ISSUE BRIEF | May 2026 | IB/202605/002

Click here for more publications

IMHO Keshav Desiraju INDIA MENTAL HEALTH OBSERVATORY

Delving into Digital Mental Health: Part 4

Ethics of digital mental health

AUTHORS
Ramya Pillutla and Ruhi Borah

ACKNOWLEDGMENTS
Tanya Fernandes, Sonali Kumar, Sayali Mahashur

CMH Centre for Mental Health Law & Policy
ILS

Introduction

The rapid growth of digital mental health (DMH) applications offers promising solutions to address mental health challenges in India. However, these apps target vulnerable populations who might be in significant distress, with increased risk of worsening mental health through apps that are not evidence-based, and potential exposure to high levels of stigma and discrimination if sensitive data is leaked. This makes it essential that safeguards are in place. Safeguarding could take two complementary forms: regulation and the promotion of best practices or ethical guidelines.

Laws and regulatory bodies for digital mental health apps, while important, may be insufficient considering:

- Mental health apps see rapid innovation and development; they evolve quickly, beyond what regulatory frameworks can keep up with.
- There is a wide range of apps with varied functionality and risk. Apps range from wellness tools to those making clinical claims, requiring different levels of scrutiny that would be hard to account for through regulations.
- Legal requirements, even if developed, would be limited, cannot cover every aspect of the development of apps, and cannot promote ethical and responsible decision-making.
- Legal requirements come with the need for oversight – a concern in India, where regulatory bodies often do not function in a timely manner and face challenges related to funding.

Safeguarding users from harm by promoting person-centric and ethical practices is more likely to ensure that care through these apps is delivered responsibly, fairly, and with respect for users' rights and best interests. Ethics-based best practices also provide a more practical and consistent framework that can be continually refined over time to guide digital mental health applications.

Need for a multi-disciplinary framework

Developing an ethical framework for digital mental health focused on identifying safeguards and best practices requires a multidisciplinary approach, as it involves a complex interplay of medical, technological, and social considerations.

This brief aims to explore the field of digital mental health ethics based on existing literature in key fields adjacent to digital mental health and lay out a framework that can be used to develop ethical guidelines for digital mental health.

The framework rests on a combination of person-centred medical ethics; the broader societal considerations of bioethics; ethics related to artificial intelligence, which many apps are based on; and specific issues related to digital health and digital mental health. This is the fourth brief in the Delving into Digital Mental Health series.

Why are these fields relevant?

Bioethics takes a broad view of the societal implications of fields related to biological advances. Two aspects of bioethics, medical ethics and public health ethics, are relevant to DMH.

Medical ethics is the foundation on which DMH ethics rest. DMH, at its core, is a form of healthcare. Principles such as beneficence (benefiting the user), non-maleficence (not causing harm), and autonomy are critical aspects to be considered for DMH ethics.

Public health ethics, in the context of DMH, lays the groundwork for ethics from the perspective of the good of society, including principles related to bias, access, and equity.

While DMH apps are not physical devices, they are medical devices and could draw from ethical principles of **medical devices** such as clinical effectiveness and transparency.

