Please cite as: van Kolfschooten, H. & Petročnik, T. 'Emerging Shadow Health Systems: Regulating Health-Focused Generative AI Chatbots from a European perspective' (*Zenodo* 2026) doi:10.5281/zenodo.19094764

Emerging Shadow Health Systems: Regulating Health-Focused Generative AI Chatbots from a European perspective

Hannah van Kolfschooten,[1*] Tjaša Petročnik[2]
[1] Centre for Life Sciences Law, Faculty of Law, University of Basel, Switzerland (CH)
[2] Tilburg Institute for Law, Technology, and Society, Faculty of Law, Tilburg University (NL)

*** Correspondence:**
Hannah van Kolfschooten, hannah.vankolfschooten@unibas.ch

Keywords: generative AI, health chatbots, digital public health, health equity, AI regulation, ChatGPT, ChatGPT Health, health law

Abstract

- **ChatGPT Health and other health-focused generative AI chatbots increasingly function as alternative first points of contact that may mediate - and in some cases substitute - engagement with regulated healthcare systems.**
- **At scale, these systems can shape care-seeking behavior, system capacity, trust in clinical expertise, and health equity.**
- **We describe this development as the emergence of shadow health systems: privately governed infrastructures that perform health-system functions without being subject to healthcare-specific safeguards.**
- **EU law currently regulates such tools based on declared medical purpose rather than their real-world effects, creating gaps in legal protection.**
- **We propose the adoption of stronger consumer and health data safeguards alongside extension of the scope of the Medical Devices Regulation and AI Act.**

1. Introduction

Consumer-facing artificial intelligence (AI) chatbots are rapidly becoming a primary interface through which individuals seek and act upon health information. OpenAI reports that more than 230 million people ask ChatGPT health-related questions each week,1 on topics such as diagnosis,2 medical treatment,3 medication,4 and wellbeing and lifestyle issues.5 In January 2026, OpenAI launched ChatGPT Health in the United States (US), a health-focused addition to its generative AI chatbot designed to integrate users' personal health data and generate personalized insights. Similar initiatives by competitors such as Anthropic and Google's Fitbit further indicate a growing market interest in generative AI chatbots for personal health-related use.6

1 OpenAI. (2026). Introducing ChatGPT Health. https://openai.com/sl-SI/index/introducing-chatgpt-health/ [Accessed January 15, 2026].
2 Ayre, J., Cvejic, E., McCaffery, K.J. (2025). Use of ChatGPT to obtain health information in Australia, 2024: insights from a nationally representative survey. Med. J. Aust. 222, 210–212. doi: 10.5694/mja2.52598.
3 Scaff, S.P.S., Reis, F.J.J., Ferreira, G.E., Jacob, M.F., Saragiotto, B.T. (2025). Assessing the performance of AI chatbots in answering patients' common questions about low back pain. Ann. Rheum. Dis. 84, 143–149. doi: 10.1136/ard-2024-226202.
4 Abanmy, N.O., Al-Ghreimil, N., Alsabhan, J.F., Al-Baity, H., Aljadeed, R. (2025). Evaluating the accuracy of ChatGPT in delivering patient instructions for medications: an exploratory case study. Front. Artif. Intell. 8:1550591. doi: 10.3389/frai.2025.1550591.
5 Luo, X., Ghosh, S., Tilley, J.L., Besada, P., Wang, J., and Xiang, Y. (2025). "Shaping ChatGPT into my digital therapist": a thematic analysis of social media discourse on using generative artificial intelligence for mental health. Digit. Health 11. doi: 10.1177/20552076251351088; Alanezi, F. (2024). Examining the role of ChatGPT in promoting health behaviors and lifestyle changes among cancer patients. Nutr. Health 31, 739–748. doi: 10.1177/02601060241244563.
6 Google. (2026). Fitbit Labs introduces a personal health coach. https://blog.google/products-and-platforms/devices/fitbit/personal-health-coach-public-preview/ [Accessed January 15, 2026]; Android Police. (2026). Fitbit Labs AI health records feature explained.

