Viewpoint

The Personalization-Privacy Paradox in AI-Enabled Health Care: Managing Trust and Governance Under the European Health Data Space

Maxime Ducret[1,2], PhD; Julien Cloarec[3], PhD; Nour Alrabie[4], PhD; Mouna Mouncif-Moungache[5], PhD

[1]Faculty of Dentistry, Université Claude Bernard Lyon 1, Lyon, Rhône-Alpes, France
[2]Centre de soins dentaires, Pôle d'Odontologie, Hospices Civils de Lyon, Lyon, France
[3]iaelyon School of Management, Université Jean Moulin Lyon 3, Lyon, France
[4]LEREPS, Université Toulouse Jean Jaurès, Toulouse, France
[5]Department of Public Law, Université Jean Monnet, Saint-Étienne, France

Corresponding Author:

Maxime Ducret, PhD
Faculty of Dentistry
Université Claude Bernard Lyon 1
11 Rue Guillaume Paradin
Lyon, Rhône-Alpes 69008
France
Phone: 33 472722619
Email: ducret.maxime@gmail.com

Abstract

AI enables increasingly personalized health care, but the data required intensifies long-standing concerns about privacy, confidentiality, and trust as the European Health Data Space (EHDS) expands the primary and secondary use of health data. This viewpoint examines how the EHDS reshapes the personalization-privacy paradox in AI-enabled health care and under what conditions it can manage, rather than resolve, this paradox. Drawing on privacy calculus theory, we analyze the patient-practitioner relationship, the flow of data from primary to secondary use, and the governance mechanisms introduced by Regulation (EU) 2025/327, including data access bodies, data permits, differentiated opt-out rights, and privacy-preserving technologies. We identify 5 governance conditions: purpose-specific governance, accessible opt-out design, practitioner-mediated transparency, privacy-preserving infrastructure, and independent oversight of secondary use actors. When these conditions are met, the EHDS can sustain trust while enabling personalization. We conclude that the EHDS does not eliminate the paradox but can provide a governance architecture to manage it, depending more on implementation quality and patient engagement than on the ambition of the framework itself.

J Med Internet Res 2026;28:e94903; doi: 10.2196/94903

Keywords: personalization-privacy paradox; European Health Data Space; artificial intelligence; AI; health data governance; privacy calculus; patient trust

Introduction

The personalization-privacy paradox captures a core tension in the digital ecosystem: individuals value the enhanced user experiences that personalization affords, yet remain reluctant to provide the data such personalization requires, expressing concern over how their data are collected, processed, and secured [1]. This paradox has become increasingly salient with the rise of advanced data technologies and AI, which enable refined profiling and predictive analytics [2,3]. AI systems, powered by machine learning and deep learning, can detect patterns in vast datasets and forecast behaviors, needs, and health trajectories, yet this precision amplifies anxieties about surveillance, loss of control, and opaque decision-making. Although personalization is intended to improve engagement and satisfaction, it often provokes unease in consumer and health care contexts [4]. Such concerns are even more critical in health care, where breaches of trust may directly compromise patient safety and clinical outcomes.

In health care, where the General Data Protection Regulation (GDPR) tightly regulates data flows, these tensions are sharper: rules designed to protect patients

can also limit the deployment of AI tools with the potential to improve diagnosis, treatment, and prevention [5]. This duality illustrates how personalization can be simultaneously valued and resisted, creating cognitive dissonance for individuals who desire individualized services but remain wary of data exploitation. Academic discourse conceptualizes this ambivalence as the personalization-privacy paradox, emphasizing users' contradictory attitudes and behaviors [3,6]. To unravel this paradox, scholars have applied privacy calculus theory [2,7-11], which highlights how individuals weigh disclosure trade-offs in exchange for personalization. Well-being has recently emerged as a further determinant, as positive emotional evaluations of digital interactions increase individuals' willingness to share data [2,3]. Analogous trade-offs, long documented on social media via social exchange theory [8,12-14], now emerge in health care, where patients weigh the benefits of AI-enabled personalization against the risks of misuse, third-party access, or loss of confidentiality. This concern is not uniform across health data: perceived sensitivity varies with diagnosis type, stigma, chronicity, and expected benefit, so patients may readily share routine information while resisting disclosure of information associated with stigmatized or chronic conditions [15-17].