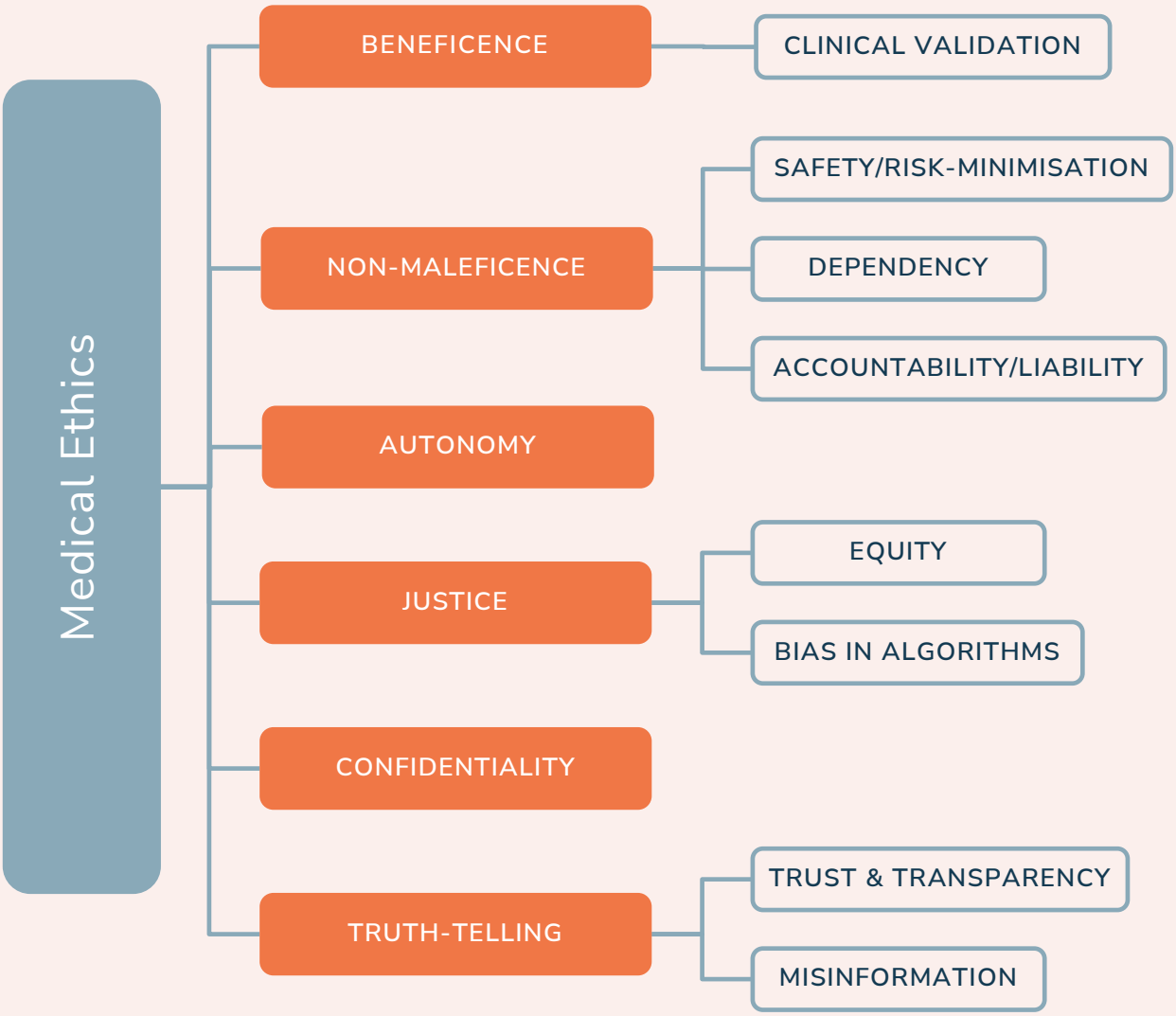
Artificial intelligence (AI) ethics are highly relevant to DMH because they address unique challenges related to specific responsibilities that arise from building and deploying autonomous, data-driven systems. Additionally, AI ethics related to healthcare are a widely discussed topic, providing a promising ground for exploring principles applicable to DMH apps in general.

Finally, ethics related to **digital health** and the ethical challenges of **digital mental health** are considered. These principles, while providing an important source of information, are also limited and must be considered within the broader context of ethical principles relevant to healthcare-adjacent fields.

As a part of our process, we have reviewed a range of academic papers and grey literature from these fields to create a list of principles to be considered. These principles will be discussed in the context of DMH.

What principles arise?

Medical ethics, comprising beneficence, non-maleficence, autonomy, justice, truth-telling, and confidentiality, form the basis through which digital mental health principles are discussed in this brief.



Beneficence

Acting for the benefit of the service user is an essential ethical obligation that applies directly to digital mental health apps. These apps should be designed with the primary purpose of doing good for the user.

Clinical validation

Clinical validation, as a principle related to beneficence, is a means of ensuring the effectiveness of a digital mental health app by being research-backed[1,2]. Research backing various digital mental health tools has been presented in the third brief of this series with the finding that many digital mental health interventions have insufficient evidence when compared to the rate at which they are used and scaled[3].

Additionally, often, research does not involve the specific population that will use the app[2] or creates test conditions that are different from the unsupervised nature of most digital mental health apps[1].

