Secondary Use of Health Data for Training Generative AI Models

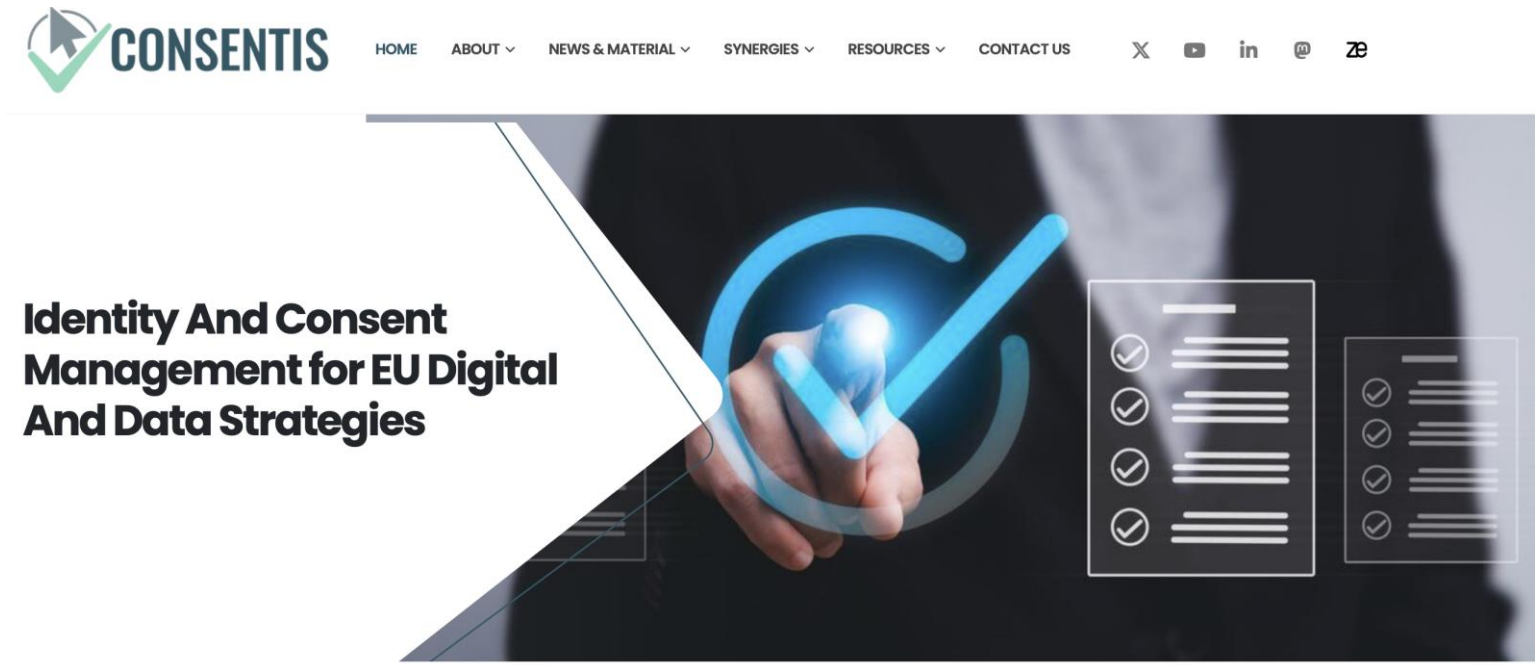
Risks and Interplay between the EHDS and the AI Act