Please cite as: van Kolfschooten, H. & Petročnik, T. 'Emerging Shadow Health Systems: Regulating Health-Focused Generative AI Chatbots from a European perspective' (*Zenodo* 2026) doi:10.5281/zenodo.19094764

This development reflects a shift in how people engage with health information. By integrating longitudinal personal data into continuous conversational interfaces, these AI chatbots can function as alternative first points of contact that may mediate – and in some cases substitute for – engagement with regular healthcare pathways. They may influence whether, when, and how individuals access professional services, yet operate outside the legal, ethical, and institutional frameworks that govern formal healthcare.7 In doing so, they effectively constitute "shadow health systems": privately governed infrastructures that increasingly mediate – and sometimes substitute – engagement with regulated healthcare, without being embedded in corresponding legal and institutional safeguards. Although these tools are not yet available in the European Union (EU), the United Kingdom (UK), and Switzerland, their likely roll-out in the Europe raises pressing regulatory questions.

Against this backdrop, this Policy Brief examines the public health implications of a potential European launch of ChatGPT Health and comparable health-focused generative AI chatbots through a regulatory lens. While these tools may reduce barriers to health information and care, thus fulfilling an important public health function, they also raise concrete concerns regarding safety, data governance, privacy, bias, accountability, and equity.8 These effects are structural: they extend beyond individual users and may shape population-level health outcomes.9 We outline how the current EU legal approach creates regulatory gaps and propose measures to align legal obligations with potential real-world effects of health-focused generative AI chatbots.

2. From ChatGPT to ChatGPT Health: What is New?

ChatGPT Health illustrates a broader shift in the role of generative AI chatbots in population health. Unlike general-purpose chatbots, which users may consult for health questions, it is designed specifically for health-related interaction and can connect to medical records and health applications to generate responses grounded in longitudinal personal data. As Table 1 shows, both tools rely on the same underlying model. The novelty of ChatGPT Health therefore lies not in the model itself but in its integration with personal health data infrastructures and its repositioning as a personalized health interface.

Table 1. Functional Differences Between General-Purpose ChatGPT and ChatGPT Health

Feature	ChatGPT (Standard)	ChatGPT Health
Purpose	General-purpose AI assistant across domains	Dedicated health & wellness environment within ChatGPT
Information Sources	Pre-trained model knowledge + user input in chat	Same pre-trained model + user input + optional connected medical records & health apps

https://www.androidpolice.com/fitbit-labs-ai-health-records [Accessed January 15, 2026]; Google Support. (2026). Fitbit Labs health records help page. https://support.google.com/fitbit/answer/16678124?hl=en [Accessed January 15, 2026].

7 Ozalp, H., et al. (2022). "Digital colonization" of highly regulated industries: an analysis of Big Tech platforms' entry into health care and education. Calif. Manage. Rev. 64, 78–101. doi: 10.1177/00081256221094307.

8 Kapsali, M.Z., et al. (2024). Ethical concerns about ChatGPT in healthcare: a useful tool or the tombstone of original and reflective thinking? Cureus 16:e54759. doi: 10.7759/cureus.54759.

9 Kraaijeveld, S.R., and Sharon, T. (2025). The increasing influence of Big Tech in health and medicine and the need for a public health ethics perspective. Public Health Ethics 18:phaf005. doi: 10.1093/phe/phaf005; Fernandez, J.A. (2023). A comparative analysis of privacy and humanitarian rights of citizens against data collection through artificial intelligence between the European Union and the United States: will ChatGPT own your data? J. Int. Law Comp. Stud. 1, 153. doi: 10.47191/ijsshr/v9-i2-32.

Please cite as: van Kolfschooten, H. & Petročnik, T. 'Emerging Shadow Health Systems: Regulating Health-Focused Generative AI Chatbots from a European perspective' (*Zenodo* 2026) doi:10.5281/zenodo.19094764

Personalization	Limited to what user types and saved memory (if enabled)	Grounded in structured, longitudinal personal health data (when connected)
Evaluation Approach	General cross-domain safety and quality testing	Health-specific evaluation framework (physician-informed, clinically aligned criteria - 'HealthBench')
Privacy Architecture	Standard ChatGPT privacy controls	Separate, isolated health space with enhanced encryption; health chats not used for model training
Regulatory Positioning	General AI assistant, not a medical device	Still not a medical device, but optimized for health-related support

These differences change the system's functional role. Integrating personal health data allows personalized health responses rather than providing general health information. Personalized outputs can shape how users interpret symptoms and make health-related decisions, while the system remains formally positioned as an informational tool. If individuals use these systems to seek health advice at scale, their significance extends beyond individual use to structural effects on public health and health system governance.

3. Public Health Implications of Health-Focused Generative AI Chatbots

By functioning as alternative first points of contact that may mediate – and in some cases substitute – engagement with regulated care, health-focused generative AI chatbots may reframe how individuals interpret symptoms, seek care, and whom they trust. This may lead to structural effects for public health.