Thus, the personalization-privacy paradox extends beyond individual users to pose a strategic challenge for organizations, which must align consumer psychology with regulatory obligations to design personalization strategies that respect privacy without undermining perceived value [2,18]. The European Health Data Space (EHDS) explicitly addresses both primary health data, collected directly from patients during care, and secondary health data, which refer to the reuse of health information for research, policymaking, or technological innovation [19]. This framework legitimizes and structures these uses, but it also generates tensions between them.

This Viewpoint analyzes the paradox at the individual behavioral level and in relation to institutional and regulatory tensions and applies this framework to the EHDS to derive the conditions under which it can manage, rather than resolve, the paradox. It moves from the patient's privacy calculus to the practitioner relationship and then to the institutional governance of secondary use. The guiding question of this manuscript is: How can the EHDS manage the personalization-privacy paradox in AI-enabled health care while sustaining patient trust and enabling medical AI innovation?

The Medical Personalization-Privacy Paradox

The personalization-privacy paradox has often been studied in the domain of human-computer interaction [20]. In health care, however, the paradox acquires greater complexity because personalization is increasingly driven by AI [21]. Unlike in other digital sectors, the stakes in medicine are higher: AI systems are not simply predicting consumer preferences but also influencing diagnoses and treatment pathways, including decisions with major clinical consequences. In this context, the paradox emerges as a tension between protecting patient privacy and harnessing AI to deliver highly personalized care.

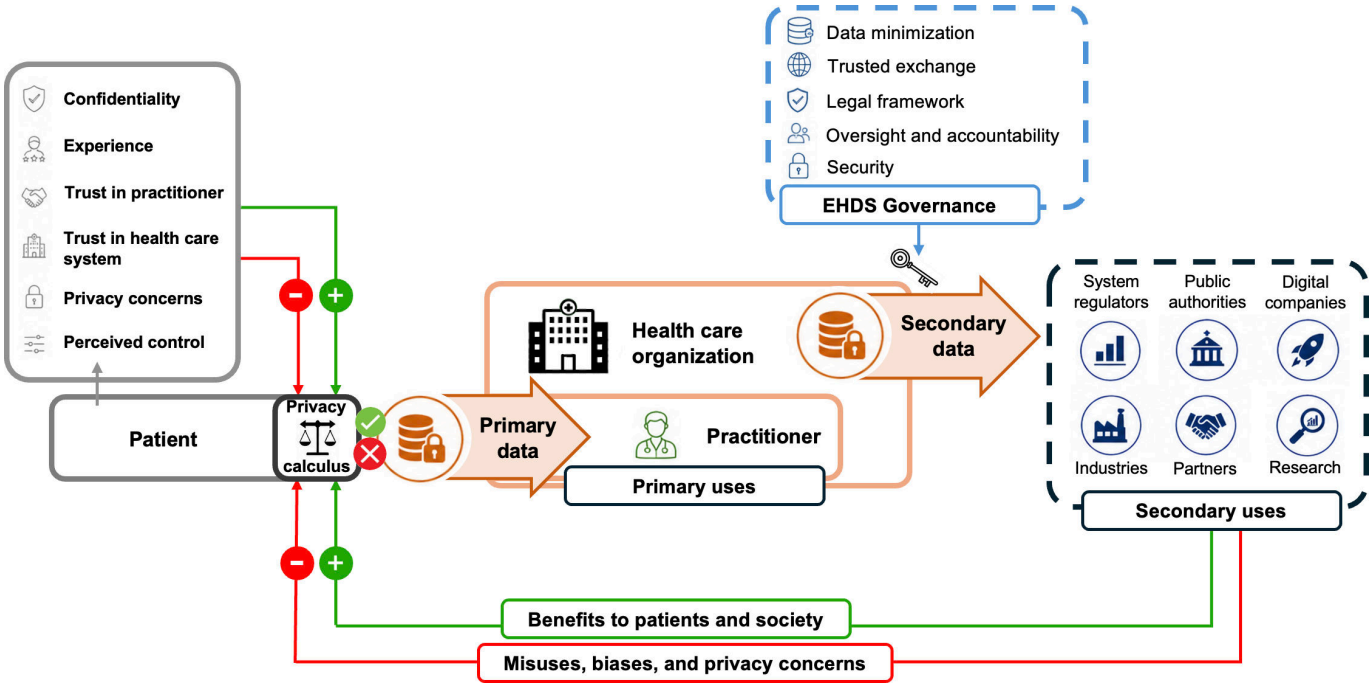
In the health care context, "personalization" means adapting diagnosis, treatment, prevention, and monitoring to an individual patient's biological, genetic, behavioral, and contextual profile, encompassing precision medicine, clinical decision support, risk stratification, and individualized treatment, as distinct from the consumer market sense of targeted content. We further distinguish direct clinical personalization, which tailors care to one patient, from population-level AI analytics that generate aggregate insights. The paradox examined here is most acute in the former: the specific tension between desiring personalized services and resisting the data collection they require, reflecting a broader gap between stated privacy preferences and actual disclosure behavior [22].

