient data, which is not always explicitly addressed in current consent processes. The analysis highlights that traditional consent frameworks are often insufficient to account for large-scale data reuse, raising concerns regarding patient autonomy, transparency, and trust. In addition, the potential for reidentification of dental imaging data challenges assumptions related to anonymization and data security. Regulatory frameworks such as HIPAA, GDPR, and the EU AI Act provide partial guidance, but inconsistencies remain in their application to artificial intelligence workflows. From a clinical perspective, the use of non-representative datasets may introduce bias and affect diagnostic reliability across populations. The study emphasizes the need for improved data governance mechanisms, including dynamic consent models and privacy-preserving techniques. Overall, the findings indicate that the sustainable integration of artificial intelligence in dentistry depends on aligning technological development with ethical standards, legal compliance, and patient-centered care.

Keywords: Artificial Intelligence; Dentistry; Ethical Implications; Informed Consent; Data Privacy; Dental Radiographs.

RESUMEN

La inteligencia artificial se ha ido integrando cada vez más en la práctica odontológica, especialmente mediante el uso de datos de imagen, como radiografías panorámicas y escáneres tridimensionales. Este estudio examina las implicaciones éticas, legales y clínicas asociadas al uso de los datos de los pacientes odontológicos para el entrenamiento de la inteligencia artificial. Una cuestión central identificada es la distinción entre el uso clínico primario y el uso algorítmico secundario de los datos de los pacientes, que no siempre se aborda de forma explícita en los procesos de consentimiento actuales. El análisis pone de relieve que los marcos de consentimiento tradicionales suelen ser insuficientes para dar cuenta de la reutilización de datos a gran escala, lo que suscita inquietudes en relación con la autonomía del paciente, la transparencia y la confianza. Además, la posibilidad de reidentificar los datos de imágenes dentales pone en tela de juicio las suposiciones relacionadas con la anonimización y la seguridad de los datos. Los marcos normativos como la HIPAA, el RGPD y la Ley de IA de la UE ofrecen una orientación parcial, pero persisten las inconsistencias en su aplicación a los flujos de trabajo de inteligencia artificial. Desde una perspectiva clínica, el uso de conjuntos de datos no representativos puede introducir sesgos y afectar a la fiabilidad del diagnóstico en las poblaciones. El estudio hace hincapié en la necesidad de mejorar los mecanismos de gobernanza de datos, incluyendo modelos de consentimiento dinámicos y técnicas de preservación de la privacidad. En general, los resultados indican que la integración sostenible de la inteligencia artificial en la odontología depende de la alineación del desarrollo tecnológico con las normas éticas, el cumplimiento legal y la atención centrada en el paciente.

Palabras clave: Inteligencia Artificial; Odontología; Implicaciones Éticas; Consentimiento Informado; Privacidad de los Datos; Radiografías Dentales.

INTRODUCTION

The integration of artificial intelligence into dentistry has expanded rapidly, particularly through the use of imaging data such as panoramic radiographs, cone beam computed tomography, and intraoral scans. These technologies are being increasingly applied to diagnostic support, treatment planning, and risk prediction, and they rely on large datasets to achieve acceptable levels of performance. As a result, dental patient data have become a critical resource for the development and validation of machine learning models.

Despite these advances, the processes by which such data are collected, processed, and repurposed raise important ethical and legal questions. In routine clinical practice, radiographic images are obtained primarily for diagnostic purposes, with patient consent typically limited to immediate care. The subsequent use of these data for training artificial intelligence systems introduces a secondary function that is not always explicitly communicated or authorized. This distinction between clinical use and algorithmic reuse has become a central issue in the governance of health data.

The sensitivity of dental imaging further complicates this scenario. Panoramic radiographs and three-dimensional imaging modalities contain detailed anatomical information that may allow indirect identification, even in the absence of conventional identifiers. These characteristic challenges traditional assumptions regarding anonymization and highlights the need for more robust data protection strategies. Moreover, differences in regulatory frameworks across jurisdictions create uncertainty regarding acceptable practices, particularly in contexts involving data sharing or commercial applications.

