Iran University of Medical Sciences

Journal of Health Administration

https://jha.iums.ac.ir/

Original article

Security barriers and facilitators in the use of mobile health applications from the perspective of paramedical students at Mashhad university of medical sciences: a descriptive cross-sectional study

Masoumeh Sarbaz[a], Seyyedeh Fatemeh Mousavi Baigi[a,b], Zahra Salehzade[a,b], Reyhane Norouzi Aval[a,b], Mojtaba Esmaeili[a], Khalil Kimiafar[a*]

[1] *Department of Health Information Technology, School of Paramedical and Rehabilitation Sciences, Mashhad University of Medical Sciences, Mashhad, Iran.*

[2]*Student Research Committee, Mashhad University of Medical Sciences, Mashhad, Iran.*

ARTICLE INFO

Corresponding Author:
Khalil Kimiafar
e-mail addresses:
KimiafraKh@mums.ac.ir

Received: 24/May/2024
Modified: 14/Sep/2024
Accepted: 20/Sep/2024
Published: 21/Dec/2024

Keywords:
Security
Privacy
Mobile health applications
Security barriers
Security facilitators

10.61186/jha.27.3.1

ABSTRACT

Introduction: Mobile health (mHealth) applications are recognized as effective tools for health management and improving the quality of healthcare services. However, concerns about data security and privacy remain significant barriers to their widespread adoption. This study aimed to identify security barriers and facilitators influencing the use of mHealth applications from the perspective of paramedical students.

Methods: This descriptive cross-sectional study was conducted in 2023 on 115 paramedical students at Mashhad University of Medical Sciences. Participants were selected through proportional stratified sampling. Data were collected using a structured questionnaire developed by Zhou et al., which was translated, back-translated, and validated in Persian (r = 0.92). The questionnaire included both Likert-scale items and open-ended questions. Descriptive statistics were used for analyzing quantitative data, while thematic analysis was employed to evaluate qualitative responses.

Results: Key security concerns included unauthorized data access and weak privacy policies, which were identified as major barriers to mHealth adoption. In contrast, remote data deletion, transparent security policies, and access controls were recognized as the main facilitators. Thematic analysis of qualitative responses revealed three main themes: security concerns, practical challenges, and suggested strategies for improving security and building trust in mHealth applications.

Conclusion: The study highlights the need for mHealth application designs to emphasize enhanced data security, transparent privacy policies, and user-friendly interfaces to boost user trust and promote adoption. These insights can inform developers and policymakers to optimize mHealth application design and implementation.

What was already known on this topic?

- Mobile health (mHealth) applications play a crucial role in improving access to healthcare services and enhancing patient-provider interactions.
- Security and privacy concerns are major determinants of the adoption or rejection of mHealth technologies.
- Prior research has emphasized the importance of data encryption, multi-level access controls, and transparent privacy policies in fostering user trust.

What this study added to our knowledge?

- Concerns about unauthorized access to personal health data and potential privacy breaches, the lack of transparency in security policies and unclear data management practices, as well as limited user control over stored information and the inability to delete data when needed are among the most important security barriers.
- The ability to remotely delete personal data in case of device loss or theft, transparent security policies that clearly outline data protection measures, and user-friendly interfaces that improve trust in security mechanisms are three key facilitators.
- Students' perception of security and privacy directly influences their willingness to adopt mHealth applications.

Extended Abstract

Introduction

Mobile health (mHealth) applications have emerged as effective tools for health management and improving the quality of healthcare services. These applications facilitate access to health information, promote patient self-management, and enhance communication between patients and healthcare providers, thereby transforming healthcare systems worldwide [1]. Furthermore, mHealth technologies, particularly wearable smart devices, enable real-time monitoring of health indicators, offering innovative solutions for disease management and prevention [2,3]. Despite these advantages, concerns regarding data security and privacy remain significant barriers to the widespread adoption of mHealth applications [4]. Studies have indicated that approximately 40% of users refrain from downloading or continuing to use these applications due to fears of data breaches or misuse of personal information [5]. Such security challenges include non-transparent privacy policies, complex security settings, and limited user control over data management [6,7]. Users expect mHealth applications to incorporate features such as data encryption, remote data deletion, and multi-level access controls to enhance security and build trust [8,9].

In Iran, the adoption of smartphones and mHealth applications has expanded rapidly. However, limited information is available regarding users' security concerns and privacy preferences [10]. Recent domestic studies have highlighted the potential of mHealth applications in enhancing medical education and learning processes among healthcare students. Nevertheless, challenges such as data security, usability issues, and the need for user-friendly features persist [11,12]. Recent research emphasizes that the integration of advanced security features—such as transparent privacy policies, access control mechanisms, and remote data erasure—can increase trust and acceptance of mHealth applications [8,13]. For instance, a 2021 study underscored the pivotal role of security features and user-friendly interfaces in improving the adoption of these technologies [6]. However, comprehensive investigations into the barriers and facilitators affecting the security of mHealth applications, particularly among healthcare and paramedical students in Iran, remain scarce [12, 14-16].

Paramedical students, as future healthcare professionals, play a crucial role in the adoption and promotion of mobile health (mHealth) technologies in clinical settings. This group is not only a potential user for such applications but will also serve as healthcare providers in the future, requiring the ability to ensure and assess patient data security. Understanding their perspectives and concerns regarding the security of mHealth applications can provide valuable insights for developing safer and more optimized applications. Furthermore, given the increasing digitization of healthcare services and the growing role of mHealth applications in education and service delivery, examining paramedical students' viewpoints in this area can help identify existing gaps and propose practical solutions to enhance security and user trust. This study aims to identify the barriers and facilitators related to the security of mHealth applications from the perspective of paramedical students at Mashhad University of Medical Sciences. The study can inform developers and policymakers, enabling them to design more secure and user-friendly mHealth applications while establishing policies that enhance security and privacy standards.

Methods

Study design: This study employed a descriptive, cross-sectional design at Mashhad University of Medical Sciences in 2023.

Population and sample size: The target population comprised paramedical students from various disciplines, including radiology, physiotherapy, laboratory sciences, speech therapy, occupational therapy, health information technology, and social working. A proportional stratified sampling method was employed to ensure representation across disciplines. The initial sample size was estimated to be 87 participants using Cochran's formula, considering a 95% confidence level and a 5% margin of error. However, to compensate for potential respondent attrition and enhance the generalizability of the findings, the final sample size increased to 115 participants.

Data collection instrument: The data were collected using a structured questionnaire adapted from a standardized instrument originally developed by Zhou et al. [17]. The questionnaire underwent a rigorous translation and localization process to meet international scientific standards. It was divided into two main sections to assess perspectives on data security and privacy features in mHealth applications:

1. Closed-ended (quantitative) questions: This section included 14 closed-ended questions based on a 7-point Likert scale (ranging from "Strongly Agree" to "Strongly Disagree"). The questions focused on evaluating students' attitudes regarding data security, privacy, and protective features of mHealth applications, such as data encryption, remote data deletion, access control, and privacy policies.
2. Open-ended (qualitative) questions: This section consisted of four open-ended questions designed

to explore participants' deeper insights and qualitative perspectives regarding barriers and facilitators related to security of mHealth applications. These questions addressed key topics, including: barriers to trust in mHealth applications, such as data breaches or unauthorized access; desired security and privacy features, including access permissions management and policy transparency; recommendations for improving security features based on personal experiences and expectations.

Translation and localization process: The questionnaire was translated from English to Persian and then back-translated into English by two bilingual experts to ensure accuracy and semantic equivalence. The translated version was reviewed and refined by a panel of five faculty member from the fields of medical informatics (n = 2), health information management (n = 1), biostatistics (n = 1), and health information technology (n = 1) to ensure cultural relevance and conceptual clarity. Any discrepancies were resolved through consensus, and the final version was validated for content.

The final version of the questionnaire was reviewed by an expert panel consisting of five faculty members: two from medical informatics, one from health information management, one from biostatistics, and one from health information technology. The panel assessed the cultural relevance and conceptual clarity of the content. All discrepancies were resolved by consensus, and the final version was approved for content validity.

Instrument validity and reliability: The validity of the questionnaire was confirmed through face and content validity, assessed by a panel of experts. Reliability was evaluated using the test-retest method over a 10-day interval involving 20 participants. The test-retest reliability of the questionnaire was confirmed with a Pearson correlation coefficient of 0.92, indicating high reliability and consistency.

Data collection procedure: The questionnaires were distributed electronically via university communication platforms and student groups. Participation was voluntary, and informed consent was obtained electronically before completing the questionnaire.

Data analysis: Quantitative data were analyzed using SPSS software (version 26). Descriptive statistics, including frequencies, and percentages were calculated. Qualitative data obtained from open-ended questions were analyzed using thematic analysis based on the framework proposed by Braun and Clarke [18]. The analysis followed six distinct steps: 1) Familiarization with the data: repeated reading of responses to gain an in-depth understanding; 2) Generating initial codes: identifying and coding meaningful segments of data; 3) Searching for themes: grouping codes into potential themes; 4) Reviewing themes: ensuring coherence and relevance of themes to the data; 5) Defining and naming themes: clearly describing and labeling each theme; 6) Producing the final report: organizing findings into a cohesive and structured narrative.To enhance the credibility of qualitative findings, two independent coders reviewed the data, and discrepancies were resolved through group consensus. Additionally, the results were shared with 15 participants to undergo a review and validation process by the contributors, ensuring that the interpretations were confirmed and approved by them.