Figure 1 illustrates this dynamic through the privacy calculus framework, in which patients' decisions to share data are mediated by perceived benefits and risks, confidentiality, prior experience, and trust in practitioners and the health care system, as well as by how primary data subsequently flow into secondary use under EHDS governance.

Over the past decade, AI-driven digital health technologies [23] have transformed how medical data are generated, analyzed, and used. Electronic health records (EHRs), wearable sensors, telemedicine platforms, and AI-powered clinical decision support systems now enable continuous data collection and advanced predictive modeling [24]. Machine learning algorithms can, for example, detect early signs of sepsis, personalize oncology treatments, or predict hospital readmission risks with high accuracy. These opportunities for personalization go far beyond traditional models of medical practice. Yet, they also intensify concerns about how patient data are stored, processed, and shared [25].

Historically, health care data exchange has been grounded in the ethical principles of confidentiality and transparent communication, which foster trust between patients and health care professionals. Transparency ensures that patients understand how their information is managed [26]. When responsibly used, AI-driven analytics can help clinicians make earlier diagnoses and tailor treatment, improving clinical outcomes and quality of life [27]. However, the same algorithms often operate as "black boxes," making it difficult for practitioners to explain how specific predictions or treatment recommendations are generated. This opacity undermines informed consent and challenges traditional notions of trust in the medical relationship. Trust in AI-enabled health care requires both algorithmic explainability (how a model generates its output) and data governance transparency (who accesses data and why). Neither alone is sufficient.

Figure 1. The privacy calculus in the patient-practitioner relationship, the flow of primary data toward secondary use under European Health Data Space (EHDS) governance, and the resulting feedback on patients' willingness to share data.



A further complication is the increasing involvement of third-party actors, including AI software vendors, private insurers, and digital health app developers, who process patient data outside the traditional patient-health care professional relationship [28]. Trust and acceptance vary markedly across these actors: patients generally trust treating clinicians most, followed by public research institutions and health authorities, with commercial companies and insurers trusted considerably less [29]. Figure 1 illustrates this extension of data flows from practitioners to secondary use stakeholders such as researchers, policymakers, and industry actors, underscoring the risks of commercial exploitation and reidentification.

Pseudonymization has been widely promoted as a safeguard to protect health data [30], and it remains an important safeguard: it reduces direct identifiability and lowers the risk of accidental disclosure. It is not equivalent to full anonymization [31], however, and AI itself heightens the risk of reidentification. Sophisticated algorithms can cross-reference pseudonymized medical records with other datasets (eg, location data, genetic information, and consumer behavior) to reidentify individuals [32]. In health care, where genetic data are inherently unique, this residual risk underscores the need for layered safeguards, combining pseudonymization with access controls, purpose limitation, and privacy-preserving technologies, rather than relying on pseudonymization alone. Within the European Union (EU), the GDPR's purpose limitation requirements, antidiscrimination law, and the EHDS framework for permitted data use substantially restrict such practices, although reidentification risk warrants continued vigilance.