Giovana Peluso Lopes

Postdoctoral Researcher on Fundamental Rights and Artificial Intelligence

3rd International Conference EHDS 2026 24 March 2026

Tilburg Institute for Law, Technology, and Society



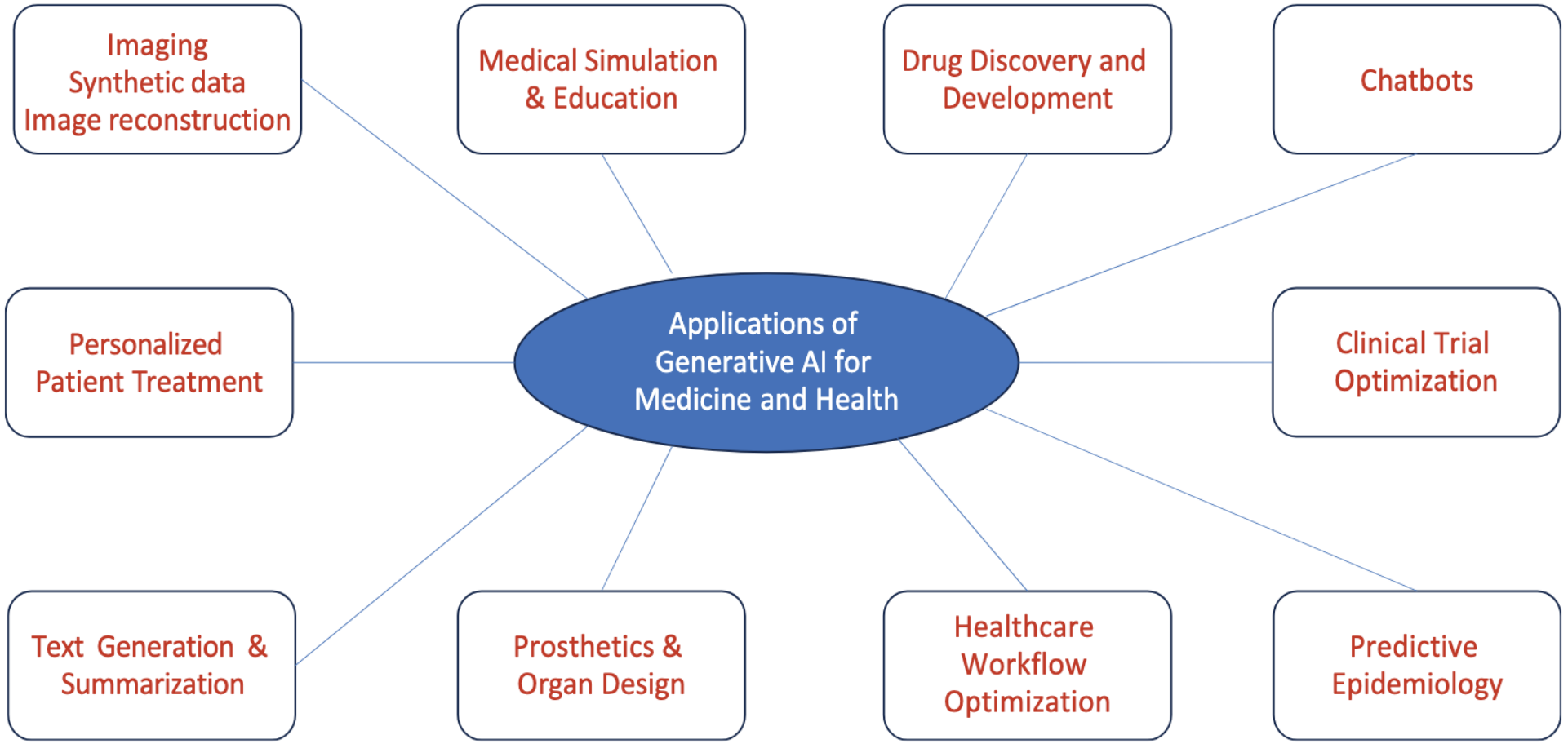
https://consentis-project.eu

This project received funding under Grant Agreement No 101168011, and is supported by the European Cybersecurity Competence Centre

CONSENTIS

TILBURG UNIVERSITY

Generative AI in Healthcare



Source: Chatterjee et al. 2024

CONSENTIS

Tilburg Institute for Law, Technology, and Society

Generative AI in Healthcare

- **Healthcare Chatbots:**
  - Symptom Checking/Triage
  - Patient Self-Management and Monitoring
  - Diagnosis Support
  - Mental Health and Well-being
  - Administrative Uses