Given these considerations, it is necessary to critically examine the implications of using dental patient data for artificial intelligence development. This paper aims to analyze the ethical, legal, and clinical dimensions of this practice, with a focus on informed consent, privacy risks, and the impact on trust in AI-assisted dentistry.

DEVELOPMENT

The Ethical Core: Autonomy and the Secondary-Use Problem

The central ethical tension is that patients consent to their data being collected for clinical care, not for AI training, a distinction that matters enormously. Traditional consent frameworks were not designed with retrospective, large-scale data mining in mind. A much-cited framework proposed by Larson et al. in *Radiology* (2020) argues that clinical data, once used for its primary purpose (patient diagnosis), should be treated as a form of public good with no further consent needed, provided that strict privacy safeguards and institutional oversight are maintained.⁽¹⁾

Krupinski's editorial in the same issue endorses the “greater good” logic but raises a hard practical objection: even fully deidentified dental imaging data, particularly 3D scans combining CBCT, facial geometry, and intraoral data, may be reidentifiable through the combination of features alone.⁽¹⁾ This is more acute in dentistry than in many other specialties since panoramic radiographs and CBCT data encode anatomically unique features that can function as biometric signatures.

Dentistry-focused reviews confirm this concern. A 2024 piece in the *Journal of Oral Biology and Craniofacial Research* (Duggal & Tripathi) frames it clearly: patients must be notified both about how their data are used and about AI's role in decision-making, with the ethical burden falling on clinicians to bridge the gap between technical opacity and patient understanding.⁽²⁾

A 2022 review covering 42 papers from the AI-in-dentistry literature (Saudagar et al.) concludes that informed consent, anonymity, and security remain among the most consistently underaddressed issues in the field and calls for explicit formal policies, not just guidelines, to govern AI use.⁽³⁾

A 2025 paper in *digital health* (Roganovič) took this further by developing a consent checklist and decision flowchart for AI-assisted dental practice, validated with practicing Serbian dentists; more than 90% of respondents agreed that standardized consent improves patient communication and trust when AI is framed as operating under clinician supervision.⁽⁴⁾

A particularly acute ethical problem arises with what a 2025 *Journal of Dental Education* letter calls “multimodal dental data”: modern chairside AI systems integrate intraoral scans, CBCT data, occlusal analysis, and facial scanning, creating datasets that combine identity-attributing biometric features with health status and even socioeconomic indicators.⁽⁵⁾

The authors argue that these datasets constitute “a special category of privacy asset requiring more stringent and nuanced protection than traditional medical information” and that patients should be able to selectively consent to specific data types within that bundle.

The Legal Landscape: the HIPAA, the GDPR, and the EU AI Act

The regulatory picture is fragmented across jurisdictions, and there is a genuine tension between each framework's principles and how AI training actually works.

Under HIPAA (US), deidentified data can generally be used for secondary purposes without explicit consent, but what counts as adequately deidentified is contested for dental imaging. Dental radiographs that retain metadata or accompanying clinical records or can be combined with other data may still constitute protected health information (PHI). HIPAA's “minimum necessary” principle applies, but the statute was drafted well before the AI training workflows existed. A 2025 narrative review in a Q1 dental journal (Brinz et al.) covering the GDPR, HIPAA, the EU AI Act, and the European Health Data Space revealed that dental data, radiographs, CBCT, photographs, and intraoral scans are subject to strict privacy regulation under all major frameworks but that practical guidance on multi-institutional sharing for AI purposes is thin and inconsistent.⁽⁶⁾

Under the GDPR (EU), the situation is more restrictive. Health data is a “special category” under Article 9 that requires explicit consent or a recognized legal basis (public interest, scientific research exemptions). Four rights create specific difficulties for AI training: the right to erasure (“right to be forgotten”), which would require the ability to remove a data point's contribution from

a trained model, technically very hard; the right to explain for automated decisions; the right against profiling; and the right to data portability. A 2018 legal analysis (Thayer) that I found in my search argues that these four rights create genuine compliance challenges that most AI operators have not adequately resolved. In the *European Data Protection Law Review*, Pierce (2018) further flags that the GDPR's purpose limitation and data minimization principles are in direct tension with the typical practice of training AI on large, richly characterized datasets.⁽⁷⁾

The DeepMind-NHS case is the canonical cautionary example here. The Royal Free London NHS Trust shared approximately 1.6 million patient records with DeepMind to develop an AI application, relying on implied consent under the assumption that the data would be used for direct care. The UK Information Commissioner's Office ruled this unlawful: AI training is not direct clinical care, and consent for clinical treatment does not extend to secondary commercial or research use.⁽⁸⁾ Dental researchers and institutions planning similar arrangements should treat this precedent as directly applicable.