Results

In this study, 115 paramedical students from various disciplines, including radiology, physiotherapy, laboratory sciences, speech therapy, occupational therapy, health information technology, and social working participated (response rate: 96%). As shown in Table 1, the mean age of the participants was 23.51 years with a standard deviation of 4.2. The majority of participants were female (64.3%) and single (84.3%). The distribution of responses indicated that most participants had prior experience using mHealth applications; however, they expressed concerns regarding the security and privacy of their information within these applications

Table 1. Demographic characteristics

Variable	Frequency (%) / Mean ± SD
Age (years)	23.51 ± 4.2
Gender	
Male	41 (35.7)
Female	74 (64.3)
Marital Status	
Single	97 (84.3)
Married	18 (15.7)
Field of Study	
Physiotherapy	5 (4.3)
Speech Therapy	15 (13.0)
Audiology	19 (16.5)

Table 1.Continued

Variable	Frequency (%) / Mean ± SD
Field of Study	
Health Information Technology	37 (32.2)
Radiology	11 (9.6)
Laboratory Sciences	15 (13.0)
Social Work	9 (7.8)
Education Level	
Bachelor's Degree (Discontinuous)	1 (0.9)
Bachelor's Degree (Continuous)	99 (86.1)
Master's Degree	14 (12.2)
PhD	1 (0.9)

Quantitative analysis:Table 2 presents the students' perspectives regarding personal data security and privacy. The majority of students (81.7%) either strongly agreed, agreed, or somewhat agreed that they were concerned about the privacy and security of their personal information in their daily lives. Furthermore, most participants (67.9%) expressed concerns about the privacy and security of their personal information when using mHealth applications. Similarly, 67.9% of students reported being worried about transmitting personal information via mHealth applications due to the potential risk of unauthorized access or tampering. In addition, 70.4% stated that they were unwilling to store personal information, such as name, national ID number, phone number, or email address, in mHealth applications—preferring to use only a unique identifier that is accessible solely by authorized personnel. Moreover, 88.6% of participants agreed that they would prefer their personal health information to be transferred to a centralized database through a highly secure process.

Table 2. students' opinions regarding personal data

Opinions about personal data	Strongly agree	Agree	Somewhat agree	Neutral	Somewhat disagree	Disagree	Strongly disagree
1. Overall, I am concerned about the privacy and security of my personal information in daily life.	46 (40.0)	22(19.1)	26 (22.6)	13(11.3)	7 (6.1)	1 (0.9)	0 (0.0)
2. I am concerned about the privacy and security of my personal information when using mHealth apps.	33 (28.7)	27(23.5)	18 (15.7)	16(13.9)	11 (9.6)	8 (7.0)	2 (1.7)
3. I am concerned that sending personal information through an mHealth app may expose it to manipulation by others.	26 (22.6)	24(20.9)	32 (27.8)	12(10.4)	10 (8.7)	6 (5.2)	5 (4.3)
4. I am not willing to store my personal information, such as name, phone number, or email, in mHealth apps, except for a unique ID trackable only by authorized personnel.	39 (33.9)	27(23.5)	15 (13.0)	14(12.2)	8 (7.0)	10 (8.7)	2 (1.7)
5. I want my personal health information to be transferred to a centralized database through a highly secure process.	61 (53.0)	29(25.2)	12 (10.4)	7 (6.1)	1 (0.9)	2 (1.7)	3 (2.6)

According to Table 3, the majority of students responded neutrally to the two questions: "Overall, I am satisfied with the privacy and security of the mHealth applications I currently use" and "Developers and healthcare providers have implemented the necessary security and privacy measures, offering a reasonable level of protection for information collected through mHealth applications." This neutrality highlights uncertainty and potential mistrust regarding the adequacy of existing privacy and security safeguards in mHealth technologies. Regarding usage patterns, 42.6% of students reported using mHealth applications to meet their healthcare needs. Furthermore, 52.2% expressed a desire for healthcare providers to adopt mHealth applications for storing and managing their health information, indicating a growing inclination toward integrating these technologies into routine care practices. In addition, 68.7% of students stated they would feel comfortable sharing their health

information among their physicians and therapists if such data sharing supported their healthcare management. This finding underscores the importance of secure communication channels and trust in data sharing processes to promote the acceptance and use of mHealth applications in healthcare management.

Table 3. students' opinions about health applications

Opinions about health applications	Strongly agree	Agree	Somewhat agree	Neutral	Somewhat disagree	Disagree	Strongly disagree
6. Overall, I am satisfied with the privacy and security of the mHealth applications I currently use.	10 (8.7)	15 (13.0)	21 (18.3)	51 (44.3)	9 (7.8)	6 (5.2)	3 (2.6)
7. Developers and healthcare providers need to ensure privacy and security measures are in place. These measures should provide reasonable protection for the data collected through mHealth applications.	6 (5.2)	17 (14.8)	30 (26.1)	42 (36.5)	6 (5.2)	12 (10.4)	2 (1.7)
8. I use mHealth applications for my healthcare needs.	3 (2.6)	22 (19.1)	24 (20.9)	25 (21.7)	15 (13.0)	14 (12.2)	12 (10.4)
9. I want healthcare providers to use mHealth applications to store and manage my health information.	18 (15.7)	22 (19.1)	20 (17.4)	22 (19.1)	17 (14.8)	5 (4.3)	6 (5.2)
10. I feel comfortable if my health information is shared among doctors and therapists for healthcare purposes.	14 (12.2)	28 (24.3)	37 (32.2)	21 (18.3)	8 (7.0)	3 (2.6)	4 (3.5)

According to Table 4, the majority of students (50.4%) strongly agreed that they should have the right to consent to any protected sharing of their health information collected through mHealth applications. Furthermore, 82.6% of students agreed or strongly agreed that they wanted assurances from developers and healthcare providers about how access to mHealth systems is restricted to authorized personnel only. In addition, a substantial proportion of students (77.4%) expressed their preference for having the capability to remotely delete all their health data from their mobile devices in cases of loss or theft.

Table 4. students' opinions about features required in mhealth applications

Features required in mHealth applications	Strongly agree	Agree	Somewhat agree	Neutral	Somewhat disagree	Disagree	Strongly disagree
11. I should have the right to consent to any protected sharing of my health information collected through mHealth applications.	58 (50.4)	33(28.7)	14 (12.2)	7 (6.1)	2 (1.7)	1 (0.9)	0
12. I want to know how developers and healthcare providers ensure that only authorized personnel have access to the mHealth systems I use.	56 (48.7)	39(33.9)	9 (7.8)	8 (7.0)	3 (2.6)	0	0
13. Privacy policies of mHealth applications should explicitly state how privacy policies influence my decision to use the application.	19 (16.5)	34(29.6)	36 (31.3)	16(13.9)	4 (3.5)	3 (2.6)	0
14. I want to have access to remotely delete all my health data from my mobile device in case it is lost or stolen.	19 (16.5)	34(29.6)	36 (31.3)	16(13.9)	4 (3.5)	3 (2.6)	3 (2.6)

Qualitative analysis: The qualitative data analysis revealed three main themes. 1) Security concerns: This theme focused on users' fears regarding data breaches, potential misuse of personal information, and the lack of transparency in the security policies of mobile health applications. Many participants expressed concerns that their sensitive information might be used without their knowledge or consent. 2) Practical challenges: This theme highlighted the difficulties users faced when utilizing mobile health applications, including complex user interfaces, weak security infrastructures, and challenges in access management. These challenges were particularly more pronounced among users with lower technical literacy, as this group had a limited understanding of how to configure and utilize the security features of these applications and required additional guidance and training. Some participants reported struggling with access control and safeguarding their personal data due to unfamiliarity with security settings. 3) Improvement suggestions: This theme encompassed suggestions aimed at enhancing security and user trust, including advanced encryption, multi-level access control, and the development of transparent privacy policies. Some participants proposed that mobile health applications should offer features enabling users to manage security settings more intuitively and, in emergency situations, remotely erase their health data.

Discussion

The present study investigated the security barriers and facilitators influencing the adoption of mobile health (mHealth) applications among allied health students. Findings based on quantitative and qualitative data analysis identified three main themes: security concerns, practical challenges, and recommendations for improvement. Results highlighted that data security and privacy remain the primary barriers to adopting these technologies. These findings, when compared to international studies, provide critical insights for the development of secure and user-friendly mHealth technologies.

Security concerns: a key priority for users: One of the key findings was the widespread concerns of participants regarding data security and privacy. Quantitative results indicated that more than 82.6% of students emphasized the importance of access control and ensuring data protection. Furthermore, 77.4% of participants expressed a desire for a remote data wipe feature in case of theft or loss of mobile devices. These findings are consistent with those of Krebs and Duncan [5], who reported that 40% of users in the United States avoided installing mHealth applications due to security concerns. Similar studies, including that of Atienza et al. [19], emphasized the relationship between users' perceptions of data security and trust-building through transparent security policies and access controls. Research conducted by Peng et al. [20] also revealed that younger users are particularly reluctant to share sensitive information via social networks and demand greater control over their data. These findings suggest that mHealth applications must incorporate transparent security policies, advanced encryption mechanisms, and multi-level access controls to build user trust.

Practical challenges: weak infrastructure and system complexity: Qualitative analysis revealed that users, in addition to security concerns, faced practical challenges, such as complex user interfaces, weak security infrastructures, and difficulty in managing access controls. These challenges were particularly more significant among users with lower technical literacy, as this group required more guidance to effectively utilize the security features available in mobile health applications. These findings align with the study by Fadaizadeh et al. [12] which identified high costs, interface complexity, and low reliability as major barriers to mHealth adoption. Similarly, Byambasuren et al. [10] highlighted challenges such as limited access to reliable information and low user awareness, which restricted adoption rates. Moreover, Prasad et al. [21] emphasized the importance of multi-level data management and the ability to remotely delete information in emergencies. Studies by Baigi et al. [22] and Swain et al. [23] further pointed to high costs and infrastructure limitations as significant barriers to widespread adoption of mHealth technologies.

