Letter to Editor

The Double-Edged Sword of Telemedicine: Privacy Risks on the Digital Health Frontier

Dear Editor

I read with considerable interest the observational case study by Haddad Soleymani and Mohammadpour.[1] This work provided a timely and crucial examination of the privacy vulnerabilities inherent in the burgeoning world of telemedicine—a field that has expanded dramatically, particularly following the COVID-19 pandemic. I commend the authors for their innovative approach in demonstrating how publicly accessible data can be leveraged to compromise patient confidentiality, a topic of paramount importance for both patient trust and the ethical implementation of digital health technologies.

The study's methodology, which involved the scraping of public data from a Persian televisit website, powerfully illustrated the real-world risks often unaddressed in the rapid rollout of new technologies. The authors' ability to reconstruct patient-doctor interaction patterns and infer potential medical conditions from seemingly innocuous public data serves as a sobering reminder that privacy breaches do not always require malicious hacking; they can also result from inadequate system design and a lack of robust data protection protocols. This critical point resonates far beyond the specific context of Iran, offering a cautionary tale for telemedicine platforms worldwide.

The authors' findings underscored a significant gap in Iran's regulatory landscape for digital health. While many countries have established comprehensive legal frameworks, such as HIPAA in the United States, to govern the use and disclosure of electronic health information,[2] the study highlighted the nascent state of such regulations in Iran. This lack of a robust national framework creates a precarious environment where patient data is at risk, and the essential trust of a functioning healthcare system can be easily eroded.

However, while the study's findings are compelling, it is important to acknowledge the inherent tension between data accessibility and privacy. Telemedicine platforms often rely on some level of public information to function effectively—for example, doctor ratings and specialties help patients make informed choices. The challenge, therefore, is not to eliminate all public data but to implement a "privacy by design" approach, as the authors rightly suggest.[3] This means integrating robust anonymization and de-identification techniques from the outset, ensuring that publicly available data cannot be reverse-engineered to identify individuals or infer sensitive health information.

The study's recommendation for a thorough national framework, developed in collaboration with IT experts, medical professionals, and the Ministry of Health and Medical Education, is a crucial and actionable step forward. Such a framework must be tailored to Iran's specific cultural and legal context while drawing on international best practices. It should provide clear guidelines on data collection, storage, and sharing, and establish strong enforcement mechanisms to ensure compliance.

Furthermore, patient education is a critical component of any comprehensive data protection strategy. Patients must be made aware of their rights regarding their health information and empowered to make informed decisions about how their data is used. This requires clear, transparent privacy policies and accessible information about the potential risks and benefits of using telemedicine platforms.

In conclusion, the study by Haddad Soleymani and Mohammadpour[1] is a vital contribution to the discourse on digital health ethics and governance. It serves as a powerful call to action for policymakers, healthcare providers, and technology developers in Iran and beyond to prioritize patient privacy and confidentiality in the design and implementation of telemedicine platforms. As we continue to embrace the convenience and accessibility of digital health, we must not lose sight of the fundamental ethical principles underpinning the patient-provider relationship. This study is a crucial reminder that the future of healthcare depends not only on technological innovation but also on our unwavering commitment to protecting the privacy and dignity of every patient.

Declaration of AI

In preparing this “Letter to the Editor”, we did not use any Artificial Intelligence (AI)-assisted technologies such as Large Language Models (LLMs), chatbots, or image creators.

Conflict of Interest: None declared.

Keywords ● Telemedicine ● Privacy ● Data confidentiality ● Health policy

Haewon Byeon, DrSc, PhD

Worker’s Care and Digital Health Lab, Korea University of Technology and Education (KOREA TECH), Cheonan 31253, South Korea

Correspondence:
Haewon Byeon, DrSc, PhD;
Worker’s Care and Digital Health Lab, Korea University of Technology and Education (KOREA TECH), Cheonan 31253, South Korea
Tel: +82 10 74046969
Email: bhwpuma@naver.com
Received: 11 December 2025
Revised: 29 December 2025
Accepted: 01 January 2026

Please cite this article as: Byeon H. The Double-Edged Sword of Telemedicine: Privacy Risks on the Digital Health Frontier. Iran J Med Sci. doi: 10.30476/ijms.2026.110133.4568.

References

1 Haddad Soleymani M, Mohammadpour A. Assessing Information Confidentiality in Telemedicine Platforms Using Public Web Data: A Case Study of Persian Televisit Websites. Iran J Med Sci. 2025;50:843-51. doi: 10.30476/ijms.2025.105205.3899. PubMed PMID: 41377901; PubMed Central PMCID: PMC12686951.
2 Mahadik SS, Pawar PM, Muthalagu R, et al. Digital privacy in healthcare: state-of-the-art and future vision. IEEE Access. 2024;12:84273-91. doi: 10.1109/ACCESS.2024.3410035.
3 Odeh A, Abdelfattah E, Salameh W. Privacy-preserving data sharing in telehealth services. Appl Sci. 2024;14:10808. doi: 10.3390/app142310808.