First, when AI systems function as first points of contact with healthcare, they can reshape how and when patients access regulated services, with consequences for capacity and safety. If a chatbot frames mild symptoms as potentially serious, precautionary consultations may increase, adding pressure to already stretched primary and emergency care.10 Conversely, if serious symptoms are under-triaged, engagement with health services may be delayed, resulting in worse clinical outcomes or more costly interventions down the line.11 Both cases distort patient flows and misallocate healthcare resources,12 impacting healthcare systems' capacities to deal with actual health needs.

Second, AI chatbots may begin to shape not only access patterns but also epistemic authority in healthcare. Because chatbot responses are personalized and seem confident, users may rely on them as if they were clinical advice, even when providers disclaim to be providing medical advice.13 At the same time, recent research shows that AI chatbots prioritize being helpful over being accurate in medical contexts, which might produce convincing but false medical information or validate users' harmful health attitudes and behaviors.14 At scale, this can be detrimental for public health. Over time, this might also generate competing sources of authority: regulated clinical expertise on the one hand and privately governed AI

10 Babic, B., Gerke, S., Evgeniou, T., et al. (2021). Direct-to-consumer medical machine learning and artificial intelligence applications. Nat. Mach. Intell. 3, 283–287. doi: 10.1038/s42256-021-00331-0.

11 Ramaswamy, A., Tyagi, A., Hugo, H., Jiang, J., Jayaraman, P., Jangda, M., et al. (2026). ChatGPT Health performance in a structured test of triage recommendations. Nat. Med. doi: 10.1038/s41591-026-04297-7.

12 Babic, B., Gerke, S., Evgeniou, T., et al. (2021). Direct-to-consumer medical machine learning and artificial intelligence applications. Nat. Mach. Intell. 3, 283–287. doi: 10.1038/s42256-021-00331-0.

13 Kıyak, Y.S., Coşkun, Ö., Budakoğlu, I.İ. (2026). "ChatGPT can make mistakes" warnings fail: a randomized controlled trial. Med. Educ. 60, 138–142. doi: 10.1111/medu.70056.

14 Chen, S., Gao, M., Sasse, K., Hartvigsen, T., Anthony, B., Fan, L., et al. (2025). When helpfulness backfires: LLMs and the risk of false medical information due to sycophantic behavior. npj Digit. Med. 8:605. doi: 10.1038/s41746-025-02008-z.

advice on the other. Diverging advice might strain patient-doctor relationships, both due to accuracy disputes and due to AI actively shaping care expectations.15

Third, widespread use of AI chatbots reinforces a broader shift in how responsibility for health risks is allocated.16 By framing users as informed, autonomous decision-makers, such systems promote a model in which individuals are expected to manage their own health. Effectively, this not only relocates the burden of medical decision-making from regulated professionals to lay-users,17 but also shifts responsibility for health away from public services onto individuals.18 While access to health information is an essential part of care, it does not equate to access to health services, as users cannot be expected to understand complex medical information in the same manner as health professionals.20

Finally, the use of health-focused generative AI may result in a two-tiered system of care. For well-resourced individuals, AI advice can function as a preliminary step before seeking treatment. For individuals who lack adequate access to healthcare, AI systems may instead operate as substitutes for professional services.21 This asymmetry can reinforce health disparities, in particular if AI systems reproduce biases or perform unevenly across demographic groups, as those already facing barriers to care would be more exposed to misdiagnosis, under-triage, or over-reassurance.19 Because they also have fewer opportunities to verify or override AI outputs through subsequent consultation, errors are less likely to be corrected,20 resulting in a feedback dynamic in which unequal reliance and biased outputs interact to reinforce or deepen inequities in access, safety, and ultimately health outcomes.21

These dynamics present the core challenge of shadow health systems. The concern is not limited to unreliable or inaccurate outputs or advice inconsistent with clinical guidelines.22 Rather, widespread adoption of health-focused generative AI could gradually reroute health information flows through private infrastructures.23 This would give technology providers significant influence over how health information is interpreted, how care is accessed, and how risks are allocated. In doing so, they may reshape healthcare

15 Kerasidou, A., and Kerasidou, C. (2025). Epistemic authority and medical AI: epistemological differences and challenges in medical practice. Med. Health Care Philos. doi: 10.1007/s11019-025-10306-2; Gross, N. (2023). What ChatGPT tells us about gender: a cautionary tale about performativity and gender biases in AI. Soc. Sci. 12:435. doi: 10.3390/socsci12080435; Van Kolfschooten, H., and Gross, N. (2025). Invisible prescribers: the risks of Google's AI summaries. J. Med. Ethics Forum. https://blogs.bmj.com/medical-ethics/2025/11/12/invisible-prescribers-the-risks-of-googles-ai-summaries [Accessed February 15, 2026].