Recommendations for the improvement: enhancing security and user trust: Based on qualitative analysis, participants suggested security enhancements, including advanced encryption, multi-level access controls, and the development of transparent privacy policies. These suggestions are consistent with findings by Simblett et al. [24], who emphasized that advanced security features and access monitoring systems can boost user trust. Additionally, Aljedaani et al. [25] highlighted the importance of developing clear legal frameworks and obtaining security and ethical approvals to enhance user confidence. König et al. [6] introduced a three-level framework that emphasized the role of user motivation, infrastructure, and social interaction in mHealth adoption.

Given the proven efficacy and effectiveness of mHealth applications and the lack of clear security policies in Iran, it is recommended that policymakers develop minimum security frameworks to protect user data. Furthermore, due to

the increasing availability of mHealth applications and the lack of reliable identification systems, evaluating and validating these applications before their deployment is of critical importance. Moreover, security education programs for mobile app users should be expanded to raise awareness about available security features. This will empower users to protect their data and privacy effectively [26-29].

Strengths and limitations: This study, utilizing quantitative and qualitative data, provided comprehensive insights into the security barriers and facilitators of mHealth adoption. However, the generalizability of the results may be limited due to the sample size and the focus on allied health students in one university. Additionally, data on cost-effectiveness and long-term impacts of these technologies were not explored, which should be addressed in future studies.

Conclusion and recommendations for future research: This study demonstrated that security concerns, infrastructure weaknesses, and complex user interfaces are key barriers to the adoption of mHealth technologies. However, the high willingness of users to adopt these applications, provided the improved security features, presents an opportunity for developers and policymakers. The development of secure mHealth technologies requires multi-faceted approaches. A key recommendation is the integration of advanced encryption and multi-level access controls to enhance data protection and user trust. Developing transparent privacy policies is also essential to alleviate user concerns and facilitate adoption.

Furthermore, expanding educational programs and awareness campaigns to enhance users' understanding of data protection strategies and secure usage can increase engagement, particularly among users with limited technical expertise. Given the financial concerns highlighted in this and prior studies, cost-effectiveness evaluations of these applications and the development of scalable deployment models should be prioritized. Finally, designing longitudinal studies to assess the impact of security features and technical capabilities on user behavior and adoption rates can provide deeper insights into barriers and facilitators. Such research can inform the development of robust frameworks for mHealth technologies, ultimately improving the quality of healthcare delivery.

Declerations

Ethical considerations: This study is derived from an approved research project at Mashhad University of Medical Sciences (Ethics Code: IR.MUMS.FHMPM.REC.1401.086).

Funding: This study was financially supported by Mashhad University of Medical Sciences (Project Code: 4002080). The funder had no role in data collection, analysis and manuscript preparation.

Conflict of interest: The authors declared no conflict of interest.

Authors' contributions: MS: Conceptualization and study design, data collection, methodology, data analysis, writing – draft preparation, final approval; **SFMB**: Data collection, validation, data management, writing – review and editing, visualization, final approval; **ZS**: Data collection, final approval; **RNA**: Data collection, final approval; **KK** (corresponding author): Conceptualization and study design, methodology, study supervision, project administration, funding acquisition, resources, final approval; **ME**: Data collection, final approval.

Consent for publication: Not applicable.

Data availability: The data can be requested from corresponding author based on a reseanable request.

AI decleration: The English parts of the manuscript was edited using the ChatGPT (developed by OpenAI). All AI-assisted revisions were thoroughly reviewed and approved by the authors to ensure accuracy and appropriateness.

Acknowledgments: We would like to extend our sincere gratitude to all students who participated in this study for their valuable contributions. We also deeply appreciate the Student Research Committee at Mashhad University of Medical Sciences for their scientific and academic support throughout the research process.

References

1. Hoikka M, Silfvast T, Ala-Kokko TI. A high Saigí-Rubió F, Borges do Nascimento IJ. The current status of telemedicine technology yse across the WHO European region. Journal of Medical Internet Research. 2022;24(10):e40877. https://doi.org/10.2196/40877
2. Sheikhtaheri A, Hashemi N, Hashemi NA. Benefits of using mobile technologies in education from the viewpoints of medical and nursing students. Studies in Health Technology and Informatics. 2018;251:289-292. https://doi.org/10.3233/978-1-61499-880-8-289
3. Nemati-Anaraki L, Mousavi S S, AliBeyk M, Mahami-Oskouei M. Medical students knowledge and use of smartphone-based applications. Journal of Health Administration. 2022; 24 (4):84-94. [In Persian]. https://doi.org/10.52547/jha.24.4.84
4. Sheikhtaheri A, Kermani F. Use of mobile apps among medical and nursing students in Iran. Studies in Health Technology and Informatics. 2018;248:33-39. https://doi.org/10.3233/978-1-61499-858-7-33
5. Krebs P, Duncan DT. Health app use among US mobile phone owners: a national survey. JMIR Mhealth Uhealth. 2015;3(4):e101. https://doi.org/10.2196/mhealth.4924
6. König L, Sproesser G, Schupp HT, Renner B. Describing the process of adopting nutrition and fitness apps: Behavior stages and determinants. JMIR Mhealth Uhealth. 2021;9(5):e22513. https://doi.org/10.2196/mhealth.8261

7. Sun L, Yang B, Kindt E, Chu J. Privacy barriers in health monitoring: scoping review. Journal of Medical Internet Research Nursing. 2024;2(1):e53592. https://doi.org/10.2196/53592
8. Mbunge E, Sibiya MN. Mobile health interventions for improving maternal and child health outcomes in south Africa: a systematic review. Global Health Journal. 2024;9(1):e41. https://doi.org/10.1016/j.glohj.2024.08.002
9. Sheikhtaheri A, Taheri Moghadam S. Challenges and facilitators of using smartphones in educational activities: medical and nursing students' perspective. Studies in Health Technology and Informatics. 2022;293:234-241. https://doi.org/10.3233/SHTI220375
10. Byambasuren O, Sanders S, Beller E, Glasziou P. Prescribable mHealth apps identified from an overview of systematic reviews. NPJ Digital Medicine. 2018;1:12. https://doi.org/10.1038/s41746-018-0021-9
11. Dennison L, Morrison L, Conway G, Yardley L. Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study. Journal of Medical Internet Research. 2013;15(4):e86. https://doi.org/10.2196/jmir.2583
12. Fadaizadeh L, Sanaat M, Yousefi E, Alizadeh N. Mobile health: a comparative study of medical and health applications in Iran. Biomedical and Biotechnology Research Journal (BBRJ). 2022;6(2):249-54. https://doi.org/10.4103/bbrj.bbrj_31_22
13. Sun L, Yang B, Kindt E, Chu J. Privacy barriers in health monitoring: scoping review. Journal of Medical Internet Research Nursing. 2024;2(1):e53592. https://doi.org/10.2196/53592.
14. Rachayu I, Riyanto Y, Dewi U, Maiziani F, Ramazan R, Perwitasari S, Wulandari R. Implementation security and privacy in the era of industry 4.0 to protect digital attacks on health profession students: SOAR analysis. Journal of Posthumanism. 2025;5(2):487-501. https://doi.org/10.63332/joph.v5i2.434
15. Alipour J, Mehdipour Y, Zakerabasali S, Karimi A. Nurses' perspectives on using mobile health applications in southeastern Iran: awareness, attitude, and obstacles. PloS One. 2025;20(3):e0316631. https://doi.org/10.1371/journal.pone.0316631
16. Ghaddaripouri K, Mousavi Baigi SF, Abbaszadeh A, Mazaheri Habibi MR. Attitude, awareness, and knowledge of telemedicine among medical students: a systematic review of cross-sectional studies. Health Science Reports. 2023;6(3):e1156. https://doi.org/10.1002/hsr2.1156
17. Zhou L, Bao J, Watzlaf V, Parmanto B. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. JMIR mHealth and uHealth. 2019;7(4):e11223. https://doi.org/10.2196/11223
18. Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;3(2):77–101. https://doi.org/10.1191/1478088706qp063oa.
19. Atienza AA, Zarcadoolas C, Vaughon W, Hughes P, Patel V, Chou WY, Pritts J. Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study. Journal of Health Communication. 2015;20(6):673-9. https://doi.org/10.1080/10810730.2015.1018560
20. Peng W, Kanthawala S, Yuan S, Hussain SA. A qualitative study of user perceptions of mobile health apps. BMC Public Health. 2016;16:1-1. https://doi.org/10.1186/s12889-016-3808-0
21. Prasad A, Sorber J, Stablein T, Anthony D, Kotz D. Understanding sharing preferences and behavior for mHealth devices. In Proceedings of the 2012 ACM workshop on Privacy in the electronic society. 2012 Oct 15 (pp. 117-128). https://doi.org/10.1145/2381966.2381983
22. Mousavi Baigi SF, Mousavi AS, Kimiafar K, Sarbaz M. Evaluating the cost effectiveness of tele-rehabilitation: a systematic review of randomized clinical trials. Frontiers in Health Informatics. 2022;11. https://doi.org/10.30699/fhi.v11i1.368
23. Swain S, Muduli K, Kumar A, Luthra S. Analysis of barriers of mHealth adoption in the context of sustainable operational practices in health care supply chains. International Journal of Industrial Engineering and Operations Management. 2024;6(2):85-116. https://doi.org/10.1108/IJIEOM-12-2022-0067
24. Simblett S, Greer B, Matcham F, Curtis H, Polhemus A, Ferrão J, Gamble P, Wykes T. Barriers to and facilitators of engagement with remote measurement technology for managing health: systematic review and content analysis of findings. Journal of Medical Internet Research. 2018;20(7):e10480. https://doi.org/10.2196/10480
25. Aljedaani B, Ahmad A, Zahedi M, Ali Babar M. Security awareness of end-users of mobile health applications: an empirical study. InMobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services 2020 Dec 7 (pp. 125-136). Available form: https://arxiv.org/abs/2008.13009
26. Breitinger F, Tully-Doyle R, Hassenfeldt C. A survey on smartphone user's security choices, awareness and education. Computers & Security. 2020;88:101647. https://doi.org/10.1016/j.cose.2019.101647
27. Aval RN, Baigi SF, Sarbaz M, Kimiafar K. Security, privacy, and confidentiality in electronic prescribing systems: a review study. Frontiers in Health Informatics. 2022;11(1):115. https://doi.org/10.30699/fhi.v11i1.374
28. Nasiri S, Sadoughi F, Tadayon M H, Dehnad A. Security and privacy mechanisms of internet of things in healthcare and non-healthcare industry. Journal of Health Administration. 2019; 22 (4) :86-105 [In Persian]. Available form: http://jha.iums.ac.ir/article-1-3233-en.html
29. Rezaee R, Khashayar M, Saeedinezhad S, Nasiri M, Zare S. Critical criteria and countermeasures for mobile health developers to ensure mobile health privacy and security: mixed methods study. JMIR mHealth and uHealth. 2023;11:e39055. https://doi.org/10.2196/39055