Source: olya osyunina/Shutterstock.com

CONSENTIS

Tilt
Tilburg Institute for Law, Technology, and Society

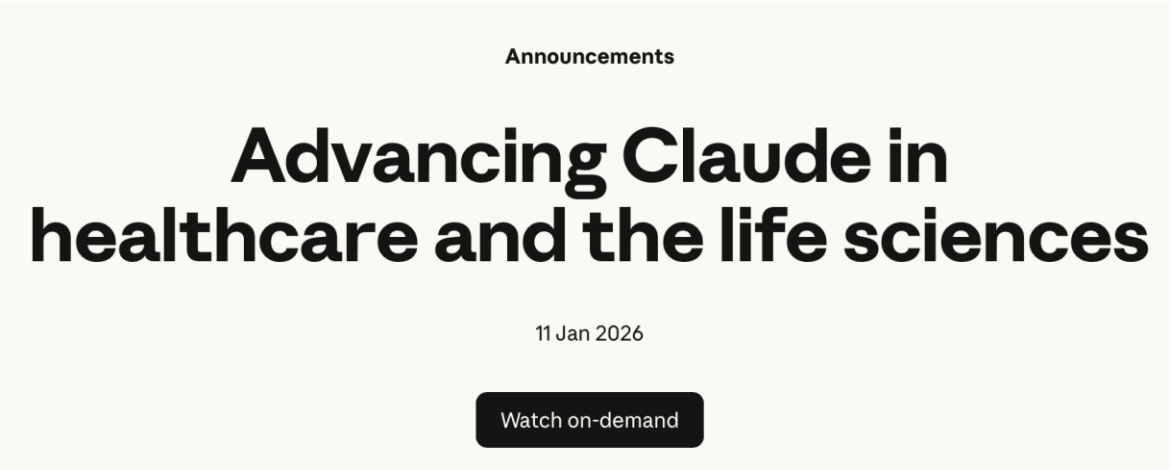
Generative AI in Healthcare

January 7, 2026 Product Company

Introducing ChatGPT Health

A dedicated experience in ChatGPT designed for health and wellness.

Source: Open AI



Source: Anthropic

CONSENTIS

Tilburg Institute for Law, Technology, and Society

Risks of Generative AI in Healthcare

REVIEW

Addressing 6 challenges in generative AI for digital health: A scoping review

Tara Templin[1,2]*, **Monika W. Perez**[3], **Sean Sylvia**[2,4,5], **Jeff Leek**[6,7], **Nasa Sinnott-Armstrong**[3,8]

1 Department of Health Policy and Management, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina, United States of America, **2** Carolina Population Center, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina, United States of America, **3** Department of Genome Sciences, University of Washington, Seattle, Washington, United States of America, **4** Department of Health Policy and Management, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina, United States of America, **5** Sheps Center for Health Services Research, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina, United States of America, **6** Biostatistics Program, Fred Hutchinson Cancer Center, Seattle, Washington, United States of America, **7** Department of Biostatistics, University of Washington, Seattle, Washington, United States of America, **8** Herbold Computational Biology Program, Fred Hutchinson Cancer Center, Seattle, Washington, United States of America

* ttemplin@unc.edu

Abstract

Generative artificial intelligence (AI) can exhibit biases, compromise data privacy, misinterpret prompts that are adversarial attacks, and produce hallucinations. Despite the potential of generative AI for many applications in digital health, practitioners must understand these tools and their limitations. This scoping review pays particular attention to the challenges with generative AI technologies in medical settings and surveys potential solutions. Using PubMed, we identified a total of 120 articles published by March 2024, which reference and evaluate generative AI in medicine, from which we synthesized themes and suggestions for future work. After first discussing general background on generative AI, we focus on collecting and presenting 6 challenges key for digital health practitioners and specific measures that can be taken to mitigate these challenges. Overall, bias, privacy, hallucination, and regulatory compliance were frequently considered, while other concerns around generative AI, such as overreliance on text models, adversarial misprompting, and jailbreaking, are not commonly evaluated in the current literature.

An Investigation of Memorization Risk in Healthcare Foundation Models

Sana Tonekaboni, Lena Stempfle, Adibvafa Fallahpour, Walter Gerych, Marzyeh Ghassemi