The EU AI Act (effective 2024–2026) adds another layer. AI systems used in healthcare are classified as high risk under Annex III, which imposes requirements for risk management, data governance, transparency, and human oversight. Systems trained on patient data without documented consent processes and audit trails may fail conformity assessments.

Clinical Implications: Bias, Validity, and Algorithm Trust

Beyond consent and legality, there are clinical validity consequences for nonconsensual, nonrepresentative training datasets. If dental AI is trained predominantly on data from specific clinical environments, patient demographics, or imaging systems, the resulting model may perform significantly worse on patients who differ from the training distribution, a classic bias propagation problem. The dental literature reflects this concern: reviews consistently flag that AI models for panoramic or CBCT analysis, when trained on convenience samples (e.g., academic hospital records without systematic inclusion efforts), tend to underperform on underserved populations, lower-resource imaging equipment, or less common pathologies.⁽⁹⁾

AI is also a “black box” in clinical decision-making. When a model trained on patient data without their knowledge informs diagnosis or treatment planning, the patient is affected by a system to which they did not agree and often cannot challenge. Albalawi et al. review explainable AI (XAI) as a partial technical solution: if the model's reasoning is interpretable, at least the clinician can evaluate and override its recommendations, preserving the locus of accountability. A 2025 review in the *Journal of Imaging Informatics in Medicine* identifies federated learning, differential privacy, and blockchain-anchored audit trails as the most promising privacy-preserving technical mitigations, although all involve trade-offs in model accuracy or implementation complexity.⁽¹⁰⁾

The OdontoAI project, a 2023 effort to create the largest public panoramic radiograph dataset, illustrates the field's practical response: pooling 4,000 images with human-in-the-loop annotation but publishing the framework explicitly so that data governance choices can be scrutinized. Whether the consent protocols behind that dataset meet contemporary standards is not clear from the abstract.

What Responsible Practice Looks Like

Several convergent recommendations emerge across the sources I found. First, broad or dynamic consent is increasingly favored over the binary choice between study-specific consent and no consent at all. Dynamic consent allows patients to revisit and adjust data use preferences over time via digital platforms and can include granular choices about which data types to share (e.g., radiographs but not full clinical records) and with whom (academic researchers but not commercial entities).⁽⁸⁾ Second, federated learning, which involves training models locally without centralizing raw data, is gaining traction as a technical route to privacy preservation, especially for multi-institutional dental AI development.^(11,12,13)

Third, clear demarcation of commercial versus public-good data use matters: Larson et al.'s framework explicitly states that it is unethical for institutions to “sell” clinical data under exclusive arrangements for monetary gain, even if sharing it freely for AI research is defensible.^(12,14,15)

The honest summary of where the field stands: dental-specific regulatory and ethical guidance remains underdeveloped relative to radiology or cardiology, where professional bodies (e.g., the Canadian Association of Radiologists) have issued white papers.^(16,17,18) Dentistry generates data, panoramic images, CBCT, intraoral scans, and clinical records that are at least as sensitive and potentially more reidentifiable than typical medical imaging, yet the consent and governance infrastructure has lagged.

Dental researchers and institutions using patient data for AI training without explicit consent are, in most jurisdictions, operating in a legal gray zone in which regulatory bodies are beginning to close and should proactively engage IRBs, obtain documented legal bases for data use, and explore privacy-preserving training architectures.^(19,20,21,22)

This is from an initial search pass, and the EU AI Act implementation guidance, national dental regulatory body positions, and jurisdiction-specific case law on the reidentification of dental biometric data would all be worth deeper examination.