> For instance, a recent study about the use of a generative AI chatbot for mental health reported significant benefits[4]. A detailed read of the study indicates that the research team was available for crisis situations – however, the study was widely cited in news as generative AI being ready for mental health use without clarifying the important detail that in real app use scenarios, crisis teams are not available at hand to respond in case of crises.

Non-maleficence

Non-maleficence is the ethical principle that lays responsibility on the medical professional to avoid causing pain or suffering. In addition to the basic requirement of not causing harm, non-maleficence underlies some of the most crucial ethical principles related to digital mental health.

Safety/risk minimisation

Any app must, primarily, be safe to use. With the proliferation of apps that claim to provide therapy or market themselves as mental health support, substandard apps can cause direct or indirect harm. Research has shown that clinical researchers are more likely to focus on safety in their testing when compared to the private sector. Research also indicates that DMH apps involving professional oversight are safer[5].

Safety, going hand-in-hand with clinical validation, is therefore crucial. It is the ethical imperative of app developers to ensure the safety of their apps based on existing research, clinical trials, and safety mechanisms. Research studies must also ensure representation of the target population of the app in safety testing[6].

Specifically with respect to AI-based apps, safety evolves into a larger concern. The risk of clinical harm arising from the AI's limitations, such as the potential for inaccurate diagnosis, inappropriate advice, AI sycophancy, and a general lack of predictability especially with respect to generative AI, needs to be addressed[7].

A significant component of a DMH platform is how equipped they are in crisis management. This entails an appropriate and timely response to situations that may require immediate attention. To this end, a robust system must be established to account for the urgent nature of crises. Recommendations include rigorous testing of digital mental health tools to understand when systems fail to prevent algorithmic errors, combined with clear pathways for users to override automated responses and access human support as an alternative mode of care to reduce risk in crises[8].

Dependency on the tool

A significant issue pertaining to digital mental health apps is the commercialisation gap[5]. An app developed through clinical research is more likely to be reliable and valid, while an app developed by the private sector is likely to prioritise user engagement, thereby having a far more wide-reaching impact and user base.

The challenge that arises from capitalising upon this user base and commercial engagement is the promotion of an unhealthy dependency to improve engagement and continued use[9,10,11]. Maximising user engagement and continued use must not be the priority of these app developers.

While these platforms significantly improve access to support, they often entail behaviour reinforcement mechanisms such as push notifications and gamified elements which mirror those prevalent on social media platforms. The commercialisation evident through the targeted advertising and premium tier access to features (often based on a subscription model) raises concerns regarding the true extent of accessibility. These mechanisms may hence prioritise user retention, which would present as habitual app usage, as opposed to therapeutic benefit, which would foster actual psychological growth. Where traditional care aims to improve autonomy as a therapeutic goal, commercialisation of an app commodifies the vulnerability of people in distress or with mental health concerns by replacing recovery goals with app engagement, ultimately inducing reward-seeking behaviour and delaying professional intervention[1].

Accountability/liability

To avoid legal liability and responsibility for safety risks, app developers often hide "disclaimers" in their fine print. This fine print usually includes long dense paragraphs that are hard to comprehend and that most users therefore do not read. These sections usually state that the app is not meant to provide medical advice or guidance and that the user is responsible for their use of the app[12]. The question that then arises is, who truly is accountable when apps do not function as intended, or cause harm to the user? Is it sufficient to waive liability with a disclaimer? These questions are particularly pertinent to AI-based apps but are relevant to all apps that do not have a human in the loop. Various partial solutions have been proposed to address this challenge.

Centralised safety frameworks and app registries could help ensure digital mental health tools are safe and responsibly governed, placing more responsibility on developers to ensure clinical validation and reduce risks. But the rapid growth of apps makes their implementation difficult.

Clearer, more accessible terms and conditions can improve user understanding of safety and liability, while impact assessments, oversight mechanisms, and publicly available audits can further strengthen accountability and transparency in data practices[5]. However, audits and users understanding liability are insufficient as they do not answer the question of who is responsible when something goes wrong.

Accountability for digital mental health is a hard problem to solve. Without a human in the loop and a wide range of digital mental health apps available, what could accountability look like? As DMH becomes more commonplace, disclaimers waiving liability will not be sufficient to ensure safety. Does this responsibility lie with developers, or users, or clinicians who recommend apps, or could this responsibility be shared?