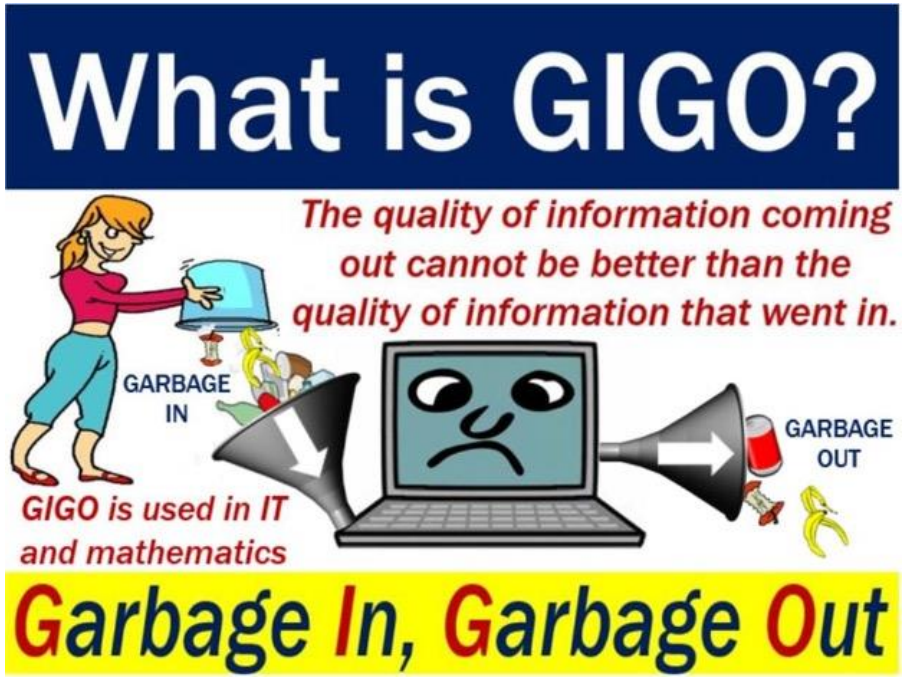
Foundation models trained on large-scale de-identified electronic health records (EHRs) hold promise for clinical applications. However, their capacity to memorize patient information raises important privacy concerns. In this work, we introduce a suite of black-box evaluation tests to assess privacy-related memorization risks in foundation models trained on structured EHR data. Our framework includes methods for probing memorization at both the embedding and generative levels, and aims to distinguish between model generalization and harmful memorization in clinically relevant settings. We contextualize memorization in terms of its potential to compromise patient privacy, particularly for vulnerable subgroups. We validate our approach on a publicly available EHR foundation model and release an open-source toolkit to facilitate reproducible and collaborative privacy assessments in healthcare AI.

Medical Hallucinations in Foundation Models and Their Impact on Healthcare

Yubin Kim, Hyewon Jeong, Shan Chen, Shuyue Stella Li, Chanwoo Park, Mingyu Lu, Kumail Alhamoud, Jimin Mun, Cristina Grau, Minseok Jung, Rodrigo Gameiro, Lizhou Fan, Eugene Park, Tristan Lin, Joonsik Yoon, Wonjin Yoon, Maarten Sap, Yulia Tsvetkov, Paul Liang, Xuhai Xu, Xin Liu, Chunjong Park, Hyeonhoon Lee, Hae Won Park, Daniel McDuff, Samir Tulebaev, Cynthia Breazeal

Hallucinations in foundation models arise from autoregressive training objectives that prioritize token-likelihood optimization over epistemic accuracy, fostering overconfidence and poorly calibrated uncertainty. We define medical hallucination as any model-generated output that is factually incorrect, logically inconsistent, or unsupported by authoritative clinical evidence in ways that could alter clinical decisions. We evaluated 11 foundation models (7 general-purpose, 4 medical-specialized) across seven medical hallucination tasks spanning

GIGO Effect and the need for high-quality data



Source: Medium

SECONDARY USE FOR ALGORITHMIC TRAINING IN THE EHDS

Article 53

Purposes for which electronic health data can be processed for secondary use

1. Health data access bodies shall only grant access to electronic health data referred to in Article 51 for secondary use to a health data user where the processing of the data by that health data user is necessary for one of the following purposes:

(e) scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators, including:

(ii) training, testing and evaluation of algorithms, including in medical devices, *in vitro* diagnostic medical devices, AI systems and digital health applications;

(61) The secondary use of health data under the EHDS should enable public, private and not-for-profit entities, as well as individual researchers, to have access to health data for research, innovation, policymaking, educational activities, patient safety, regulatory activities or personalised medicine, in line with the purposes as set out in this Regulation. Access to data for secondary use should contribute to the general interest of society. In particular, the secondary use of health data for research and development purposes remains at all times the supervisor of those activities. The provision of the data should also support activities related to scientific research. The notion of scientific research purposes should be interpreted in a broad manner, including technological development and demonstration, fundamental research, applied research and privately funded research. Activities related to scientific research include innovation activities such as training of AI algorithms that could be used in healthcare or the care of natural persons, as well as the evaluation and further development of existing algorithms and products for such purposes. It is necessary that the

EHDS Data Quality Framework

Article 78

Data quality and utility label

1. Datasets made available through health data access bodies may have a Union data quality and utility label applied by the health data holders.