The medical personalization-privacy paradox is shaped by several interrelated factors, including trust in the health care system [33]. Following Hall et al [34], this analysis distinguishes interpersonal, institutional, and system trust, each requiring different safeguards. Confidentiality has also been a cornerstone of medical ethics since the Hippocratic Oath, serving to foster openness, protect against discrimination, and maintain institutional legitimacy. Yet, AI-enabled personalization is challenging these traditional principles [35]. By aggregating longitudinal health data, including genomics, lifestyle patterns, and real-time biometrics, AI systems magnify both the potential benefits of personalization and the risks of privacy intrusion [36]. Patients face an increasingly difficult calculus: whether to share intimate data with practitioners and institutions that promise better health outcomes but may expose them to unintended risks. Trust in primary use and the governance of secondary use are not independent: when patients discover, or merely suspect, that data shared with their practitioner have circulated to insurers or unfamiliar research institutions, this can retroactively undermine trust in the original clinical relationship and reduce future willingness to share data. The medical personalization-privacy paradox in the age of AI, and its manifestation under the EHDS, can therefore be conceptualized through 5 interdependent dimensions (Table 1).

Table 1. Dimensions, opportunities, and challenges of the personalization-privacy paradox within the European Health Data Space (EHDS).

Dimensions	Opportunity	Privacy and ethical challenge	Implication for the paradox
Data requirements and cross-border scale	AI needs vast, multimodal datasets, and EHDS interoperability expands cross-border access, especially for rare diseases.	Larger, cross-border datasets raise the risk of reidentification and expose legal and cultural heterogeneity across member states.	Precision medicine must reconcile data depth and scale with harmonized safeguards.
Transparency and patient awareness	EU[a] AI Act explainability obligations, combined with EHDS transparency on data access and use, can make AI decision support more interpretable and trustworthy.	Patients see AI as opaque, and practitioners are not always equipped to explain data use.	Trust needs both algorithmic explainability and clear data governance communication.
Patient empowerment and opt-out	Digital platforms and EHDS opt-out give patients differentiated control over data sharing.	Complex consent or opt-out design may exclude less digitally literate patients, skewing AI training data.	Empowerment builds trust but may widen inequity if access is uneven.
Privacy-preserving technologies	Federated learning, homomorphic encryption, and synthetic data enable AI training without centralizing records.	These technologies can be resource-intensive and may reduce performance, while synthetic data and pseudonymization still carry residual risk.	These technologies balance personalization with safeguards but require investment and standardization.
Governance, regulatory, and sectoral tensions	General Data Protection Regulation, EHDS, and the EU AI Act layer protections while enabling responsible innovation across clinical, research, and industry uses.	Oversight may lag behind innovation, and tensions arise when clinical, research, commercial, and insurance actors use data differently.	This dimension requires actor-differentiated, cross-layer governance so AI serves individual and public interests without conflating distinct purposes.

[a]EU: European Union.

This synthesis illustrates that the personalization-privacy paradox in health care cannot be reduced to a trade-off between convenience and privacy, as in consumer markets. Instead, it reflects a deeper dilemma: whether patients and practitioners can trust AI systems to deliver personalization without compromising the ethical foundation of medicine.

The EHDS: A New Environment for Patient-Practitioner Data Exchange

The EHDS is a landmark initiative by the EU to create a secure, interoperable framework for health data exchange across member states, with AI-enabled personalization as one particularly salient and privacy-sensitive application among several rather than its defining purpose [37]. It distinguishes between primary use, which involves access for the direct care of the patient concerned, and secondary use, which involves the reuse of health data for research, innovation, policymaking, or regulatory purposes. This distinction structures the governance mechanisms discussed below.

Regulation (EU) 2025/327 establishes mechanisms central to this paradox: Health Data Access Bodies in each member state govern secondary access requests and issue data permits specifying the purpose, scope, and duration of access; patients retain differentiated opt-out rights for primary portability and secondary use; and mandatory interoperability standards ensure consistency in cross-border data exchange. These mechanisms operate within 3 regulatory layers that should not be treated as interchangeable: the GDPR sets the general data protection floor, the EHDS adds a health-specific access and secondary use layer, and the EU AI Act adds risk-based transparency and oversight obligations for high-risk clinical AI.

The EHDS is particularly significant because it situates health data governance at the intersection of health care delivery, digital innovation, and market integration. The EHDS has explicit economic objectives [37]: by facilitating the flow of data across borders, it contributes to the functioning of the internal market and strengthens Europe's competitiveness in digital health industries.