Author perspective

The use of dental patient data, particularly panoramic radiographs and related imaging modalities, for training artificial intelligence systems introduces a set of interrelated ethical, legal, and clinical implications that require careful examination. These data are generated within a clinical context in which the primary purpose is diagnosis and treatment, yet their subsequent incorporation into machine learning pipelines reflects a secondary use that is not always anticipated by patients. This distinction between primary and secondary use is central to understanding the current tensions in the development of dental AI.

From an ethical standpoint, the principle of patient autonomy is directly involved. In clinical dentistry, informed consent is traditionally structured around procedures, risks, and treatment alternatives. The extension of consent to include downstream data

processing for algorithm training remains inconsistently addressed. Many existing workflows rely on broad or implicit consent mechanisms embedded in institutional forms, which may not clearly specify the potential reuse of radiographic data for computational purposes. This creates a gap between what patients reasonably understand and what is technically performed with their data. This issue is compounded by the scale of data aggregation required for effective model training, where individual awareness becomes diluted within large datasets.

Confidentiality represents another critical dimension. Dental radiographs, including panoramic and three-dimensional images, contain anatomical structures that may be distinctive at the individual level. Even when traditional identifiers are removed, the possibility of reidentification cannot be fully excluded, particularly when imaging data are combined with other clinical or demographic variables. This characteristic challenges the assumption that deidentification alone is sufficient to mitigate privacy risks. In practice, the uniqueness of craniofacial morphology introduces a form of biometric signature that may persist across datasets, raising questions about long-term data security and traceability.

The legal landscape governing these practices is heterogeneous and, in many cases, not fully aligned with the technical realities of artificial intelligence. Regulatory frameworks addressing health data generally emphasize consent, purpose limitations, and data minimization. These principles are difficult to reconcile with machine learning approaches that benefit from large, diverse, and richly annotated datasets. The requirement to define a specific purpose at the time of data collection contrasts with the exploratory nature of AI development, where future applications may not be known in advance. This creates uncertainty regarding the legitimacy of reusing dental imaging data beyond their original clinical intent, particularly in cross-institutional or commercial contexts.

Clinical implications extend beyond regulatory compliance. The performance and reliability of AI systems in dentistry depend on the representativeness and quality of the training data. When datasets are assembled without systematic inclusion criteria or without consideration of demographic diversity, there is a risk of introducing bias into the resulting models. For example, a model trained predominantly on images from a specific population or imaging device may exhibit reduced accuracy when applied in different clinical settings. This variability has direct consequences for diagnostic consistency and patient safety. The absence of transparency in how training data are sourced further complicates the evaluation of model validity.

Trust in AI-assisted clinical decision-making is also affected by these dynamics. Patients are becoming increasingly aware of digital technologies in healthcare, yet their understanding of how personal data contribute to algorithm development remains limited. If patients perceive that their data are used without explicit permission or clear explanation, confidence in both the technology and the clinician may be undermined. This erosion of trust can influence the acceptance of AI-supported diagnostics and treatment planning, which are expected to play an expanding role in dental practice. The clinician's responsibility extends to communicating not only clinical findings but also the presence and role of AI systems in the decision process.

The opacity of many machine learning models introduces additional challenges. When diagnostic outputs are generated by systems that lack interpretability, assessing the influence of specific data inputs on the result becomes difficult. This limitation is particularly relevant when the training data include records obtained without explicit consent, as patients are indirectly affected by systems whose development they did not authorize. Efforts to improve model explainability aim to address this issue, yet there remains a trade-off between interpretability and performance in many applications. The degree to which explainable systems can restore accountability in the context of dental AI remains an open question.

Data governance mechanisms are central to addressing these concerns. Institutional review processes, data access controls, and audit trails provide a framework for responsible data handling, yet their implementation varies widely across institutions. The development of standardized protocols for the use of dental data in AI is still in progress. Approaches such as federated learning, where models are trained across decentralized data sources without transferring raw data, have been proposed as a means to reduce privacy risks. These methods introduce additional technical complexity and may affect model performance; however, they offer a pathway toward balancing data utility with data protection.