نشریه مدیریت سلامت
https://jha.iums.ac.ir/
دانشگاه علوم پزشکی ایران

مقاله اصیل

موانع و تسهیل‌کننده‌های امنیتی در استفاده از برنامه‌های سلامت همراه از دیدگاه دانشجویان پیراپزشکی دانشگاه علوم پزشکی مشهد: یک مطالعه توصیفی–مقطعی

معصومه سرباز[1]، سیده فاطمه موسوی بایگی[1,2]، زهرا صالح زاده[1,2]، ریحانه نوروزی اول[1,2]، مجتبی اسماعیلی[1]، خلیل کیمیافر[1*]

[1] گروه فناوری اطلاعات سلامت، دانشکده علوم پیراپزشکی و توان‌بخشی، دانشگاه علوم پزشکی مشهد، مشهد، ایران.
[2] کمیته تحقیقات دانشجویی، دانشگاه علوم پزشکی مشهد، مشهد، ایران.

اطلاعات مقاله

نویسنده مسئول:
خلیل کیمیافر
رایانامه:
Kimiafarkh@mums.ac.ir

وصول مقاله: ۱۴۰۳/۰۳/۰۴
اصلاح نهایی: ۱۴۰۳/۰۶/۲۴
پذیرش نهایی: ۱۴۰۳/۰۶/۳۰
انتشارآنلاین: ۱۴۰۳/۱۰/۰۱

واژه‌های کلیدی:
امنیت
حریم خصوصی
اپلیکیشن سلامت همراه
موانع امنیتی
تسهیل‌کننده‌های امنیتی

چکیده

مقدمه: برنامه‌های سلامت همراه (mHealth) به‌عنوان ابزاری مؤثر برای مدیریت سلامت و بهبود کیفیت مراقبت‌های سلامت شناخته شده‌اند. بااین‌حال، نگرانی‌های مرتبط با امنیت اطلاعات و حریم خصوصی از موانع اصلی پذیرش این فناوری‌ها است. این مطالعه با هدف شناسایی موانع و تسهیل‌کننده‌های امنیتی استفاده از برنامه‌های سلامت همراه از دیدگاه دانشجویان پیراپزشکی انجام شد.

روش‌ها: این پژوهش مقطعی-توصیفی در سال ۱۴۰۲ روی ۱۱۵ دانشجوی پیراپزشکی دانشگاه علوم پزشکی مشهد انجام شد. نمونه‌گیری به روش طبقه‌ای متناسب با حجم انجام شد. ابزار جمع‌آوری داده‌ها پرسشنامه‌ای ساختاریافته بود که توسط ژو و همکاران طراحی و پس از ترجمه فارسی، بازترجمه و تأیید روایی و پایایی (ضریب همبستگی: ۹۲ درصد) بومی‌سازی شد. پرسشنامه شامل سوالات بسته (طیف لیکرت) و سوالات باز بود. تحلیل سوالات بسته با آمار توصیفی و تحلیل سوالات باز به روش تحلیل موضوعی (Thematic Analysis) انجام شد.

یافته‌ها: نتایج نشان داد نگرانی‌های امنیتی مانند دسترسی غیرمجاز به اطلاعات و ضعف در سیاست‌های حریم خصوصی، موانع اصلی استفاده از برنامه‌های سلامت همراه بودند. در مقابل، قابلیت حذف داده‌ها از راه دور، شفافیت در سیاست‌های امنیتی و کنترل دسترسی به‌عنوان تسهیل‌کننده‌های کلیدی شناسایی شدند. همچنین، تحلیل کیفی پاسخ‌های باز سه مضمون اصلی شامل نگرانی‌های امنیتی، مشکلات کاربردی و راهکارهای پیشنهادی برای بهبود امنیت و اعتمادپذیری برنامه‌ها را نشان داد.

نتیجه‌گیری: این پژوهش نشان می‌دهد که طراحی برنامه‌های سلامت همراه با تمرکز بر تقویت امنیت اطلاعات، شفافیت در سیاست‌های حریم خصوصی و سادگی کاربرد می‌تواند اعتماد کاربران را افزایش داده و پذیرش این فناوری‌ها را بهبود بخشد.

آنچه می‌دانیم:

- برنامه‌های سلامت همراه (mHealth) ابزارهای مهمی برای بهبود دسترسی به خدمات سلامت و افزایش تعامل کاربران با سیستم‌های درمانی هستند.
- ملاحظات امنیتی و حریم خصوصی از عوامل کلیدی در پذیرش یا عدم پذیرش برنامه‌های سلامت همراه محسوب می‌شوند.
- رمزگذاری داده‌ها، کنترل‌های دسترسی چندسطحی و سیاست‌های شفاف حریم خصوصی در افزایش اعتماد کاربران مهم است.

آنچه این مطالعه اضافه کرده است:

- سه دسته اصلی از موانع امنیتی در استفاده از برنامه‌های سلامت شامل نگرانی از دسترسی غیرمجاز به داده‌های شخصی و احتمال نقض حریم خصوصی، ابهام در سیاست‌های امنیتی و نبود شفافیت در نحوه مدیریت اطلاعات کاربران و محدودیت‌های کاربران در کنترل و حذف اطلاعات ذخیره‌شده در این برنامه‌ها است.
- سه عامل کلیدی تسهیل‌کننده پذیرش برنامه‌های سلامت همراه از بُعد امنیتی شامل امکان حذف از راه دور داده‌های شخصی در صورت سرقت یا مفقود شدن دستگاه، سیاست‌های امنیتی شفاف و ارایه اطلاعات واضح درباره نحوه حفاظت از داده‌ها و طراحی رابطهای کاربری کاربرپسند درراستای افزایش اعتماد به روش‌های امنیتی برنامه است.
- درک دانشجویان از امنیت و حریم خصوصی در برنامه‌های سلامت همراه می‌تواند مستقیماً بر پذیرش یا رد این فناوری تأثیر بگذارد.

مقدمه

برنامه‌های سلامت همراه (mHealth) به‌عنوان ابزارهایی مؤثر برای مدیریت سلامت و بهبود کیفیت مراقبت‌های سلامت، در سال‌های اخیر رشد چشمگیری داشته‌اند. این برنامه‌ها با تسهیل دسترسی به اطلاعات سلامت، ارتقای خودمدیریتی بیماران و بهبود تعامل بین بیماران و متخصصان سلامت، تحول مهمی در سیستم‌های سلامت ایجاد کرده‌اند [۲، ۳]. افزون‌براین، فناوری‌های سلامت همراه با بهره‌گیری از دستگاه‌های هوشمند پوشیدنی، امکان نظارت لحظه‌ای بر شاخص‌های سلامت را فراهم کرده‌اند [۴]. باوجود مزایای فراوان، نگرانی‌های امنیتی و حریم خصوصی کاربران یکی از موانع اصلی پذیرش این فناوری‌ها است [۵]. مطالعات نشان داده‌اند که حدود ۴۰ درصد کاربران به دلیل نگرانی درباره نشت اطلاعات شخصی یا سوءاستفاده از داده‌ها، از نصب یا ادامه استفاده از این برنامه‌ها خودداری می‌کنند [۶]. چالش‌های امنیتی شامل سیاست‌های غیرشفاف حفظ حریم خصوصی، پیچیدگی تنظیمات امنیتی و عدم کنترل کاربران بر داده‌های خود است [۷]. کاربران انتظار دارند این برنامه‌ها دارای ویژگی‌هایی مانند رمزگذاری داده‌ها، حذف اطلاعات از راه دور و کنترل دسترسی چندسطحی باشند تا اعتمادشان تقویت شود [۸، ۹].