To achieve these ambitions, the EHDS incorporates robust safeguards aligned with the GDPR and mandates common interoperability standards, seeking to overcome the fragmentation of European health systems while promoting continuity of care and research collaboration.

Nevertheless, the implementation of the EHDS faces significant challenges. Marelli et al [38] argue that the EHDS may be "too big to succeed," given the risk of fragmented national transposition, disparate data quality, and uneven capacity among access bodies across 27 member states. Ganna et al [39] add that realizing its research potential also depends on data access timelines and investment in federated infrastructure. Governance arrangements will need to be carefully calibrated to prevent fragmented approaches at the national level [40], requiring coordination between EU-wide authorities and those of member states.

The Challenges of the Personalization-Privacy Paradox in the Context of the EHDS

The EHDS raises new challenges that could exacerbate the personalization-privacy paradox. AI systems in health care require large volumes of sensitive, high-quality data to function effectively, but the very practices that enable personalization may compromise privacy and erode trust [41]. If poorly governed, the EHDS could unintentionally facilitate reidentification, misuse by third parties, or algorithmic biases that harm vulnerable populations [42]. To navigate this tension, it is essential to understand the opportunities and risks of the EHDS in an AI-driven medical context (Table 1).

Three privacy-preserving technologies are particularly relevant here: federated learning, homomorphic encryption, and synthetic data, which are detailed in Table 1. Rare disease research illustrates the stakes: the EHDS's cross-border pooling of data is essential because no single member state has enough patients to validate AI diagnostic tools, making secondary use for this purpose a clear public interest case, even though it requires sharing data with unfamiliar institutions. Patients are not generally opposed to secondary use: many support it when it serves clear public interest purposes, is governed transparently, and involves trustworthy actors [43,44]. Patient empowerment tools such as consent dashboards and opt-out portals presuppose digital access and health literacy, which are unevenly distributed across EU populations. Consequently, patients with lower levels of digital literacy may be underrepresented or overrepresented in training datasets.

Finally, concerns persist about the potential misuse of data, including discriminatory practices by insurers or the commodification of sensitive health information. AI magnifies these risks: predictive algorithms could be used to deny coverage to high-risk individuals or to market treatments selectively, raising profound ethical dilemmas [45,46]. The long-term success of the EHDS will therefore depend on its ability to sustain public trust by ensuring that the collective benefits of data sharing and AI innovation clearly outweigh the individual risks to privacy. This requires continuous collaboration among stakeholders and vigilant adaptation of regulatory and ethical frameworks to meet the evolving challenges of medical AI.

Taken together, these considerations suggest that the EHDS can manage rather than intensify the paradox when 5 conditions are met: purpose-specific governance separating public interest uses from commercial uses; accessible, user-centered opt-out design; practitioner-mediated transparency; standardized privacy-preserving infrastructure; and independent oversight of secondary use actors. Without these conditions, expanding data access without commensurate safeguards risks deepening rather than resolving the paradox.

Conclusions

This Viewpoint asked how the EHDS can foster trustworthy AI-enabled personalization while safeguarding patient privacy. The answer is that the EHDS does not resolve the personalization-privacy paradox but, when the 5 conditions identified above are met, provides a governance architecture that can manage it. The future of the paradox will be defined by the EU's ability to harness AI for transformative health care innovation while preserving the trust that underpins the patient-practitioner relationship.

Success will depend on embedding these conditions into the architecture of AI-enabled health care. Practitioner-mediated transparency and user-centered opt-out design are the most directly actionable conditions in the short term, but the EHDS will offer a replicable model for managing the paradox only if the EU also sustains investment in privacy-preserving infrastructure and independent oversight.

Generative AI Use

The authors used generative AI (Sonnet 5; Claude) solely during the final stage of manuscript preparation to improve the readability, fluency, and English language style of selected sections of the manuscript. No AI tool was used to generate scientific ideas, interpret results, perform analyses, or draw conclusions. All scientific content was developed and validated exclusively by the authors, who take full responsibility for the accuracy and integrity of the manuscript.

Funding

The authors declared no financial support was received for this work

Conflicts of Interest

None declared.