This responsibility could sometimes depend on where the DMH tool failed – wrong, misleading, or outdated content leading to harm being the responsibility of the developers and wrong interpretation by the clinician being the responsibility of the clinician[13].

Recent discourse suggests that there should be widespread regulation of mental health apps, despite rapid growth in this space. The UK requires classification of apps that diagnose, prevent, monitor, or treat mental health conditions as medical devices that must meet medical device standards before entering the market. These standards depend on risk classification – “minimal impact on health if something goes wrong” classifies an app as low risk, “influencing treatment decisions or outcomes” classifies it as medium risk, and an app that has the “potential for life-threatening consequences or serious harm” is classified as high risk. The intention is to ensure the level of scrutiny matches the level of risk[14].

Additionally, a paper also suggests AI regulation in mental health through a comprehensive framework that combines medical device grade certification for any AI marketed as a mental health tool with strict mental health professional oversight for the use of AI-based tools. Under this model, AI systems would also be required to meet minimum safety, transparency, and data-privacy standards before approval and be supplemented by mandatory audits of adverse events[15].

Autonomy

Autonomy, as a principle, emphasises a person's right to self-determination. This includes the right to make decisions and moral choices. In the context of digital mental health, this stands out as the right to informed consent and to make independent choices related to one's mental health.

True autonomy requires full informed consent. The complexity of app policies and algorithms makes it difficult for users to understand risks. When users do not genuinely understand risks, the treatment plan, the rationale, and what they are signing up for, even if their decision to use the app is technically consensual, this consent is not fully informed or autonomous[9,16].

The opacity of AI algorithms directly challenges the principle of autonomy in digital mental health apps. Users are given AI recommendations with no information on how that conclusion was reached, leaving it impossible to critically assess the information before making a choice.

AI opacity also limits a user's ability to intervene or negotiate the guidance received, reducing their control and fostering dependency on an inexplicable system. This inability to negotiate the guidance is a challenge directly caused by how digital mental health apps function and is not relevant only to AI apps.

As previously discussed in the context of dependency, the autonomy of an individual is also imperilled when DMH platforms include mechanisms which increase user retention and app usage. The choice of the individual to continue engaging with the platform can be manipulated, in many cases without the awareness of the user – a UI/UX concept called "dark patterns".

Dark patterns are UI/UX choices intended to bring about a certain decision from the user through manipulative interfaces. As an example, subscribing to an app or service could be very straightforward, while unsubscribing could be far more complicated – a specific form of manipulation called the Roach Motel Effect.

Unsubscribing could also be designed to induce guilt through an interface where instead of a simple "Cancel Subscription" option, the user could be led to another screen with two buttons: one with the text, "Keep taking care of my mental health" and another with "No thanks, I don't care about my well-being anymore".

Additionally, when apps are designed to increase user engagement, addictive behaviours are reinforced through dark patterns, especially in vulnerable populations[17,18,19]. This brings into question whether the user has true autonomy over their choice to use the app as well.

Justice

Justice refers to fair and equitable treatment of service users, including healthcare access, fair distribution of healthcare resources, and ensuring that no person is discriminated against based on their socioeconomic status, race, gender, caste, religious identity, etc. In the context of digital mental health, justice can be broken down into two main principles: equity and bias.

Equity

Equitable access to technology is not only a principle derived from the principle of justice in medical ethics. Not exacerbating socioeconomic disadvantages is an essential principle of public health ethics too.

Digital access and literacy inequities could lead to widening healthcare inequities. In this scenario, it is important to make access to apps as equitable for various populations as possible to prevent the worsening of healthcare access gaps. This could take the form of developing user-friendly apps for people with lower levels of digital literacy and various linguistic needs and apps that function without constant internet use. However, very few of the ethical frameworks considered in this review include this principle[16,20,21].

In a 2025 survey in India, phone ownership among those aged 15 and over is 81.2% in urban areas, but only 64.6% in rural areas. This gap is widened further when it comes to smartphones - 72.6% of phone owners in rural areas own smartphones, compared to 82.9% in urban areas. Across the country, ownership is at 83.9% in males and 56.2% in females. In rural areas, 80.7% of males own a phone when compared to 48.4% of females, while in urban areas, the numbers are at 90.0% for males and 71.8% for females. Additionally, in rural areas, 83.3% of households have access to the internet, compared to 91.6% in urban areas[22].