در ایران، استفاده از تلفن‌های هوشمند به‌سرعت گسترش یافته است اما اطلاعات محدودی درباره نگرانی‌های امنیتی و حریم خصوصی کاربران در دسترس است [۱۰]. پژوهش‌های داخلی، مانند مطالعه‌ای در سال ۲۰۲۲، نشان داده‌اند که برنامه‌های سلامت همراه می‌توانند در آموزش و یادگیری دانشجویان علوم پزشکی مؤثر باشند اما چالش‌هایی مانند امنیت اطلاعات و نیاز به توسعه قابلیت‌های کاربرپسند همچنان مطرح هستند [۱۱، ۱۲]. تحقیقات اخیر تأکید دارند که طراحی برنامه‌های سلامت همراه با ویژگی‌هایی مانند شفافیت در سیاست‌های حفظ حریم خصوصی، کنترل دسترسی و قابلیت حذف داده‌ها از راه دور می‌تواند پذیرش این فناوری‌ها را افزایش دهد [۱۳، ۸]. به‌عنوان نمونه، مطالعه‌ای در سال ۲۰۲۱ به نقش کلیدی قابلیت‌های امنیتی و دسترسی آسان در افزایش اعتماد و پذیرش سلامت همراه اشاره کرده است [۶]. بااین‌حال، کمبود اطلاعات جامع درباره موانع و تسهیل‌کننده‌های امنیتی در میان دانشجویان علوم پزشکی و پیراپزشکی در ایران، نیاز به انجام مطالعات بیشتر را نشان می‌دهد [۱۲، ۱۴-۱۶].

دانشجویان پیراپزشکی به‌عنوان متخصصان آینده حوزه سلامت، نقش کلیدی در به‌کارگیری و ترویج فناوری‌های سلامت همراه در محیط‌های درمانی ایفا می‌کنند. این گروه کاربران بالقوه این برنامه‌ها هستند، و همچنین، در آینده به‌عنوان ارایه‌دهندگان خدمات سلامت، باید بتوانند امنیت اطلاعات بیماران را تأمین و ارزیابی کنند. درک نگرش و دغدغه‌های این گروه درباره امنیت برنامه‌های سلامت همراه می‌تواند اطلاعات ارزشمندی برای توسعه برنامه‌های ایمن‌تر و بهینه‌تر فراهم کند. علاوه‌براین، با توجه به افزایش دیجیتالی‌شدن خدمات سلامت و نقش فزاینده برنامه‌های سلامت همراه در آموزش و ارایه خدمات درمانی، بررسی دیدگاه دانشجویان پیراپزشکی در این زمینه می‌تواند به شناسایی خلأهای موجود و ارایه راهکارهای عملی برای افزایش امنیت و اعتماد کاربران کمک کند. بنابراین، این مطالعه با هدف شناسایی موانع و تسهیل‌کننده‌های امنیتی در استفاده از سلامت همراه از دیدگاه دانشجویان پیراپزشکی دانشگاه علوم پزشکی مشهد انجام شد. یافته‌های این تحقیق می‌تواند به توسعه‌دهندگان و سیاست‌گذاران در طراحی بهتر برنامه‌های سلامت همراه و تدوین راهکارهایی برای ارتقای امنیت و حریم خصوصی کمک کند.

روش ها

طراحی مطالعه: این پژوهش یک مطالعه مقطعی- توصیفی است که در سال ۱۴۰۲ در دانشگاه علوم پزشکی مشهد انجام شد.

جامعه و حجم نمونه: جامعه آماری شامل دانشجویان پیراپزشکی در رشته‌های مختلف مانند رادیولوژی، فیزیوتراپی، علوم آزمایشگاهی، گفتاردرمانی، کاردرمانی، فناوری اطلاعات سلامت و مددکاری اجتماعی بود. روش نمونه‌گیری به‌صورت طبقه‌ای متناسب با حجم (Proportional Stratified Sampling) انجام شد. حجم نمونه اولیه با استفاده از فرمول کوکران و با در نظر گرفتن سطح اطمینان ۹۵ درصد و خطای ۵ درصد برابر با ۸۷ نفر برآورد شد. بااین‌حال، به‌منظور جبران ریزش احتمالی پاسخ‌دهندگان و افزایش قابلیت تعمیم‌پذیری یافته‌ها، تعداد نمونه نهایی به ۱۱۵ نفر افزایش یافت.

ابزار جمع‌آوری داده‌ها: پرسشنامه پژوهش بر اساس ابزار استاندارد توسعه‌یافته توسط ژو و همکاران [۱۷] طراحی شد که مراحل ترجمه و بومی‌سازی آن مطابق با استانداردهای علمی بین‌المللی انجام گرفت. این پرسشنامه شامل دو بخش اصلی برای بررسی دیدگاه‌ها درباره امنیت و حریم خصوصی سلامت همراه است.

- سؤالات بسته (کمی): این بخش شامل ۱۴ سؤال بسته در قالب طیف لیکرت هفت گزینه‌ای (از کاملاً موافق تا کاملاً مخالف) بود. این سؤالات برای بررسی نگرش‌های دانشجویان نسبت به امنیت داده‌ها، حریم خصوصی، قابلیت‌های حفاظتی مانند رمزگذاری اطلاعات، قابلیت حذف از راه دور، کنترل دسترسی و سیاست‌های حفظ حریم خصوصی طراحی شد.
- سؤالات باز (کیفی): این بخش شامل چهار سؤال باز بود که برای کشف بینش‌های عمیق‌تر و ارایه توضیحات کیفی از تجربیات و انتظارات دانشجویان درباره موانع و تسهیل‌کننده‌های امنیتی طراحی شد. این سؤالات به بررسی موارد زیر پرداختند: موانع کلیدی در اعتماد به سلامت همراه (به‌عنوان نمونه، ترس از نشت داده‌ها یا دسترسی غیرمجاز)، ویژگی‌های امنیتی و حریم خصوصی مورد انتظار (مانند گزینه‌های مدیریت اجازه دسترسی و شفافیت در سیاست‌های حفظ اطلاعات)، توصیه‌ها برای بهبود قابلیت‌های امنیتی بر اساس نیازها و تجربیات شخصی.
- فرآیند ترجمه و بومی‌سازی ابزار: پرسشنامه از زبان انگلیسی به فارسی ترجمه شد و سپس فرآیند بازترجمه توسط دو متخصص دوزبانه انجام شد. پس از مقایسه نسخه ترجمه شده با نسخه اصلی، اصلاحات لازم برای تطابق فرهنگی و معنایی ابزار اعمال گردید. نسخه نهایی پرسشنامه توسط یک هیئت تخصصی شامل پنج عضو هیئت علمی از رشته های انفورماتیک پزشکی (تعداد: ۲)، مدیریت اطلاعات سلامت (تعداد: ۱)، آمار زیستی (تعداد: ۱) و فناوری اطلاعات سلامت (تعداد: ۱) بررسی و اعتبار محتوایی آن تأیید شد.

- اعتبار و پایایی ابزار: اعتبار پرسشنامه از نظر صوری و محتوایی با استفاده از نظرات متخصصان ارزیابی شد. برای بررسی پایایی، پرسشنامه با استفاده از روش آزمون بازآزمون (Test-Retest) در یک فاصله ۱۰ روزه به ۲۰ نفر از دانشجویان ارایه شد. مقدار ضریب همبستگی پیرسون ۰/۹۲ برای کل پرسشنامه به‌دست آمد که نشان‌دهنده پایایی بالا و قابلیت اعتماد ابزار بود.

روش گردآوری داده‌ها: پرسشنامه‌ها به‌صورت الکترونیکی از طریق سامانه‌های ارتباطی دانشگاه و گروه‌های دانشجویی توزیع شدند. شرکت‌کنندگان به‌طور داوطلبانه در مطالعه شرکت کردند و رضایت‌نامه آگاهانه الکترونیکی قبل از تکمیل پرسشنامه اخذ شد.

تحلیل داده‌ها: داده‌های کمی به کمک نرم‌افزار SPSS نسخه ۲۶ تحلیل شدند. برای تحلیل این داده‌ها، آمار توصیفی شامل میانگین، انحراف معیار، فراوانی و درصد به‌کار گرفته شد. برای تحلیل داده‌های کیفی حاصل از سؤالات باز، روش تحلیل موضوعی (Thematic Analysis) مطابق با مدل براون و کلارک [۱۸] مورد استفاده قرار گرفت. مراحل تحلیل به شرح زیر انجام شد:۱) آشنایی با داده‌ها: خواندن مکرر پاسخ‌ها برای درک عمیق؛ ۲) کدگذاری اولیه: شناسایی مفاهیم و کدگذاری آنها بر اساس محتوای پاسخ‌ها؛ ۳) تشکیل مضامین: گروه‌بندی کدها در مضامین اصلی؛ ۴) بازبینی مضامین: مرور مضامین برای اطمینان از ارتباط با داده‌ها؛ ۵) تعریف و نام‌گذاری مضامین: توضیح واضح هر مضمون؛ ۶) تهیه گزارش نهایی: مستندسازی یافته‌ها به‌صورت منسجم. برای افزایش دقت تحلیل کیفی، بررسی نتایج توسط دو کدگذار مستقل انجام شد و اختلاف‌نظرها از طریق اجماع گروهی حل شد. همچنین، نتایج با ۱۵ نفر از شرکت‌کنندگان به اشتراک گذاشته شد تا فرآیند بازبینی و تأیید توسط مشارکت‌کنندگان انجام شود و تفاسیر به تأیید آنان برسد.

یافته ها

در این مطالعه، ۱۱۵ دانشجوی پیراپزشکی از رشته‌های مختلف از جمله رادیولوژی، فیزیوتراپی، علوم آزمایشگاهی، گفتاردرمانی، کاردرمانی، فناوری اطلاعات سلامت و مددکاری اجتماعی شرکت کردند (نرخ پاسخ‌دهی: ۹۶ درصد). مطابق با جدول یک، میانگین سنی شرکت‌کنندگان ۲۳/۵۱ سال با انحراف معیار ۴/۲ بود. اکثریت شرکت‌کنندگان زن (۶۴/۳ درصد) و مجرد (۸۴/۳ درصد) بودند. توزیع پاسخ‌ها نشان داد که اکثر شرکت‌کنندگان دارای تجربه استفاده از برنامه‌های سلامت همراه بودند، اما نگرانی‌هایی درباره امنیت و حریم خصوصی اطلاعات خود در این برنامه‌ها داشتند.