References

1. Schweidel DA, Bart Y, Inman JJ, et al. How consumer digital signals are reshaping the customer journey. J Acad Mark Sci. 2022;50(6):1257-1276. [doi: 10.1007/s11747-022-00839-w] [Medline: 35221393]
2. Cloarec J, Meyer-Waarden L, Munzel A. The personalization–privacy paradox at the nexus of social exchange and construal level theories. Psychol Mark. Mar 2022;39(3):647-661. [doi: 10.1002/mar.21587]
3. Cloarec J, Meyer-Waarden L, Munzel A. Transformative privacy calculus: conceptualizing the personalization-privacy paradox on social media. Psychol Mark. Jul 2024;41(7):1574-1596. [doi: 10.1002/mar.21998]

4. Grewal D, Hulland J, Kopalle PK, Karahanna E. The future of technology and marketing: a multidisciplinary perspective. J Acad Mark Sci. Jan 2020;48:1-8. [doi: 10.1007/s11747-019-00711-4]
5. Dubé JP, Lynch JG, Bergemann D, et al. Frontiers: the intended and unintended consequences of privacy regulation for consumer marketing. Mark Sci. 2025;44(5):975-984. [doi: 10.1287/mksc.2024.0901]
6. Awad NF, Krishnan MS. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Q. Mar 1, 2006;30(1):13-28. [doi: 10.2307/25148715]
7. Bawack RE, Wamba SF, Carillo KD. Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: evidence from SEM and fuzzy set qualitative comparative analysis. Int J Inf Manag. Jun 2021;58:102309. [doi: 10.1016/j.ijinfomgt.2021.102309]
8. Shih HP, Liu W. Beyond the trade-offs on Facebook: the underlying mechanisms of privacy choices. Inf Syst E-Bus Manage. Jun 2023;21:353-387. [doi: 10.1007/s10257-023-00622-6]
9. Cherif E, Bezaz N, Mzoughi M. Do personal health concerns and trust in healthcare providers mitigate privacy concerns? Effects on patients' intention to share personal health data on electronic health records. Soc Sci Med. Aug 2021;283:114146. [doi: 10.1016/j.socscimed.2021.114146] [Medline: 34242891]
10. Dinev T, Albano V, Xu H, D'Atri A, Hart P. Individuals' attitudes towards electronic health records: a privacy calculus perspective. In: Gupta A, Patel V, Greenes R, editors. Advances in Healthcare Informatics and Analytics. Springer; 2016:19-50. [doi: 10.1007/978-3-319-23294-2_2]
11. von Kalckreuth N, Feufel MA. Extending the privacy calculus to the mHealth domain: survey study on the intention to use mHealth apps in Germany. JMIR Hum Factors. Aug 16, 2023;10:e45503. [doi: 10.2196/45503] [Medline: 37585259]
12. Aguirre E, Roggeveen AL, Grewal D, Wetzels M. The personalization-privacy paradox: implications for new media. J Consum Mark. Mar 21, 2016;33(2):98-110. [doi: 10.1108/JCM-06-2015-1458]
13. Krafft M, Kumar V, Harmeling C, et al. Insight is power: understanding the terms of the consumer-firm data exchange. J Retail. Mar 2021;97(1):133-149. [doi: 10.1016/j.jretai.2020.11.001]