Bias in algorithms

AI algorithms are often trained on datasets which are not representative of the population that the platform may be catering to. Skewed information and algorithmic bias may play a role in perpetuating social inequities, as training modelled on datasets that lack diverse cultural and socioeconomic representation could lead to systemic misdiagnosis or under-prediction of risk for marginalised groups.

This bias could also create a dangerous loop: an algorithm might under-diagnose a specific community, and the resulting lack of positive data is taken as confirmation that that community requires fewer resources in the future.

Confidentiality

Another principle that is directly relevant to DMH is confidentiality. With the extent of data shared by users directly or collected by an app in the background, data privacy and security are critical concerns. Through the review undertaken, data privacy is the most common ethical principle discussed in existing literature around this subject[1,5,9,12,16,20,23,24,25,26].

Apart from challenges related to maintaining good security standards, data is often sold to third parties. In India, the Digital Personal Data Protection Act (DPDPA) governs digital data privacy across all fields. The DPDPA is a powerful law when it comes to ensuring data security, with consequences for data leaks.

However, the DPDPA faces its share of pitfalls when it comes to mental health data – lack of stringent regulations with respect to sensitive data; broad exemptions to start-ups and the state; and exemptions for research and statistical purposes[27]. The combined legal and ethical requirements result in a responsibility upon the app developers and deployers to ensure that only minimal data is collected, and this data is securely stored and not sold to third parties.

Additionally, Large Language Models (LLMs) like ChatGPT are increasingly being used for informal mental health care. What users may not be aware of is that LLM conversations are often not private and may also be used for LLM training[28].

Some common recommendations in the existing literature on this subject are[1]:

- It should be clear what, if any, data is being sold and to whom in the privacy policies.
- These privacy policies should be written in simple language.
- It should be ensured that no data that is not required is collected.
- Services should make it clear to users who will have access to the data, what kind of data is being collected, and how it is being used and stored.
- Data should be deidentified where possible, and privacy and protection must be ensured through all stages of development and deployment.

Truth-telling

Truth-telling is the obligation of a healthcare provider to be transparent and honest. Taking the principle at its core, related principles for DMH can be translated as trust and transparency, and countering misinformation.

Trust and transparency

Trust and transparency are ethical principles underlying many other principles. Establishing and maintaining trust requires DMH tools to demonstrate robust technical performance, clinical

efficacy, and ensuring data security, privacy, and algorithmic transparency. A breakdown of trust can lead to non-use of the DMH apps, with transparency being a predominant requirement to establish trust[16,21,29,30].

Most often encountered in the context of AI ethics, trust revolves around the expectation that the model will competently behave in ways that serve the users. It can be approached through evidence of performance and its limitations. Steps that could be taken towards transparency are full disclosure of information regarding development, training data, performance, and data stored.

Of note is the fact that all stakeholders might not have the same viewpoint of what constitutes transparency – as an example, a paper noted that while developers focused on algorithm validation, users had a desire to understand how the AI worked[24].

Misinformation

One consequence of a lack of trust and transparency is non-use of the app, but a larger ethical issue arises under the umbrella of truth-telling – misinformation about what the app does, or its effectiveness, is detrimental to user well-being[20]. It is the imperative of the app developer to provide clear and complete information about the app, its use, and its research backing.

> As an example, a meditation app that claims to provide a programme for depression could lead to worsened mental health – a fact found in academic research[31]. Such an app could not only be detrimental to the user but could also prevent timely help-seeking by claiming to treat depression.

Conclusion

Digital mental health offers significant opportunities to strengthen access to care, yet its ethical deployment requires careful management of the risks it introduces. A responsible framework integrating established principles from medical ethics, public health ethics, AI ethics, and digital health governance, while recognising the practical constraints of rapidly evolving innovation, must be identified and widely followed.

Evidence-based design, robust safety mechanisms, and continuous monitoring to prevent unintended harm lead to beneficence and non-maleficence in delivering digital care. Autonomy must be protected through transparency, informed consent, and awareness of manipulative engagement practices, while justice requires measures to address inequities in access, data representation, and outcomes. Data protection and accountable governance structures are essential to maintaining trust. As DMH tools become increasingly embedded in mental healthcare, ethics are essential to effectively adapt and integrate the virtues such technologies may have to offer.

