Journal of Medical Education Development
e-ISSN: 2980-7670
www.https://edujournal.zums.ac.ir

Volume 18, Issue 3
December 2025
Pages 163-164

Letter to Editor

Acceptable use policy: an ethical imperative in medical education

Zohrehsadat Mirmoghtadaie [1], Somayeh Shapoori[1*]

[1]Department of e-Learning in Medical Sciences, School of Medical Education and Learning Technologies,Shahid Beheshti University of Medical Sciences, Tehran, Iran.

Letter info

Letter history:
Received 25 Sep. 2025
Revised 19 Oct. 2025
Accepted 25 Oct. 2025
Published 19 Nov. 2025

***Corresponding author:**
Somayeh Shapoori. Department of e-Learning in Medical Sciences, School of Medical Education and Learning Technologies,Shahid Beheshti University of Medical Sciences, Tehran, Iran..
Email: somayehshapoori@gmail.com

How to cite this letter:
Mirmoghtadaie Z, Shapoori S. Acceptable use policy: an ethical imperative in medical education. *J Med Educ Dev*. 2025; 18(4): 163-164.

The quick digital transformation of healthcare and medical education has made electronic health data, online learning platforms, and digital communication tools easier to get to than ever before. These improvements have made it easier for people to get an education, but they have also made it more likely that patient data will be shared without permission. Patient data is inherently sensitive in medical education, and unauthorized disclosure can significantly compromise the welfare of patients, the integrity of medical personnel, and the credibility of institutions [1]. Consequently, the protection of patient data has become a fundamental ethical and professional duty in medical education [2].

As more and more people use Electronic Health Records (EHRs) and online resources for learning and clinical training, it is even more important to protect patient privacy, keep data safe, and hold people accountable. Medical students and educators who have access to this information need clear instructions on how to use it responsibly. The Acceptable Use Policy (AUP) gives schools a set of rules for how to use information systems and data in the classroom [3]. AUP lists what users can and can't do, what they are responsible for, and what will happen if they break the rules, especially when it comes to sensitive patient data.

AUP helps keep data from getting out, stops people from using it in ways that aren't right, and helps people make ethical choices about patient privacy. An AUP might say, for example, that medical students can only look at EHRs with permission and supervision [4]. This policy is more than just a technical safeguard; it is also part of professional and ethical training for doctors. In a lot of places, the law sets the rules for global AUP principles. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States stops people from getting to protected electronic health information in the wrong way by using protections like data minimization and required training [5].

But in Iran, there are still problems because there aren't enough national standards and hospitals don't do enough to manage risks. Problems like students getting into EHRs without permission and institutions not always following their own rules show that there are gaps in oversight [6, 7]. Iran needs detailed and localized AUP policies based on international data protection principles. This is different from the GDPR, which focuses on clear consent and data minimization, and South Africa's POPIA, which focuses on awareness and device control. New technologies like blockchain and artificial intelligence can help keep information private and stop it from being accidentally shared [6, 7].

To deal with these problems, medical schools should use AUP not just as a set of rules, but also as part of the curriculum. Teaching students about ethical responsibility when it comes to handling data from the very beginning of their education helps them

remember it. This method creates professionals who are not only good at their jobs but also good at protecting patient privacy and information security.

As a result, it is advised that every medical university form a special committee to plan, develop, instruct, and oversee the application of AUP. A committee like this can guarantee that rules are applied correctly and in the right context. AUP is not just administrative; it is an ethical requirement in a world where digital technologies are being incorporated into medical education more and more.

References

1.Hoffman S. Privacy and security—protecting patients' health information. *N Engl J Med*. 2022;387(21):1911-3. https://doi.org/10.1056/NEJMp2213163

2. Cohen IG, Mello MM. HIPAA and protection of health information in the 21st century. *JAMA*. 2018;320(3):231-2. https://doi.org/10.1001/jama.2018.5630

3. Klyman K. Acceptable use policies for foundation models. In: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society; 2024 Oct 16; Vancouver, Canada. New York: ACM; 2024. p. 752-67.

4. Mirmoghtadaie Z, Ahmady S, Kohan N, Rakhshani T. An interesting result of a qualitative research: academic exhaustion barrier to professionalism in medical students. *J Educ Health Promot*. 2020;9:212. https://doi.org/10.4103/jehp.jehp_230_20

5 Edemekong PF, Annamaraju P, Afzal M, Haydel MJ. Health Insurance Portability and Accountability Act (HIPAA) Compliance. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. [Updated 2024 Nov 24; cited 2025 Oct 13]. Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/

6 Nabilou B, Feizi A, Seyedin H. Patient Safety in Medical Education: Students' Perceptions, Knowledge and Attitudes. *PLoS One*. 2015;10(8):e0135610. https://doi.org/10.1371/journal.pone.0135610

7 Zarei J, Sadoughi F. Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk Manag Healthc Policy*. 2016;9:75-85. https://doi.org/10.2147/RMHP.S99908