16 Erikainen, S., et al. (2019). Patienthood and participation in the digital era. Digit. Health 5:2055207619845546. doi: 10.1177/2055207619845546; Ricciardi, W., and Boccia, S. (2017). New challenges of public health: bringing the future of personalised healthcare into focus. Eur. J. Public Health 27, 36–39. doi: 10.1093/eurpub/ckx164.

17 Parth, S., Manoharan, B., Parthiban, R., Qureshi, I., Bhatt, B., and Rakshit, K. (2021). Digital technology-enabled transformative consumer responsibilisation: a case study. Eur. J. Mark. 55, 2538–2565. doi: 10.1108/EJM-02-2020-0139.

18 Erikainen, S., et al. (2019). Patienthood and participation in the digital era. Digit. Health 5:2055207619845546. doi: 10.1177/2055207619845546.

20 Gray, J., and Mertes, H. (2025). On misempowerment and mobile health. Med. Health Care Philos. 28:549. doi: 10.1007/s11019-025-10277-4.

21 Iloanusi, N.J., and Chun, S.A. (2024). AI impact on health equity for marginalized, racial, and ethnic minorities. In: Proceedings of the 25th Annual International Conference on Digital Government Research (DGO 2024), Taipei, Taiwan, June 11–14, 2024 (New York, NY: ACM), 1–8. doi: 10.1145/3657054.3657152.

19 Van Kolfschooten H. The AI cycle of health inequity and digital ageism: mitigating biases through the EU regulatory framework on medical devices. J Law Biosci. 2023;10(2):lsad031. doi:10.1093/jlb/lsad031; Iloanusi, N.J., Chun, S.A. (2024). AI impact on health equity for marginalized, racial, and ethnic minorities. Proc. 25th Annu. Int. Conf. Digital Gov. Res. (DGO 2024), Taipei, Taiwan, pp. 1–8. doi: 10.1145/3657054.3657152

20 Brown JEH, Halpern J. AI chatbots cannot replace human interactions in the pursuit of more inclusive mental healthcare. SSM Ment Health. 2021;1:100017. doi:10.1016/j.ssmmh.2021.100017.

21 Eichenberger, A., Thielke, S., and Van Buskirk, A. (2025). A case of bromism influenced by use of artificial intelligence. AIM Clin. Cases 4:e241260. doi: 10.7326/aimcc.2024.1260; Iloanusi, N.J., and Chun, S.A. (2024). AI impact on health equity for marginalized, racial, and ethnic minorities. In: Proceedings of the 25th Annual International Conference on Digital Government Research (DGO 2024), Taipei, Taiwan, June 11–14, 2024 (New York, NY: ACM), 1–8. doi: 10.1145/3657054.3657152.

22 Huisman, M., Joye, S., and Biltereyst, D. (2020). Searching for health: Doctor Google and the shifting dynamics of the middle-aged and older adult patient–physician relationship and interaction. J. Aging Health 32, 998–1011. doi: 10.1177/0898264319873809.

23 Erikainen, S., et al. (2019). Patienthood and participation in the digital era. Digit. Health 5:2055207619845546. doi: 10.1177/2055207619845546.

Please cite as: van Kolfschooten, H. & Petročnik, T. 'Emerging Shadow Health Systems: Regulating Health-Focused Generative AI Chatbots from a European perspective' (*Zenodo* 2026) doi:10.5281/zenodo.19094764

practices, challenge expertise, and deepen inequity without being subject to the same accountability mechanisms that apply to healthcare institutions and professionals.24

4. Gaps in EU Digital Health Regulation

These public health concerns are compounded by a structural legal mismatch. Systems such as ChatGPT Health blur the boundaries between medical and consumer technology, performing health-system functions without clearly falling under healthcare-specific safeguards. At the same time, the initial exclusion of EEA, UK, and Swiss users from early access to ChatGPT Health suggests that providers anticipate regulatory friction at exactly this grey area. Health-focused generative AI chatbots are thus not unregulated. Yet we contend they are governed by legal frameworks that are not suitable to address the public health risks identified above. This section examines how this misalignment arises across different areas of EU law.