A discussion of ethics and ethical issues alone is insufficient. It is essential to go a step further and understand how these ethical principles look in practice. This can only be achieved through a collaboration among various stakeholders who have expertise in different facets of digital mental health – app developers and organisations, professionals in the field of healthcare ethics, mental health professionals, researchers, and users of digital mental health.

References

1. Wykes, T., Lipshitz, J., & Schueller, S. M. (2019). Towards the Design of Ethical Standards Related to Digital Mental Health and all Its Applications. *Current Treatment Options in Psychiatry*, *6*(3), 232–242. https://doi.org/10.1007/s40501-019-00180-0

2. Harishbhai Tilala, M., Kumar Chenchala, P., Choppadandi, A., Kaur, J., Naguri, S., Saoji, R., & Devaguptapu, B. (2024). Ethical Considerations in the Use of Artificial Intelligence and Machine Learning in Health Care: A Comprehensive Review. *Cureus*. https://doi.org/10.7759/cureus.62443

3. Pillutla, R. (2025). *Delving into Digital Mental Health: Part 3* (Delving into Digital Mental Health). Centre for Mental Health Law & Policy. https://cmhlp.org/wp-content/uploads/2025/04/Digital-Mental-Health-Part-3.pdf

4. Heinz, M. V., Mackin, D. M., Trudeau, B. M., Bhattacharya, S., Wang, Y., Banta, H. A., Jewett, A. D., Salzhauer, A. J., Griffin, T. Z., & Jacobson, N. C. (2025). Randomized Trial of a Generative AI Chatbot for Mental Health Treatment. *NEJM AI*, *2*(4), AIoa2400802. https://doi.org/10.1056/AIoa2400802

5. Martinez-Martin, N., & Kreitmair, K. (2018). Ethical Issues for Direct-to-Consumer Digital Psychotherapy Apps: Addressing Accountability, Data Protection, and Consent. *JMIR Mental Health*, *5*(2), e9423. https://doi.org/10.2196/mental.9423

6. *Socio-ethical challenges and opportunities for advancing diversity, equity, and inclusion in digital medicine—Ivana Paccoud, Anja K. Leist, Isabel Schwaninger, Robin van Kessel, Jochen Klucken, 2024*. (n.d.). Retrieved May 4, 2026, from https://journals.sagepub.com/doi/full/10.1177/20552076241277705

7. Chustecki, M. (2024). Benefits and Risks of AI in Health Care: Narrative Review. *Interactive Journal of Medical Research*, *13*, e53616. https://doi.org/10.2196/53616

8. Indian Council of Medical Research. (2023). *Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare*.

9. Wies, B., Landers, C., & Ienca, M. (2021). Digital Mental Health for Young People: A Scoping Review of Ethical Promises and Challenges. *Frontiers in Digital Health*, *3*. https://doi.org/10.3389/fdgth.2021.697072

10. Babu, A., & Joseph, A. P. (2025). Digital wellness or digital dependency? A critical examination of mental health apps and their implications. *Frontiers in Psychiatry*, *16*. https://doi.org/10.3389/fpsyt.2025.1581779

11. Torous, J., Nicholas, J., Larsen, M. E., Firth, J., & Christensen, H. (2018). Clinical review of user engagement with mental health smartphone apps: Evidence, theory and improvements. *Evidence Based Mental Health*, *21*(3). https://doi.org/10.1136/eb-2018-102891

12. Martinez-Martin, N., Dasgupta, I., Carter, A., Chandler, J. A., Kellmeyer, P., Kreitmair, K., Weiss, A., & Cabrera, L. Y. (2020). Ethics of Digital Mental Health During COVID-19: Crisis and Opportunities. *JMIR Mental Health*, *7*(12), e23776. https://doi.org/10.2196/23776

13. Prictor, M. (2023). WHERE DOES RESPONSIBILITY LIE? ANALYSING LEGAL AND REGULATORY RESPONSES TO FLAWED CLINICAL DECISION SUPPORT SYSTEMS WHEN PATIENTS SUFFER HARM. *Medical Law Review*, *31*(1), 1–24. https://doi.org/10.1093/medlaw/fwac022