جدول ۱. ویژگی‌های جمعیت‌شناختی

متغیر		فراوانی	درصد
جنسیت	مرد	۴۱	۳۵/۷
	زن	۷۴	۶۴/۳
وضعیت تأهل	مجرد	۹۷	۸۴/۳
	متأهل	۱۸	۱۵/۷
رشته تحصیلی	فیزیوتراپی	۵	۴/۳
	گفتاردرمانی	۱۵	۱۳/۰
	بینایی‌سنجی	۱۹	۱۶/۵
	فناوری اطلاعات سلامت	۳۷	۳۲/۲
	رادیولوژی	۱۱	۹/۶
	علوم آزمایشگاهی	۱۵	۱۳/۰
	مددکاری اجتماعی	۹	۷/۸
مقطع تحصیلی	کارشناسی ناپیوسته	۱	۰/۹
	کارشناسی پیوسته	۹۹	۸۶/۱
	کارشناسی‌ارشد	۱۴	۱۲/۲
	دکترای تخصصی	۱	۰/۹

تحلیل کمی: در جدول دو، نظرات دانشجویان در رابطه با داده های شخصی نشان داده شده است. اکثریت دانشجویان کاملا موافق، موافق و تا حدودی موافق (۸۱/۷ درصد) بودند که نگران حفظ حریم خصوصی و امنیت اطلاعات شخصی خود در زندگی روزمره شان هستند. علاوه‌براین، اکثریت آنان (۶۷/۹ درصد) بیان کردند که هنگام استفاده از نرم‌افزار های سلامت همراه نگران حریم خصوصی و امنیت اطلاعات شخصی خود هستند. اکثریت دانشجویان (۶۷/۹ درصد) اظهار کردند که نگران ارسال اطلاعات شخصی در یک نرم‌افزار سلامت همراه هستند زیرا ممکن است در معرض دستکاری دیگران قرار گیرد. همچنین اکثریت دانشجویان (۷۰/۴ درصد) بیان کردند که مایل نیستند اطلاعات شخصی خود (مانند نام، کدملی، شماره تلفن، آدرس ایمیل) را در نرم‌افزار های سلامت همراه ذخیره کنند، به جز یک شماره شناسایی منحصر به فرد که فقط توسط کارکنان مجاز قابل ردیابی است. ۸۸/۶ درصد دانشجویان نیز اظهار موافقت کردند که مایلند اطلاعات سلامت شخصی شان از طریق یک فرآیند بسیار امن به پایگاه داده متمرکز منتقل شود.

جدول ۲. نظرات در رابطه با داده‌های شخصی دانشجویان

نظرات در رابطه با داده‌های شخصی	تعداد (درصد)					
	کاملاً موافقم	موافقم	تا حدودی موافقم	نظری ندارم	تا حدودی مخالفم	مخالفم	کاملاً مخالفم
۱. به‌طور کلی، من نگران حفظ حریم خصوصی و امنیت اطلاعات شخصی خود در زندگی روزمره هستم.	۴۶ (۴۰/۰)	۲ (۱۹/۱)	۲۶ (۲۲/۶)	۱۳ (۱۱/۳)	۷ (۶/۱)	۱ (۰/۹)	۰
۲. هنگام استفاده از نرم‌افزارهای سلامت‌همراه نگران حریم خصوصی و امنیت اطلاعات شخصی خود هستم.	۳۳ (۲۸/۷)	۲۷ (۲۳/۵)	۱۸ (۱۵/۷)	۱۶ (۱۳/۹)	۱۱ (۹/۶)	۸ (۷/۰)	۲ (۱/۷)
۳. من نگران ارسال اطلاعات شخصی در نرم‌افزار سلامت همراه هستم زیرا ممکن است در معرض دستکاری دیگران قرار گیرد.	۲۶ (۲۲/۶)	۲۴ (۲۰/۹)	۳۲ (۲۷/۸)	۱۲ (۱۰/۴)	۱۰ (۸/۷)	۶ (۵/۲)	۵ (۴/۳)
۴. مایل نیستم اطلاعات شخصی خود (مانند نام، کدملی، شماره تلفن، آدرس ایمیل) را در نرم‌افزارهای سلامت همراه ذخیره کنم، به جز یک شماره شناسایی منحصر به فرد که فقط توسط کارکنان مجاز قابل ردیابی است.	۳۹ (۳۳/۹)	۲۷ (۲۳/۵)	۱۵ (۱۳/۰)	۱۴ (۱۲/۲)	۸ (۷/۰)	۱۰ (۸/۷)	۲ (۱/۷)
۵. مایلم اطلاعات سلامت شخصی من از طریق فرآیند بسیار امن به پایگاه داده متمرکز منتقل شود.	۶۱ (۵۳/۰)	۲۹ (۲۵/۲)	۱۲ (۱۰/۴)	۷ (۶/۱)	۱ (۰/۹)	۲ (۱/۷)	۳ (۲/۶)

مطابق با جدول ۳، اکثریت دانشجویان در پاسخ به دو سؤال "به‌طورکلی، من از حریم خصوصی و امنیت نرم‌افزارهای سلامت همراه که در حال حاضر استفاده می‌کنم راضی هستم" و " توسعه‌دهندگان و ارایه‌دهندگان مراقبت‌های بهداشتی اقدامات امنیتی و حریم خصوصی لازم را در محل دارند. این اقدامات سطح معقولی از محافظت را برای اطلاعات جمع‌آوری‌شده از نرم‌افزارهای سلامت همراه فراهم می‌کند" اظهار کردند که نظری ندارند. ۴۲/۶ درصد از دانشجویان بیان کردند که از نرم‌افزار های سلامت همراه برای نیازهای مراقبت‌های سلامت خود استفاده می‌کنند. علاوه‌براین، ۵۲/۲ درصد دانشجویان اظهار کردند که از ارایه‌دهندگان مراقبت‌های سلامت می‌خواهند که از نرم‌افزارهای سلامت همراه برای ذخیره و مدیریت اطلاعات سلامت استفاده کنند. همچنین، ۶۸/۷ درصد دانشجویان اظهار موافقت کردند که اگر اطلاعات سلامتی آنها برای اهداف مراقبتی در میان پزشکان و درمانگران به‌اشتراک گذاشته شود، احساس راحتی می‌کنند.

جدول ۳. نظرات دانشجویان در رابطه با نرم‌افزارهای سلامت همراه

ویژگی‌های موردنظر در نرم‌افزارهای سلامت همراه	تعداد (درصد)						
	کاملاً موافقم	موافقم	تا حدودی موافقم	نظری ندارم	تا حدودی مخالفم	مخالفم	کاملاً مخالفم
۶. به‌طور کلی، من از حریم خصوصی و امنیت نرم‌افزارهای سلامت همراه که در حال حاضر استفاده می‌کنم، راضی هستم.	۱۰ (۸/۷)	۱۵ (۱۳/۰)	۲۱ (۱۸/۳)	۵۱ (۴۴/۳)	۹ (۷/۸)	۶ (۵/۲)	۳ (۲/۶)
۷. توسعه‌دهندگان و ارایه‌دهندگان مراقبت‌های سلامت اقدامات امنیتی و حریم خصوصی لازم را در محل دارند. این اقدامات سطح معقولی از محافظت را برای اطلاعات جمع‌آوری شده از نرم‌افزارهای سلامت همراه فراهم می‌کنند.	۶ (۵/۲)	۱۷ (۱۴/۸)	۳۰ (۲۶/۱)	۴۲ (۳۶/۵)	۶ (۵/۲)	۱۲ (۱۰/۴)	۲ (۱/۷)
۸. من از نرم‌افزارهای سلامت همراه برای نیازهای مراقبت‌های سلامت خود استفاده می‌کنم.	۳ (۲/۶)	۲۲ (۱۹/۱)	۲۴ (۲۰/۹)	۲۵ (۲۱/۷)	۱۵ (۱۳/۰)	۱۴ (۱۲/۲)	۱۲ (۱۰/۴)
۹. من از ارایه‌دهندگان مراقبت‌های سلامت می‌خواهم که از نرم‌افزارهای سلامت همراه برای ذخیره و مدیریت اطلاعات سلامت من استفاده کنند.	۱۸ (۱۵/۷)	۲۲ (۱۹/۱)	۲۰ (۱۷/۴)	۲۲ (۱۹/۱)	۱۷ (۱۴/۸)	۵ (۴/۳)	۶ (۵/۲)
۱۰. اگر اطلاعات سلامتی من برای اهداف مراقبتی من در میان پزشکان و درمانگرانم به اشتراک گذاشته شود، احساس راحتی می‌کنم.	۱۴ (۱۲/۲)	۲۸ (۲۴/۳)	۳۷ (۳۲/۲)	۲۱ (۱۸/۳)	۸ (۷/۰)	۳ (۲/۶)	۴ (۳/۵)

مطابق با جدول چهار، اکثریت دانشجویان (۵۰/۴ درصد) کاملا موافق بودند که باید این حق را داشته باشند که با هر گونه اشتراک‌گذاری محافظت‌شده اطلاعات مراقبت سلامت از طریق نرم‌افزارهای سلامت همراه موافقت کنند. ۸۲/۶ درصد از دانشجویان موافق و کاملا موافق بودند که می‌خواهند بدانند چگونه توسعه‌دهندگان و ارایه‌دهندگان مراقبت مطمئن می‌شوند که فقط کارکنان مجاز به نرم‌افزارهای سلامت همراه دسترسی دارند. همچنین، اکثریت دانشجویان (۷۷/۴درصد) اظهار موافقت کردند که می‌خواهند این دسترسی را داشته باشند که در صورت مفقود یا سرقت شدن، بتوانند تمام داده‌های سلامتی خود را از راه دور از روی دستگاه تلفن همراه خود حذف کنند.