14. Le C, Zhang Z, Liu Y. Research on privacy disclosure behavior of mobile app users from perspectives of online social support and gender differences. Int J Hum Comput Interact. 2025;41(2):861-875. [doi: 10.1080/10447318.2024.2305988]
15. von Kalckreuth N, Feufel MA. Disease characteristics influence the privacy calculus to adopt electronic health records: a survey study in Germany. Digit Health. 2024;10:20552076241274245. [doi: 10.1177/20552076241274245] [Medline: 39247096]
16. von Kalckreuth N, Prümper AM, Feufel MA. The influence of health data on the use of the electronic health record (EHR) – a mixed methods approach. In: AMCIS 2023 Proceedings. Association for Information Systems; 2023. ISBN: 9781958200056
17. von Kalckreuth N, Feufel MA. Influence of disease-related stigma on patients' decisions to upload medical reports to the German electronic health record: randomized controlled trial. JMIR Hum Factors. Apr 10, 2024;11(1):e52625. [doi: 10.2196/52625] [Medline: 38598271]
18. Aubert-Hassouni C, Cloarec J. Privacy regulation in the age of artificial intelligence. In: Hanlon A, Tuten TL, editors. The SAGE Handbook of Digital Marketing. SAGE Publications; 2022:544-556. [doi: 10.4135/9781529782509.n31]
19. Hussein R, Gyrard A, Abedian S, Gribbon P, Martínez SA. Interoperability framework of the European Health Data Space for the secondary use of data: interactive European Interoperability Framework-based standards compliance toolkit for AI-driven projects. J Med Internet Res. Apr 23, 2025;27:e69813. [doi: 10.2196/69813] [Medline: 40266673]
20. Xu H, Luo X, Carroll JM, Rosson MB. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Decis Support Syst. Apr 2011;51(1):42-52. [doi: 10.1016/j.dss.2010.11.017]
21. Herriger C, Merlo O, Eisingerich AB, Arigayota AR. Context-contingent privacy concerns and exploration of the privacy paradox in the age of AI, augmented reality, big data, and the Internet of Things: systematic review. J Med Internet Res. May 14, 2025;27:e71951. [doi: 10.2196/71951] [Medline: 40367513]
22. Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. J Consum Aff. 2007;41(1):100-126. [doi: 10.1111/j.1745-6606.2006.00070.x]
23. Oh H, Rizo C, Enkin M, Jadad A. What is eHealth (3): a systematic review of published definitions. J Med Internet Res. Feb 24, 2005;7(1):e1. [doi: 10.2196/jmir.7.1.e1] [Medline: 15829471]
24. Borges do Nascimento IJ, Abdulazeem HM, Vasanthan LT, et al. The global effect of digital health technologies on health workers' competencies and health workplace: an umbrella review of systematic reviews and lexical-based and sentence-based meta-analysis. Lancet Digit Health. Aug 2023;5(8):e534-e544. [doi: 10.1016/S2589-7500(23)00092-4] [Medline: 37507197]
25. Desai AN. Artificial intelligence: promise, pitfalls, and perspective. JAMA. Jun 23, 2020;323(24):2448-2449. [doi: 10.1001/jama.2020.8737] [Medline: 32492093]