14. Digital Mental Health Technology—Regulation and Evaluation for Safe and Effective Products. (2024). Medicine & Healthcare products Regulation Agency. https://assets.publishing.service.gov.uk/media/6866572fadfe29730ea3a9d5/MHRA_guidance_on_DMHT_-_Device_characterisation_regulatory_qualification_and_classification.pdf

15. Iftikhar, Z., Xiao, A., Ransom, S., Huang, J., & Suresh, H. (2025). How LLM Counselors Violate Ethical Standards in Mental Health Practice: A Practitioner-Informed Framework. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 8(2), 1311–1323. https://doi.org/10.1609/aies.v8i2.36632

16. Ning, Y., Teixayavong, S., Shang, Y., Savulescu, J., Nagaraj, V., Miao, D., Mertens, M., Ting, D. S. W., Ong, J. C. L., Liu, M., Cao, J., Dunn, M., Vaughan, R., Ong, M. E. H., Sung, J. J.-Y., Topol, E. J., & Liu, N. (2024). Generative artificial intelligence and ethical considerations in health care: A scoping review and ethics checklist. The Lancet Digital Health, 6(11), e848–e856. https://doi.org/10.1016/S2589-7500(24)00143-2

17. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18, 1–14. https://doi.org/10.1145/3173574.3174108

18. Rossi, A., Carli, R., Botes, M. W., Fernandez, A., Sergeeva, A., & Sánchez Chamorro, L. (2024). Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multi-dimensional nature of digital vulnerability1. Computer Law & Security Review, 55, 106031. https://doi.org/10.1016/j.clsr.2024.106031

19. Hilton, M. (2023). Dark Patterns and User Mental Health: Identifying Theoretical Impacts of Deceptive Design on Vulnerable Demographics. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 67(1), 2124–2127. https://doi.org/10.1177/21695067231199684

20. World Health Organization. (2025). Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. https://www.who.int/publications/i/item/9789240084759

21. Zhang, J., & Zhang, Z. (2023). Ethics and governance of trustworthy medical artificial intelligence. BMC Medical Informatics and Decision Making, 23(1), 7. https://doi.org/10.1186/s12911-023-02103-9

22. Comprehensive Modular Survey: Telecom, 2025. (2025). National Statistics Office, Ministry of Statistics and Programme Implementation, Government of India. https://www.mospi.gov.in/sites/default/files/publication_reports/CMST_report_m.pdf

23. Varkey, B. (2020). Principles of Clinical Ethics and Their Application to Practice. Medical Principles and Practice, 30(1), 17–28. https://doi.org/10.1159/000509119

24. Maccaro, A., Stokes, K., Statham, L., He, L., Williams, A., Pecchia, L., & Piaggio, D. (2024). Clearing the Fog: A Scoping Literature Review on the Ethical Issues Surrounding Artificial Intelligence-Based Medical Devices. Journal of Personalized Medicine, 14(5), 443. https://doi.org/10.3390/jpm14050443

25. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000380455

26. Gooding, P., & Kariotis, T. (2021). Ethics and Law in Research on Algorithmic and Data-Driven Technology in Mental Health Care: Scoping Review. JMIR Mental Health, 8(6), e24668. https://doi.org/10.2196/24668

27. Mathew, E. (2025). Delving into Digital Mental Health: Part 2. Centre for Mental Health Law & Policy. https://cmhlp.org/wp-content/uploads/2025/04/Delving-Into-Digital-Mental-Health-Part-2.pdf

28. Srivastava, V. (2025, July 25). ChatGPT therapy chats are not private, warns OpenAI CEO Sam Altman. Hindustan Times. https://www.hindustantimes.com/world-news/us-news/chatgpt-therapy-chats-are-not-private-warns-openai-ceo-sam-altman-101753462807870.html

29. Terrasse, M., Gorin, M., & Sisti, D. (2019). Social Media, E-Health, and Medical Ethics. Hastings Center Report, 49(1), 24–33. https://doi.org/10.1002/hast.975

30. Lauer, D. (2021). You cannot have AI ethics without ethics. AI and Ethics, 1(1), 21–25. https://doi.org/10.1007/s43681-020-00013-4

31. Farias, M., Maraldi, E., Wallenkampf, K. C., & Lucchetti, G. (2020). Adverse events in meditation practices and meditation-based therapies: A systematic review. Acta Psychiatrica Scandinavica, 142(5), 374–393. https://doi.org/10.1111/acps.13225