جدول ۴. ویژگی‌های مورد نظر دانشجویان در رابطه با نرم‌افزارهای سلامت همراه

ویژگی‌های موردنظر در نرم‌افزارهای سلامت همراه	تعداد (درصد)					
	کاملاً موافقم	موافقم	تا حدودی موافقم	نظری ندارم	تا حدودی مخالفم	مخالفم	کاملاً مخالفم
۱۱. من باید این حق را داشته باشم که با هر گونه اشتراک‌گذاری محافظت شده اطلاعات مراقبت سلامتم که از طریق نرم‌افزارهای سلامت همراه جمع‌آوری شده، موافقت کنم.	(۵۰/۴)۵۸	(۲۸/۷)۳۳	(۱۲/۲)۱۴	(۶/۱) ۷	(۱/۷) ۲	(۰/۹)۱	۰
۱۲. من می‌خواهم بدانم چگونه توسعه‌دهندگان و ارایه‌دهندگان مراقبت‌های سلامت من مطمئن می‌شوند که فقط کارکنان مجاز به نرم‌افزارهای سلامت همراه که من استفاده می‌کنم دسترسی دارند.	(۴۸/۷)۵۶	(۳۳/۹)۳۹	(۷/۸) ۹	(۷/۰) ۸	(۲/۶) ۳	۰	۰
۱۳. من سیاست‌های حفظ حریم خصوصی نرم‌افزارهای سلامت همراه را خوانده‌ام. محتوای خط‌مشی‌ها بر تصمیم من در مورد استفاده از نرم‌افزار تأثیر می‌گذارد.	(۱۶/۵)۱۹	(۲۹/۶)۳۴	(۳۱/۳) ۳۶	(۱۳/۹)۱۶	(۳/۵) ۴	(۲/۶)۳	۰
۱۴. می‌خواهم این دسترسی را داشته باشم که در صورت مفقود یا سرقت شدن، بتوانم تمام داده‌های سلامتی خود را از راه دور از روی دستگاه تلفن همراه خود حذف کنم.	(۱۶/۵)۱۹	(۲۹/۶)۳۴	(۳۱/۳) ۳۶	(۱۳/۹)۱۶	(۳/۵) ۴	(۲/۶)۳	(۲/۶) ۳

تحلیل کیفی: تحلیل داده‌های کیفی به روش تحلیل موضوعی، سه مضمون اصلی را آشکار کرد: ۱) نگرانی‌های امنیتی: این مضمون بر ترس کاربران از نشت اطلاعات، سوءاستفاده احتمالی از داده‌های شخصی و عدم شفافیت در سیاست‌های امنیتی برنامه‌ها متمرکز بود. بسیاری از شرکت‌کنندگان ابراز نگرانی کردند که اطلاعات حساس آنها ممکن است بدون اطلاع و رضایت‌شان مورد استفاده قرار گیرد. ۲) چالش‌های عملی: این مضمون به مشکلاتی اشاره داشت که کاربران در استفاده از نرم‌افزارهای سلامت همراه با آن مواجه بودند، از جمله پیچیدگی رابط کاربری، ضعف زیرساخت‌های امنیتی و دشواری مدیریت دسترسی‌ها. این چالش‌ها به‌ویژه در میان کاربران با دانش فنی پایین‌تر محسوس‌تر بود، زیرا این دسته از کاربران درک محدودی از نحوه تنظیم و استفاده از قابلیت‌های امنیتی این نرم‌افزارها داشتند و نیاز به راهنمایی و آموزش بیشتری احساس می‌کردند. برخی از شرکت‌کنندگان بیان کردند که به دلیل ناآشنایی با تنظیمات امنیتی، در مدیریت دسترسی‌ها و حفاظت از داده‌های شخصی خود دچار مشکل می‌شوند. ۳) پیشنهادهای بهبود: این مضمون شامل پیشنهادهایی برای افزایش امنیت و اعتماد کاربران بود، از جمله رمزگذاری پیشرفته، کنترل دسترسی چندسطحی و توسعه سیاست‌های شفاف حریم خصوصی. برخی شرکت‌کنندگان پیشنهاد دادند که نرم‌افزارهای سلامت همراه باید راهکارهایی ارایه دهند که به کاربران امکان دهد تنظیمات امنیتی را ساده‌تر مدیریت کنند و در شرایط اضطراری، داده‌های خود را از راه دور حذف نمایند.

بحث

مطالعه حاضر به بررسی موانع و تسهیل‌کننده‌های امنیتی در پذیرش برنامه‌های سلامت همراه از دیدگاه دانشجویان علوم پیراپزشکی پرداخت. یافته‌ها براساس تحلیل داده‌های کمی و کیفی، شامل سه مضمون اصلی نگرانی‌های امنیتی، چالش‌های عملی و پیشنهادهای بهبود، نشان داد که امنیت اطلاعات و حریم خصوصی همچنان موانع اصلی پذیرش این فناوری‌ها هستند. این نتایج در مقایسه با مطالعات بین‌المللی، نکات مهمی برای توسعه فناوری‌های سلامت همراه ایمن و کاربرپسند ارایه می‌کند.

نگرانی‌های امنیتی(اولویت اصلی کاربران): یکی از یافته‌های کلیدی این مطالعه، نگرانی گسترده شرکت‌کنندگان در مورد امنیت اطلاعات و حریم خصوصی بود. نتایج کمی نشان داد که بیش از ۸۲/۶ درصد دانشجویان بر اهمیت کنترل دسترسی و اطمینان از محافظت اطلاعات تأکید داشتند. علاوه‌براین، ۷۷/۴ درصد شرکت‌کنندگان تمایل داشتند قابلیت حذف داده‌ها از راه دور در صورت سرقت یا گم شدن

دستگاه تلفن همراه را داشته باشند. این نتایج با یافته‌های کربس و همکاران [۵] مطابقت دارد که نشان داد ۴۰ درصد کاربران در ایالات متحده به دلیل نگرانی‌های امنیتی، از نصب برنامه‌های سلامت همراه خودداری کردند. مطالعات مشابه، ازجمله پژوهش آتینزا و همکاران [۱۹] نیز به ارتباط نگرش کاربران با امنیت اطلاعات تأکید داشتند و نشان دادند که شفافیت در سیاست‌های امنیتی و کنترل دسترسی نقش کلیدی در اعتمادسازی دارد. مطالعه پنگ و همکاران [۲۰] نیز نشان داد که کاربران، به‌ویژه جوان‌ترها، نسبت به اشتراک‌گذاری اطلاعات حساس در شبکه‌های اجتماعی حساس بوده و خواستار کنترل بیشتری بر روی داده‌های خود هستند. این نتایج نشان می‌دهد که برنامه‌های سلامت همراه برای جلب اعتماد کاربران نیازمند سیاست‌های امنیتی شفاف، قابلیت رمزگذاری پیشرفته و دسترسی چندسطحی هستند.

چالش‌های عملی (ضعف زیرساخت‌ها و پیچیدگی سیستم‌ها): تحلیل کیفی نشان داد که کاربران علاوه بر نگرانی‌های امنیتی، با چالش‌های عملی مانند پیچیدگی رابط‌های کاربری، ضعف زیرساخت‌های امنیتی و دشواری مدیریت دسترسی‌ها روبه‌رو بودند. این مشکلات به‌ویژه در میان کاربران با دانش فنی پایین‌تر، چالش‌های بیشتری ایجاد کرد، زیرا این دسته از کاربران نیاز به راهنمایی بیشتری برای استفاده از قابلیت‌های امنیتی موجود در نرم‌افزارهای سلامت همراه داشتند. این یافته‌ها با مطالعه فدائی‌زاده و همکاران همخوانی دارد که نشان داد هزینه‌های بالا، پیچیدگی رابط کاربری، و قابلیت اعتماد پایین، از موانع اصلی پذیرش فناوری‌های سلامت همراه هستند [۱۲]. پژوهش بیامباسورن و همکاران [۱۰] نیز به چالش‌های مشابهی اشاره کرد و افزود که عدم دسترسی به اطلاعات قابل اعتماد و آگاهی پایین کاربران، پذیرش این برنامه‌ها را محدود می‌کند. همچنین، مطالعه پراساد و همکاران [۲۱] بر اهمیت مدیریت چندسطحی داده‌ها و امکان حذف اطلاعات در شرایط اضطراری تأکید کرد. پژوهش بایگی و همکاران [۲۲] و سوین و همکاران [۲۳] به هزینه‌های بالا و محدودیت در زیرساخت‌ها به‌عنوان موانعی اشاره کرد که بر پذیرش فناوری‌های سلامت همراه تأثیر می‌گذارند.

پیشنهادهای بهبود(افزایش امنیت و اعتماد کاربران): براساس تحلیل کیفی، شرکت‌کنندگان پیشنهادهایی برای بهبود امنیت ارایه دادند که شامل رمزگذاری پیشرفته، کنترل دسترسی چندسطحی و تدوین سیاست‌های شفاف حریم خصوصی بود. این پیشنهادها با یافته‌های سیمبلت و همکاران [۲۴] همخوانی دارد که تأکید کردند قابلیت‌های امنیتی پیشرفته و نظارت بر دسترسی‌ها می‌تواند اعتماد کاربران را افزایش دهد. علاوه‌براین، پژوهش الجدانی و همکاران [۲۵] تأکید کرد که تدوین چارچوب‌های قانونی شفاف و ارایه مجوزهای امنیتی و اخلاقی می‌تواند موجب ارتقای اعتماد کاربران شود. مطالعه کونیگ و همکاران [۶] نیز با معرفی چارچوبی سه‌سطحی بر نقش انگیزه‌های کاربر، زیرساخت‌ها و تعامل اجتماعی در پذیرش فناوری‌های سلامت همراه تأکید داشت.