2. Datasets with electronic health data collected and processed with the support of Union or national public funding shall have a data quality and utility label covering the elements set out in paragraph 3.

3. The data quality and utility label shall cover the following elements, where applicable:

(a) for data documentation: metadata, support documentation, the data dictionary, the format and standards used, the source of the data and, where applicable, the data model;

(b) for assessment of technical quality: the completeness, uniqueness, accuracy, validity, timeliness and consistency of the data;

(c) for data quality management processes: the level of maturity of the data quality management processes, including review and audit processes, and bias examination;

(d) for assessment of coverage: the period, population coverage and, where applicable, representativity of the population sampled, and the average timeframe in which a natural person appears in a dataset;

(e) for information on access and provision: the time between the collection of the electronic health data and their addition to the dataset and the time needed to provide electronic health data following the issuing of a data permit or a health data request approval;

(f) for information on data modifications: merging and adding data to an existing dataset, including links with other datasets.

6. By 26 March 2027, the Commission shall, by means of implementing acts, set out the visual characteristics and technical specifications of the data quality and utility label, based on the elements referred to in paragraph 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2) of this Regulation. Those implementing acts shall take into account the requirements in Article 10 of Regulation (EU) 2024/1689 and any adopted common specifications or harmonised standards supporting those requirements, where applicable.

AI Act Data Governance Framework

Article 10

Data and data governance

1. High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.

2. Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

(a) the relevant design choices;

(b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;

(c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

(d) the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;

(e) an assessment of the availability, quantity and suitability of the data sets that are needed;

(f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;

(g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);

(h) the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

3. Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof.

4. Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used.

5. To the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems in accordance with paragraph (2), points (f) and (g) of this Article, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the provisions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, all the following conditions must be met in order for such processing to occur:

AI Act Data Governance Framework

Article 53

Obligations for providers of general-purpose AI models

1. Providers of general-purpose AI models shall:

(a) draw up and keep up-to-date the technical documentation of the model, including its training and testing process and the results of its evaluation, which shall contain, at a minimum, the information set out in Annex XI for the purpose of providing it, upon request, to the AI Office and the national competent authorities;

(b) draw up, keep up-to-date and make available information and documentation to providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. Without prejudice to the need to observe and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law, the information and documentation shall:

(i) enable providers of AI systems to have a good understanding of the capabilities and limitations of the general-purpose AI model and to comply with their obligations pursuant to this Regulation; and

(ii) contain, at a minimum, the elements set out in Annex XII;

(c) put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790;

(d) draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office.

Obligations of providers of general-purpose AI models with systemic risk

1. In addition to the obligations listed in Articles 53 and 54, providers of general-purpose AI models with systemic risk shall:

(a) perform model evaluation in accordance with standardised protocols and tools reflecting the state of the art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks;

(b) assess and mitigate possible systemic risks at Union level, including their sources, that may stem from the development, the placing on the market, or the use of general-purpose AI models with systemic risk;

(c) keep track of, document, and report, without undue delay, to the AI Office and, as appropriate, to national competent authorities, relevant information about serious incidents and possible corrective measures to address them;

(d) ensure an adequate level of cybersecurity protection for the general-purpose AI model with systemic risk and the physical infrastructure of the model.

Challenges and Future Research

- Voluntary adoption of "Data Quality and Utility Label" risks lack of data harmonisation – mandatory adoption?
  - Limited obligations placed by the EHDS on data holders of data sets regarding the structural and semantic representation of the data (i.e., the use of interoperability standards)
  - Different data entry practices across medical facilities can lead to inconsistencies in datasets
  - Lack of incentives to ensure appropriate data quality
- Need for "relevant, sufficiently representative (…), free of errors and complete" datasets under the AI Act might encounter a barrier in the EHDS opt-out mechanism
  - Particularly given the lack of granularity and (lack of) public awareness/trust
- Possible disconnect between EHDS and AI Act regulatory frameworks: organisations might receive theoretical permission to process sensitive data for bias mitigation under the AI Act while simultaneously finding themselves restricted from accessing that same information under the EHDS

CONSENTIS

Tilburg Institute for Law, Technology, and Society

Thank you for your attention!