The concept of dynamic consent has been proposed as a more flexible alternative to traditional consent models. In this framework, patients are given the opportunity to manage their data-sharing preferences over time, with options to approve or withdraw specific uses. This approach aligns more closely with the evolving nature of AI research, although its practical implementation requires digital infrastructure and sustained patient engagement. The feasibility of such systems in routine dental practice remains uncertain, particularly in settings with limited resources.

Methodological limitations in the current body of research should be acknowledged. Many studies evaluating AI in dentistry rely on retrospective datasets with incomplete documentation of consent procedures. The lack of standardized reporting on data provenance, preprocessing steps, and patient inclusion criteria limits the ability to assess ethical compliance and reproducibility. There is also variability in how privacy-preserving techniques are applied and evaluated, making comparisons across studies difficult. These gaps highlight the need for clearer reporting standards and more rigorous study designs.

Uncertainty persists regarding the long-term implications of integrating AI into dental workflows. While potential benefits include improved diagnostic efficiency and consistency, these gains must be weighed against risks related to data misuse, bias, and loss of patient trust. The rapid pace of technological development has outstripped the evolution of ethical guidelines specific to dentistry, creating a transitional period in which practices may not be fully aligned with emerging expectations.

In conclusion, the use of panoramic radiographs and other dental patient data for AI training without explicit informed consent raises complex issues that span ethical principles, legal requirements, and clinical practice. Addressing these challenges requires coordinated efforts to develop transparent consent processes, robust data governance frameworks, and methodologies that account for bias and variability. The sustainability of AI in dentistry depends not only on technical performance but also on the ability to maintain patient trust and uphold established standards of care.

FUNDING

The authors received no funding for this research.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest.

AUTHORSHIP CONTRIBUTIONS

Conceptualization: Youris Samón Mayán, Ana Rodríguez Yanes, Yivelin Fernández Queija, Lourdes Hernández Cuétara, Arlin Castro Diaz.

Writing – original draft: Youris Samón Mayán, Ana Rodríguez Yanes, Yivelin Fernández Queija, Lourdes Hernández Cuétara, Arlin Castro Diaz.

Writing – review and editing: Youris Samón Mayán, Ana Rodríguez Yanes, Yivelin Fernández Queija, Lourdes Hernández Cuétara, Arlin Castro Diaz.

REFERENCES

1. Larson DB, Magnus DC, Lungren MP, Shah NH, Langlotz CP. Ethics of Using and Sharing Clinical Imaging Data for Artificial Intelligence: A Proposed Framework. *Radiology* 2020;295:675–82. <https://doi.org/10.1148/radiol.2020192536>.
2. Duggal I, Tripathi T. Ethical principles in dental healthcare: Relevance in the current technological era of artificial intelligence. *J Oral Biol Craniofac Res* 2024;14:317–21. <https://doi.org/10.1016/j.jobcr.2024.04.003>.
3. Saudagar N, Jabeen R, Sharma P, Mong S, Vaderhobli RM. Ethical Implications with the Utilization of Artificial Intelligence in Dentistry. *EBEM* 2021;12. <https://doi.org/10.1615/EthicsBiologyEngMed.2022043936>.
4. Roganović J. Developing a consent checklist for AI in dentistry: Thematic analysis and pilot survey validation. *Digit Health* 2025;11:20552076251393227. <https://doi.org/10.1177/20552076251393227>.
5. Li J, He X. Multimodal Data Privacy Challenges in Chairside Generative AI. *J Dent Educ* 2026;90:8–9. <https://doi.org/10.1002/jdd.70083>.
6. Brinz J, Eslamiamirabadi N, Salamaty A, Tresp V, Schwendicke F, Tichy A. Data sharing for responsible artificial intelligence in dentistry: a narrative review of legal frameworks and privacy-preserving techniques. *J Dent* 2025;163:106130. <https://doi.org/10.1016/j.jdent.2025.106130>.
7. Monah SR, Wagner MW, Biswas A, Khalvati F, Erdman LE, Amirabadi A, et al. Data governance functions to support responsible data stewardship in pediatric radiology research studies using artificial intelligence. *Pediatr Radiol* 2022;52:2111–9. <https://doi.org/10.1007/s00247-022-05427-2>.
8. Sangaraju VV. AI and Data Privacy in Healthcare: Compliance with HIPAA, GDPR, and emerging regulations. *International Journal of Emerging Trends in Computer Science and Information Technology* 2025:67–74. <https://doi.org/10.56472/ICCSAIML25-108>.
9. Shah SMM. Harnessing electronic patient records for ai innovation: balancing data privacy and diagnostic advancement. *Journal of khyber college of dentistry* 2024;14:1–1. <https://doi.org/10.33279/jkcd.v14i4.843>.
10. Krupinski EA. An Ethics Framework for Clinical Imaging Data Sharing and the Greater Good. *Radiology* 2020;295:683–4. <https://doi.org/10.1148/radiol.2020200416>.
11. Dauda B, Denier Y, Dierickx K. What Do the Various Principles of Justice Mean Within the Concept of Benefit Sharing? *J Bioeth Inq* 2016;13:281–93. <https://doi.org/10.1007/s11673-016-9706-4>.
12. Hogue CJ. Ethical issues in sharing epidemiologic data. *J Clin Epidemiol* 1991;44 Suppl 1:103S-107S. [https://doi.org/10.1016/0895-4356\(91\)90183-a](https://doi.org/10.1016/0895-4356(91)90183-a).
13. Marshall E. Data sharing: a declining ethic? *Science* 1990;248:952–7. <https://doi.org/10.1126/science.2343306>.
14. Kelley M, Fryer-Edwards K, Fullerton SM, Gallagher TH, Wilfond B. Sharing data and experience: using the Clinical and Translational Science Award (CTSA) “moral community” to improve research ethics consultation. *Am J Bioeth* 2008;8:37–9; discussion W4-6. <https://doi.org/10.1080/15265160802109397>.