4.1 Safety and Efficacy of Health Technologies

The first issue concerns safety and performance of health-focused generative AI chatbots. Under EU law, medical software is generally regulated under the Medical Devices Regulation (MDR). The MDR applies when the manufacturer *intends* software to have a medical purpose, for instance diagnosis or treatment. It explicitly excludes wellness and fitness apps from its scope.28 As a result, manufacturers can, through disclaimers and product descriptions, avoid application of the MDR by arguing that their product was not intended to have a medical function. This results in a regulatory asymmetry where tools performing similar functions may face different obligations, depending on the declared intended purpose.25

When an AI chatbot does qualify as a medical device, the MDR imposes various quality and safety rules, including clinical evaluation, quality and risk management systems, documentation, conformity assessments and post-market surveillance,26 safeguards developed precisely to address risks related to efficacy, quality and safety.27 This qualification is also decisive for the scope of application of the Artificial Intelligence Act (AI Act), which applies more stringent rules for AI systems deemed to pose higher risks. In general, medical device AI systems covered by the MDR are considered high-risk AI systems.28 This high-risk classification adds additional, and considerable, obligations related to risk management, bias

24 Sharon, T., and Gellert, R. (2024). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. Inf. Commun. Soc. 27, 2651–2667. doi: 10.1080/1369118X.2023.2246526; Taylor, L. (2021). Public actors without public values: legitimacy, domination and the regulation of the technology sector. Philos. Technol. 34, 897–922. doi: 10.1007/s13347-020-00441-4; Ozalp, H., et al. (2022). "Digital colonization" of highly regulated industries: an analysis of Big Tech platforms' entry into health care and education. Calif. Manage. Rev. 64, 78–101. doi: 10.1177/00081256221094307.

28 Medical Device Coordination Group (MDCG). (2025). MDCG 2019-11 Rev. 1: guidance on qualification and classification of software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR. Brussels: European Commission. https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf [Accessed February 10, 2026].

25 Van Kolfschooten, H. (2022). The mHealth power paradox: improving data protection in health apps through self-regulation in the European Union. In: Cohen, I.G., Minssen, T., Price, W.N. II, Robertson, C., and Shachar, C., eds. The future of medical device regulation: innovation and protection. Cambridge: Cambridge University Press, 63–76. doi: 10.1017/9781108975452.

26 Medical Device Coordination Group (MDCG). (2025). MDCG 2019-11 Rev. 1: guidance on qualification and classification of software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR. Brussels: European Commission. https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf [Accessed February 10, 2026].

27 Onitiu, D., Wachter, S., and Mittelstadt, B. (2024). How AI challenges the medical device regulation: patient safety, benefits, and intended uses. J. Law Biosci. lsae007. doi: 10.1093/jlb/lsae007.

28 Joint Artificial Intelligence Board and Medical Device Coordination Group. (2025). AIB 2025-1, MDCG 2025-6: interplay between the Medical Devices Regulation (MDR) and In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA). Brussels: European Commission. https://health.ec.europa.eu/document/download/b78a17d7-e3cd-4943-851d-e02a2f22bbb4_en [Accessed January 15, 2026].

mitigation, data governance, and documentation, specific to AI risks.29 Thus, if a health-focused generative AI system escapes the MDR qualification, it also avoids the rules for high-risk systems under the AI Act. This leaves only the AI Act's general-purpose AI regime applicable, which does not require a demonstration of clinical validity or real-world safety and efficacy.30 It does pose the obligation to inform users they are interacting with an AI system and not a human.31 Moreover, the prohibited risk regime will still be applicable, which prohibits purposefully manipulative and exploitative AI systems.32

This legal gap directly contributes to the public health risks outlined in the previous section. When health-focused AI chatbots operate outside medical device regulation, the responsibility for assessing the reliability of their advice effectively shifts to users.33 Transparency obligations and disclaimers offer limited protection, as repeated, personalized interaction with AI can create a sense of credibility that exceeds lay-users' ability to evaluate the quality of information.34 At the system level, such allocation of responsibility can lead to delays in seeking care or increased workload for healthcare personnel.[35] Moreover, avoiding high-risk classification under the AI Act also circumvents the (limited) anti-discrimination rules under the AI Act,[36] which may reinforce existing health disparities.