Giovana Peluso Lopes
g.lopes@tilburguniversity.edu

References

Anthropic. Advancing Claude in healthcare and the life sciences, 11 Jan. 2026. Available at: https://www.anthropic.com/news/healthcare-life-sciences, last accessed on 27 Jan. 2026.

Ayers J.W., A. Poliak, M. Dredze, et al. Comparing Physician and Artificial Intelligence Chatbot Responses to Patient Questions Posted to a Public Social Media Forum. JAMA Intern Med. 2023, 183(6): 589-596. doi:10.1001/jamainternmed.2023.1838.

Chatterjee, Samir, Ann Fruhling, Kathy Kotiadis, and Daniel Gartner. 2024. "Towards New Frontiers of Healthcare Systems Research Using Artificial Intelligence and Generative AI." *Health Systems* 13 (4): 263–73. https://doi.org/10.1080/20476965.2024.2402128.

Doğan, Fatma Sümeyra. 2025. "Balancing Bias Mitigation and Data Protection in AI-Driven Healthcare: Insights from the European Health Data Space, AI Act and GDPR." *University of Vienna Law Review* 9 (3): 99–123. https://doi.org/10.25365/vlr-2025-9-3-99.

Drumpt, Sarah van, Kartik Chawla, Tom Barbereau, Dayana Spagnuelo, and Linda van de Burgwal. 2025. "Secondary Use under the European Health Data Space: Setting the Scene and towards a Research Agenda on Privacy-Enhancing Technologies." *Frontiers in Digital Health* 7 (June). https://doi.org/10.3389/fdgth.2025.1602101.

Kalra, Dipak, Eva Sabajova, Birgit Bauer, Dmitry Etin, and Henrique Martins. 2025. "AI Needs High-Quality Health Data at Scale - Will the EHDS Deliver?" *Journal of Applied Interdisciplinary Research*, no. Special Issue (November): 116–18. https://doi.org/10.25929/d5p2-np32.

Kim, Yubin, Hyewon Jeong, Shan Chen, et al. 2025. "Medical Hallucinations in Foundation Models and Their Impact on Healthcare." arXiv:2503.05777. Preprint, arXiv, November 2. https://doi.org/10.48550/arXiv.2503.05777.

OpenAI. Introducing ChatGPT Health: A dedicated experience in ChatGPT designed for health and wellness, 7 Jan. 2026. Available at: https://openai.com/index/introducing-chatgpt-health, last accessed on 27 Jan. 2026.

Richdale, Kelly. 2025. "AI in Healthcare: Exploring the Opportunities, Risks, and Challenges." In *The Oxford Handbook of the Foundations and Regulation of Generative AI*, edited by Philipp Hacker, Andreas Engel, Sarah Hammer, and Brent Mittelstadt. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198940272.013.0031.

Templin, Tara, Monika W. Perez, Sean Sylvia, Jeff Leek, and Nasa Sinnott-Armstrong. 2024. "Addressing 6 Challenges in Generative AI for Digital Health: A Scoping Review." *PLOS Digital Health* 3 (5): e0000503. https://doi.org/10.1371/journal.pdig.0000503.

Tonekaboni, Sana, Lena Stempfle, Adibvafa Fallahpour, Walter Gerych, and Marzyeh Ghassemi. 2025. "An Investigation of Memorization Risk in Healthcare Foundation Models." arXiv:2510.12950. Preprint, arXiv, October 14. https://doi.org/10.48550/arXiv.2510.12950.

Yao, Xuxin, Zheyuan Sun, and Hongjie Man. 2026. "Balancing Scientific and Commercial Interests: The European Health Data Space Response to Commercial Scientific Research." *INQUIRY: The Journal of Health Care Organization, Provision, and Financing* 63 (March): 00469580261420714. https://doi.org/10.1177/00469580261420714.