26. Cloarec J, Cadieu C, Alrabie N. Tracking technologies in eHealth: revisiting the personalization-privacy paradox through the transparency-control framework. Technol Forecast Soc Change. Mar 2024;200:123101. [doi: 10.1016/j.techfore.2023.123101]
27. Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. Health Inf Sci Syst. 2014;2:3. [doi: 10.1186/2047-2501-2-3] [Medline: 25825667]
28. Taddeo M, Floridi L. New civic responsibilities for online service providers. In: Taddeo M, Floridi L, editors. The Responsibilities of Online Service Providers. Springer; 2017:1-10. [doi: 10.1007/978-3-319-47852-4_1]
29. Kühnel E, Wilke F. Health data sharing in Germany: individual preconditions, trust and motives. Front Public Health. 2025;13:1538106. [doi: 10.3389/fpubh.2025.1538106] [Medline: 39975784]
30. Neubauer T, Heurix J. A methodology for the pseudonymization of medical data. Int J Med Inform. Mar 2011;80(3):190-204. [doi: 10.1016/j.ijmedinf.2010.10.016] [Medline: 21075676]
31. El Emam K, Jonker E, Arbuckle L, Malin B. A systematic review of re-identification attacks on health data. PLoS One. 2011;6(12):e28071. [doi: 10.1371/journal.pone.0028071] [Medline: 22164229]
32. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun. Jul 23, 2019;10(1):3069. [doi: 10.1038/s41467-019-10933-3] [Medline: 31337762]
33. Nong P, Platt J. Patients' trust in health systems to use artificial intelligence. JAMA Netw Open. Feb 3, 2025;8(2):e2460628. [doi: 10.1001/jamanetworkopen.2024.60628] [Medline: 39951270]
34. Hall MA, Dugan E, Zheng B, Mishra AK. Trust in physicians and medical institutions: what is it, can it be measured, and does it matter? Milbank Q. 2001;79(4):613-639, v. [doi: 10.1111/1468-0009.00223] [Medline: 11789119]
35. Ning Y, Teixayavong S, Shang Y, et al. Generative artificial intelligence and ethical considerations in health care: a scoping review and ethics checklist. Lancet Digit Health. Nov 2024;6(11):e848-e856. [doi: 10.1016/S2589-7500(24)00143-2] [Medline: 39294061]
36. Topol EJ. High-performance medicine: the convergence of human and artificial intelligence. Nat Med. Jan 2019;25(1):44-56. [doi: 10.1038/s41591-018-0300-7] [Medline: 30617339]
37. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (text with EEA relevance). European Union. 2024. URL: https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng [Accessed 2026-10-16]
38. Marelli L, Stevens M, Sharon T, et al. The European Health Data Space: too big to succeed? Health Policy. Sep 2023;135:104861. [doi: 10.1016/j.healthpol.2023.104861] [Medline: 37399677]
39. Ganna A, Carracedo A, Christiansen CF, et al. The European Health Data Space can be a boost for research beyond borders. Nat Med. Nov 2024;30(11):3053-3056. [doi: 10.1038/s41591-024-03246-6] [Medline: 39266746]
40. Bouaynaya W, Cloarec J, Bidan M. European territorialization of digital sovereignty: towards strategic autonomy through coopetition [Article in French]. Manag Int. 2026;30(2):40-48. [doi: 10.59876/a-8jv2-9kyc]
41. Deslée A, Cloarec J. Safeguarding privacy: ethical considerations in data-driven marketing. In: Matosas-López L, editor. The Impact of Digitalization on Current Marketing Strategies. Emerald Publishing; 2024:147-161. [doi: 10.1108/9781837536863]
42. McCradden MD, Joshi S, Mazwi M, Anderson JA. Ethical limitations of algorithmic fairness solutions in health care machine learning. Lancet Digit Health. May 2020;2(5):e221-e223. [doi: 10.1016/S2589-7500(20)30065-0] [Medline: 33328054]
43. Baines R, Stevens S, Austin D, et al. Patient and public willingness to share personal health data for third-party or secondary uses: systematic review. J Med Internet Res. Mar 5, 2024;26:e50421. [doi: 10.2196/50421] [Medline: 38441944]
44. Fesl S, Lang C, Schmitt J, et al. Factors influencing patients' willingness to share their digital health data for primary and secondary use: a theory- and evidence-based overview of reviews. Digit Health. 2025;11:20552076251340254. [doi: 10.1177/20552076251340254] [Medline: 40599675]
45. Price WN 2nd, Cohen IG. Privacy in the age of medical big data. Nat Med. Jan 2019;25(1):37-43. [doi: 10.1038/s41591-018-0272-7] [Medline: 30617331]
46. Mello MM, Rose S. Denial-artificial intelligence tools and health insurance coverage decisions. JAMA Health Forum. Mar 1, 2024;5(3):e240622. [doi: 10.1001/jamahealthforum.2024.0622] [Medline: 38451493]

Abbreviations

EHDS: European Health Data Space
EHR: electronic health record
EU: European Union
GDPR: General Data Protection Regulation

Edited by Guy Tsafnat; peer-reviewed by Baby Satravada, Lavanya Ramnath, Niklas von Kalckreuth; submitted 08.Mar.2026; final revised version received 16.Sep.2026; accepted 24.Sep.2026; published 27.Oct.2026

Please cite as:
Ducret M, Cloarec J, Alrabie N, Mouncif-Moungache M
The Personalization-Privacy Paradox in AI-Enabled Health Care: Managing Trust and Governance Under the European Health Data Space
J Med Internet Res 2026;28:e94903
URL: https://www.jmir.org/2026/1/e94903
doi: 10.2196/94903

© Maxime Ducret, Julien Cloarec, Nour Alrabie, Mouna Mouncif-Moungache. Originally published in the Journal of Medical Internet Research (https://www.jmir.org), 27.Oct.2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in the Journal of Medical Internet Research (ISSN 1438-8871), is properly cited. The complete bibliographic information, a link to the original publication on https://www.jmir.org/, as well as this copyright and license information must be included.