To close this gap, the European Commission could clarify that software processing clinical-grade health data and producing personalized health guidance is presumed to have a medical purpose under the MDR, unless explicitly demonstrated this is not the case. One pathway is adding these systems to Annex XVI of the MDR, which lists products without an intended medical purpose, to which the MDR nevertheless applies.37 Another pathway is to adopt a delegated act to add certain uses of health-focused AI to Annex III of the AI Act, bringing them under the high-risk regime without MDR classification.38

Yet, even when these rules do apply, they do little to address the distributive consequences of medical AI. These EU safety frameworks focus on technical performance, but largely ignore how AI adoption may differentially affect populations. To mitigate this, sector-specific safety regimes should require evaluations of medical AI systems that explicitly assess equity effects, ensuring that AI deployment does not entrench two-tiered healthcare systems.

4.2 Health Claims Without Accountability

The second gap concerns legal safeguards governing the accuracy and reliability of health information produced by health-focused generative AI chatbots. When medical devices laws do not apply, systems like ChatGPT Health primarily fall under general consumer protection frameworks that prohibit misleading,

29 Onitiu, D., Wachter, S., and Mittelstadt, B. (2024). How AI challenges the medical device regulation: patient safety, benefits, and intended uses. J. Law Biosci. lsae007. doi: 10.1093/jlb/lsae007.
30 Van Kolfschooten, H. (2023). The AI cycle of health inequity and digital ageism: mitigating biases through the EU regulatory framework on medical devices. J. Law Biosci. 10:lsad031. doi: 10.1093/jlb/lsad031.
31 See Article 50, AI Act.
32 Biber, E. (2025). A close reading of the European Commission's guidelines on prohibited artificial intelligence practices: a powerful reflection of the European approach to AI. J. AI Law Regul. 2, 266–273. doi: 10.21552/aire/2025/3/9; Van Kolfschooten, H. (2026). Prohibited AI practices in healthcare under the European Artificial Intelligence Act. J. Law Med. Ethics (forthcoming).
33 Wang, C., et al. (2023). Ethical considerations of using ChatGPT in health care. J. Med. Internet Res. 25:e48009. doi: 10.2196/48009.
34 Lim, J.E., Schaefer, O., and Savulescu, J. (2026). Critical engagement: the value of transparency of AI in healthcare. Philos. Technol. 39:1. doi: 10.1007/s13347-025-01009-w; Duffourc, M.N., Verhees, F.G., and Gilbert, S. (2025). Artificial intelligence characters are dangerous without legal guardrails. Nat. Hum. Behav. doi: 10.1038/s41562-025-02375-3.
35 Babic, B., Gerke, S., Evgeniou, T., et al. (2021). Direct-to-consumer medical machine learning and artificial intelligence applications. Nat. Mach. Intell. 3, 283–287. doi: 10.1038/s42256-021-00331-0.
36 Van Kolfschooten, H. (2023). The AI cycle of health inequity and digital ageism: mitigating biases through the EU regulatory framework on medical devices. J. Law Biosci. 10:lsad031. doi: 10.1093/jlb/lsad031.
37 Svempe, L. (2025). The regulatory landscape of health apps in the European Union. JIPITEC 16, 24.
38 See articles 7, 97 and Annex III, AI Act.

dangerous, or manipulative products or claims. However, these regimes are not designed to address the public health risks that arise when AI systems begin to function as sources of health advice.

For example, under the General Product Safety Regulation (GPSR), the safety of digitally connected products must be assessed against relevant standards, certification schemes, or good practices, including risks to health. However, these standards are not (yet) developed for AI chatbots, especially in the health domain.39 EU consumer law may also address misleading medical-like claims, omissions, or manipulative interface design, but this regime primarily protects consumers' economic interests rather than public health considerations. The Digital Services Act (DSA) provides another potential avenue for protection by regulating systemic misinformation risks, including to health, by imposing risk mitigation obligations on very large online platforms. However, ChatGPT currently falls outside of the scope of the DSA's most stringent obligations.40

The public health concern therefore lies not merely in the possibility that users may receive incorrect information, but in the structural positioning of these systems as stand-ins for regulated care. By presenting personalized outputs that resemble clinical advice, AI chatbots can acquire an aura of medical authority without being subject to healthcare laws or standards of clinical validation. Consumer law offers limited tools to address this transition of epistemic authority in healthcare, as it does not – for example – require providers to systematically correct medically incorrect assumptions or demonstrate ex ante clinical validation.41 Again, this shifts the responsibility for assessing the reliability of their advice to users.