15. Hedlund J, Eklund A, Lundström C. Key insights in the AIDA community policy on sharing of clinical imaging data for research in Sweden. *Sci Data* 2020; 7:331. <https://doi.org/10.1038/s41597-020-00674-0>.
16. Orhan K, Bayrakdar IS, Celik O, Ayan B, Polat E. Can the blockchain-enabled interplanetary file system (Block-IPFS) be a solution for securely transferring imaging data for artificial intelligence research in oral and maxillofacial radiology? *Imaging Sci Dent* 2021;51:337. <https://doi.org/10.5624/isd.20210144>.
17. Fasterholdt I, Naghavi-Behzad M, Rasmussen BSB, Kjølhede T, Skjøth MM, Hildebrandt MG, et al. Value assessment of artificial intelligence in medical imaging: a scoping review. *BMC Med Imaging* 2022;22:187. <https://doi.org/10.1186/s12880-022-00918-y>.
18. Goisauf M, Cano Abadía M. Ethics of AI in Radiology: A Review of Ethical and Societal Implications. *Front Big Data* 2022;5:850383. <https://doi.org/10.3389/fdata.2022.850383>.
19. Liaw S-T, Liyanage H, Kuziemy C, Terry AL, Schreiber R, Jonnagaddala J, et al. Ethical Use of Electronic Health Record Data and Artificial Intelligence: Recommendations of the Primary Care Informatics Working Group of the International Medical Informatics Association. *Yearb Med Inform* 2020;29:51–7. <https://doi.org/10.1055/s-0040-1701980>.
20. Reddy S, Allan S, Coghlan S, Cooper P. A governance model for the application of AI in health care. *J Am Med Inform Assoc* 2020;27:491–7. <https://doi.org/10.1093/jamia/ocz192>.
21. Jaremko JL, Azar M, Bromwich R, Lum A, Alicia Cheong LH, Gibert M, et al. Canadian Association of Radiologists White Paper on Ethical and Legal Issues Related to Artificial Intelligence in Radiology. *Can Assoc Radiol J* 2019;70:107–18. <https://doi.org/10.1016/j.carj.2019.03.001>.
22. Aledhari M, Razzak R, Parizi RM, Saeed F. Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Access*. 2020; 8:140699–725. <https://doi.org/10.1109/access.2020.3013541>.