To address this gap, harmonized standards under the GPSR should be developed specifically for health-focused generative AI chatbots,42 requiring demonstrable performance against clinically relevant quality benchmarks. In parallel, the planned modification of the consumer law regime (including the Digital Fairness Act) should clarify that presenting personalized health outputs in a manner that creates a reasonable impression of clinical reliability without adequate validation constitutes a misleading practice.43

4.3 The Protection of Health Data

Lastly, deficiencies in EU's data governance are particularly relevant because ChatGPT Health's central functionality lies in linking health data across contexts. As discussed in Section 3, these AI systems operate not only through advice but also through the data infrastructures that collect, aggregate, and repurpose health data outside regulated care settings. This raises important questions about health data protection. Transferring data from clinical contexts into privately-run AI systems may create privacy risks because the norms and expectations governing data flows in these contexts differ substantially.44 In regulated healthcare settings, providers are bound by ethical and professional duties such as medical confidentiality, therapeutic-purpose limitations, and public interest obligations, that constrain how health data may be used. In contrast, the processing of health data within generative AI chatbots is primarily governed by contractual terms and consent requirements under the General Data Protection Regulation (GDPR). Although the GDPR provides enhanced protection for health data, reliance on (informed) consent as the

39 Duffourc, M.N., Verhees, F.G., and Gilbert, S. (2025). Artificial intelligence characters are dangerous without legal guardrails. Nat. Hum. Behav. doi: 10.1038/s41562-025-02375-3.

40 Jahangir, R. (2025). EU weighs regulating OpenAI's ChatGPT under the DSA. What does that mean? Tech Policy Press. https://www.techpolicy.press/eu-weighs-regulating-openais-chatgpt-under-the-dsa-what-does-that-mean/ [Accessed March 10, 2026].

41 Bean, A.M., Payne, R.E., Parsons, G., et al. (2026). Reliability of LLMs as medical assistants for the general public: a randomized preregistered study. Nat. Med. doi: 10.1038/s41591-025-04074-y.

42 Duffourc, M.N., Verhees, F.G., and Gilbert, S. (2025). Artificial intelligence characters are dangerous without legal guardrails. Nat. Hum. Behav. doi: 10.1038/s41562-025-02375-3.

43 Van Kolfschooten, H. (2025). Addictive algorithms and the Digital Fairness Act: a new chapter in EU public health policy? Bill of Health. https://petrieflom.law.harvard.edu/2025/08/20/addictive-algorithms-and-the-digital-fairness-act-a-new-chapter-in-eu-public-health-policy/ [Accessed March 10, 2026].

44 Nissenbaum, H. (2004). Privacy as contextual integrity. Wash. Law Rev. 79, 119–157.

Please cite as: van Kolfschooten, H. & Petročnik, T. 'Emerging Shadow Health Systems: Regulating Health-Focused Generative AI Chatbots from a European perspective' (*Zenodo* 2026) doi:10.5281/zenodo.19094764

main legal basis for integrating health data is problematic. As previously discussed, public health implications extend beyond the individual user, yet individuals are made responsible to decide on collective dimensions of data processing.45 Considering the inability of platform's privacy policies to meaningfully address relevant information asymmetries,46 expecting users to make these informed decisions is misguided.

Further, because ChatGPT Health processes highly sensitive personal data, serious risks may arise regarding data breaches and further commercial use of such data.47 Although OpenAI states data security is a priority and claims that health data processed through ChatGPT Health will not be used to further train its AI models, the trustworthiness (and enforceability) of such claims remains uncertain. Furthermore, even if these systems comply formally with existing data protection rules, this does not resolve the public health issues identified above. By mediating healthcare practices and aggregating health data within privately governed infrastructures, these systems may redirect both informational and economic value toward private providers. As a result, any benefits generated from processing health data may be channeled towards companies like OpenAI, rather than returning to the public healthcare systems from which much of this data originated.48

To remedy these regulatory limitations, EU regulators should clarify that large-scale aggregation of health data and medical records within generative AI advice systems triggers safeguards beyond GDPR compliance. In particular, stricter limits should apply to the secondary use of such data for AI training and model improvement, alongside reinforced data minimization requirements considering the longitudinal integration of health data across contexts. These safeguards should aim to reflect institutional data safeguards in formal healthcare settings. Closer cooperation between data protection and health authorities should also become the norm, reflecting the hybrid nature of these systems as both digital services and quasi-health infrastructures.

Moreover, the data protection framework should clearly establish that health data collected through AI chatbots for the purpose of providing health advice cannot be repurposed for AI training and development unless users are presented with a separate, explicit, and granular choice that enables genuinely informed consent. 49 Such safeguards are particularly important in light of ongoing policy initiatives that may broaden the lawful bases for data reuse in the name of innovation and regulatory simplification. 50 Finally, given that the large-scale processing of health data may generate significant economic value for private providers, policymakers should also consider benefit-sharing mechanisms (including targeted taxation or data value return schemes) to ensure that value derived from health data ultimately flows back to the public systems from which much of this data originates.51

45 Graef, I., Petročnik, T., and Tombal, T. (2023). Conceptualizing autonomy in an era of collective data processing: from theory to practice. Digit. Soc. 2:19.

46 Hriscu, A.M., and Kosta, E. (2025). Fit for purpose? The role of consent in EU data protection law in light of very large online platforms' processing of personal data. In: Van der Sloot, B., Monti, G., and Bostoen, F., eds. From regulating human behaviour to regulating data. Tilburg: Open Press Tilburg University, 99–129.

47 Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Med. Ethics 22:122. doi: 10.1186/s12910-021-00687-3.

48 Sharon, T., and Gellert, R. (2024). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. Inf. Commun. Soc. 27, 2651–2667. doi: 10.1080/1369118X.2023.2246526.

49 Gilbert, S., et al. (2024). Citizen data sovereignty is key to wearables and wellness data reuse for the common good. npj Digit. Med. 7:27. doi: 10.1038/s41746-024-01004-z.

50 Domínguez de Olazábal, I. (2025). The EU's digital omnibus must be rejected by lawmakers. Here is why. Tech Policy Press. https://www.techpolicy.press/the-eus-digital-omnibus-must-be-rejected-by-lawmakers-here-is-why/ [Accessed March 10, 2026].

51 El-Sayed, S., Kickbusch, I., and Prainsack, B. (2025). Data solidarity: operationalising public value through a digital tool. Glob. Public Health 20:2450403. doi: 10.1080/17441692.2025.2450403.

5. Conclusion and the Road Ahead

This paper has argued that health-focused generative AI chatbots such as ChatGPT Health give rise to what we describe as shadow health systems: privately governed infrastructures that increasingly mediate – and sometimes substitute – engagement with regulated healthcare, without being embedded in corresponding legal and institutional safeguards. By shaping symptom interpretation, triage decisions, care-seeking behavior, and access pathways, these systems can influence healthcare utilization, redistribute responsibility to individuals, and reinforce structural inequities. Yet, EU law is unequipped to address their real-world function and systemic effects. As a result, tools that perform health-system roles can avoid health technology-specific obligations, while remaining governed mainly by consumer and data protection frameworks that are not designed to ensure clinical reliability, equity monitoring, or institutional accountability. If these gaps persist, shadow health systems may become embedded in everyday practice while their power to affect public health remains unchecked.

The regulatory objective should therefore not be to prohibit consumer-facing health AI, but to align legal obligations with functional impact. Where AI systems operate as personalized health advisors at scale, they should be subject to proportionate duties of safety validation, transparency, equity monitoring, and accountability, irrespective of disclaimers or formal product labels. This requires clarifying medical device presumptions, extending high-risk designations where appropriate, developing harmonized safety standards for conversational health AI, and strengthening the limits on health data reuse. More fundamentally, it requires recognizing that health-focused generative AI chatbots are a matter of public health governance, not merely product regulation,52 necessitating the activities of their providers are transparent, justifiable to the public, and contestable.53 Ensuring that these emerging infrastructures are aligned with principles of universality, equity, and solidarity is thus essential to preserving a "distinctly European" approach to healthcare.54

Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Author Contributions

HvK: Writing – original draft; Writing – review & editing; Investigation; Conceptualization. TP: Writing – original draft; Writing – review & editing; Investigation.

Funding

HvK received no funding for this research. TP received no funding for this research.

Supplementary Material

Not applicable.

Data Availability Statement

Not applicable.

52 Sharon, T., and Gellert, R. (2024). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. Inf. Commun. Soc. 27, 2651–2667. doi: 10.1080/1369118X.2023.2246526.

53 Taylor, L. (2021). Public actors without public values: legitimacy, domination and the regulation of the technology sector. Philos. Technol. 34, 897–922. doi: 10.1007/s13347-020-00441-4.

54 Frischhut, M., et al. (2026). 20 years of EU health values (2006–2026): four proposals for the future. Lancet Reg. Health Eur. 61:101589. doi: 10.1016/j.lanepe.2026.101589.