باتوجه‌به اثبات مؤثر و کارآمد بودن نرم‌افزارهای سلامت همراه و فقدان خط‌ومشی‌ها و سیاست‌های امنیتی در حوزه نرم‌افزارهای سلامت همراه در ایران پیشنهاد می‌گردد سیاست‌گذاران در این زمینه به طراحی چارچوب حداقلی برای حفظ امنیت و محرمانگی اطلاعات سلامت کاربران بپردازند. از سوی دیگر باتوجه‌به افزونی نرم‌افزارهای سلامت همراه و عدم شناسایی نرم‌افزارهای صحیح و موثق، شناسایی و ارزیابی صحیح این نرم‌افزارها در وهله اول قبل از اشتراک‌گذاری در جوامع بسیار حائز اهمیت می‌باشد. همچنین، لازم است آموزش امنیت برای کاربران نرم‌افزارهای تلفن همراه افزایش یابد تا آنها به‌خوبی از بسیاری از ویژگی‌های امنیتی موجود در تلفن‌های همراه خودآگاه باشند و بتوانند از این ویژگی‌ها برای محافظت از داده‌ها و حریم خصوصی خود استفاده کنند [۲۹-۲۶].

در نهایت، این مطالعه طیف گسترده‌ای از موانع و تسهیل‌کننده‌های امنیتی استفاده از نرم‌افزارهای سلامت همراه از دیدگاه دانشجویان علوم پیراپزشکی را نشان داد. نتایج حاصل از این پژوهش می‌تواند چراغ راهی برای راهنمایی توسعه‌دهندگان نرم‌افزارهای سلامت همراه برای ایجاد نرم‌افزارهای کارآمدتر و ایمن‌تر باشد که مورد استقبال کاربران نهایی آن قرار گیرند.

نقاط قوت و محدودیت‌ها: این مطالعه با استفاده از تحلیل ترکیبی داده‌های کمی و کیفی، بینش جامعی درباره موانع و تسهیل‌کننده‌های امنیتی ارایه داد. بااین‌حال، تعمیم‌پذیری نتایج به دلیل محدودیت در حجم نمونه و تمرکز بر دانشجویان علوم پیراپزشکی نیاز به احتیاط دارد. همچنین، داده‌های مربوط به هزینه-اثربخشی و اثرات طولانی‌مدت این فناوری‌ها بررسی نشده و پیشنهاد می‌شود در مطالعات آتی مورد توجه قرار گیرد.

نتیجه‌گیری و پیشنهادها برای مطالعات آینده: این مطالعه نشان داد که نگرانی‌های امنیتی، ضعف زیرساخت‌ها و پیچیدگی رابط‌های کاربری از موانع کلیدی پذیرش فناوری‌های سلامت همراه هستند. بااین‌حال، تمایل بالای کاربران برای استفاده از این برنامه‌ها در صورت بهبود ویژگی‌های امنیتی، فرصت‌های مهمی را برای توسعه‌دهندگان و سیاست‌گذاران فراهم می‌کند. با توجه به یافته‌های این مطالعه، توسعه فناوری‌های سلامت همراه با تأکید بر امنیت داده‌ها و قابلیت اعتماد، نیازمند رویکردهای چندوجهی است. یکی از پیشنهادهای کلیدی، به‌کارگیری رمزگذاری پیشرفته و کنترل دسترسی چندسطحی است که می‌تواند حفاظت از اطلاعات حساس کاربران را تقویت کرده و اعتماد آنها را نسبت به استفاده از این برنامه‌ها افزایش دهد. همچنین، تدوین سیاست‌های شفاف و استاندارد درباره حریم خصوصی و امنیت اطلاعات، گامی ضروری برای کاهش نگرانی‌های کاربران و تسهیل پذیرش این فناوری‌ها محسوب می‌شود.

از سوی دیگر، افزایش آموزش‌های کاربردی و برنامه‌های آگاهی‌رسانی در مورد چگونگی محافظت از داده‌ها و بهره‌برداری ایمن از قابلیت‌های سلامت همراه، به‌ویژه برای گروه‌های کاربری با دانش فنی محدودتر، می‌تواند میزان مشارکت و تعامل کاربران را بهبود بخشد. به‌علاوه، باتوجه‌به نگرانی‌های مالی که در برخی مطالعات پیشین نیز برجسته شده است، انجام پژوهش‌هایی برای ارزیابی هزینه-اثربخشی این برنامه‌ها و تدوین راهکارهایی برای به‌کارگیری گسترده‌تر آنها در سیستم‌های بهداشتی پیشنهاد می‌شود. در نهایت، طراحی مطالعات

طولانی‌مدت برای ارزیابی تأثیر ویژگی‌های امنیتی و قابلیت‌های فنی بر تغییر رفتار کاربران و میزان پذیرش این فناوری‌ها، به درک عمیق‌تر از موانع و تسهیل‌کننده‌های مرتبط کمک خواهد کرد. چنین پژوهش‌هایی می‌توانند به توسعه چارچوب‌های علمی و عملی منسجم برای برنامه‌های سلامت همراه منجر شده و مسیر را برای بهبود کیفیت مراقبت‌های بهداشتی هموار سازند.

اعلان ها

ملاحظات اخلاقی : این مطالعه برگرفته شده از طرح تحقیقاتی مصوب در دانشگاه علوم پزشکی مشهد می‌باشد (کد اخلاق : R.MUMS.FHMPM.REC.1401.086).

مدیریت داده، نگارش- بررسی و ویرایش، بصری‌سازی، تایید نهایی؛ **زهرا صالح زاده**: گردآوری داده و تایید نهایی؛ **ریحانه نوروزی اول**: گردآوری داده و تایید نهایی. **خلیل کیمیافر** (نویسنده مسئول): مفهوم‌سازی و طراحی مطالعه، روش‌شناسی، سرپرستی مطالعه، مدیریت پروژه، تامین مالی، منابع، تایید نهایی؛ **مجتبی اسماعیلی**: گردآوری داده و تایید نهایی.

رضایت برای انتشار: مورد ندارد.

دسترسی به داده‌ها: داده‌های این مطالعه از طریق ایمیل نویسنده مسئول با ذکر دلیل منطقی در دسترس است.

استفاده از هوش مصنوعی: برای ویرایش بخش انگلیسی این مقاله، از ChatGPT شرکت OpenAI استفاده شده است. کلیه محتوای ویرایش‌شده توسط این ابزار، به‌دقت توسط نویسندگان بازبینی و تأیید شده است.

تشکر و قدردانی: بدین‌وسیله از تمامی دانشجویان که با مشارکت ارزشمند خود در این مطالعه همکاری داشتند، صمیمانه سپاسگزاری می‌کنیم. همچنین، از کمیته تحقیقات دانشجویی دانشگاه علوم پزشکی مشهد به‌دلیل حمایت‌های علمی و پژوهشی سازنده، نهایت قدردانی و تشکر را داریم.

منابع

1. Saigí-Rubió F, Borges do Nascimento IJ. The current status of telemedicine technology yse across the WHO European region. Journal of Medical Internet Research. 2022;24(10):e40877. https://doi.org/10.2196/40877
2. Sheikhtaheri A, Hashemi N, Hashemi NA. Benefits of using mobile technologies in education from the viewpoints of medical and nursing students. Studies in Health Technology and Informatics. 2018;251:289-292. https://doi.org/10.3233/978-1-61499-880-8-289
3. Nemati-Anaraki L, Mousavi S S, AliBeyk M, Mahami-Oskouei M. Medical students knowledge and use of smartphone-based applications. Journal of Health Administration. 2022; 24 (4):84-94.

حمایت مالی: این مطالعه با حمایت مالی دانشگاه علوم پزشکی مشهد انجام شده است (کد طرح: ۴۰۰۲۰۸۰). حامی مالی نقشی در گردآوری و تحلیل داده و نگارش مقاله نداشته است.

تضاد منافع: نویسندگان اظهار داشتند که تضاد منافعی وجود ندارد.

سهم نویسندگان: معصومه سرباز: مفهوم‌سازی و طراحی مطالعه، گردآوری داده، روش‌شناسی، تحلیل داده، نگارش- پیش‌نویس، تایید نهایی؛ **سیده فاطمه موسوی بایگی**: گردآوری داده، اعتبارسنجی،

[In Persian]. https://doi.org/10.52547/jha.24.4.84
4. Sheikhtaheri A, Kermani F. Use of mobile apps among medical and nursing students in Iran. Studies in Health Technology and Informatics. 2018;248:33-39. https://doi.org/10.3233/978-1-61499-858-7-33
5. Krebs P, Duncan DT. Health app use among US mobile phone owners: a national survey. JMIR Mhealth Uhealth. 2015;3(4):e101. https://doi.org/10.2196/mhealth.4924
6. König L, Sproesser G, Schupp HT, Renner B. Describing the process of adopting nutrition and fitness apps: Behavior stages and determinants. JMIR Mhealth Uhealth. 2021;9(5):e22513. https://doi.org/10.2196/mhealth.8261
7. Sun L, Yang B, Kindt E, Chu J. Privacy barriers in health monitoring: scoping review. Journal of Medical Internet Research Nursing. 2024;2(1):e53592. https://doi.org/10.2196/53592
8. Mbunge E, Sibiya MN. Mobile health interventions for improving maternal and child health outcomes in south Africa: a systematic review. Global Health Journal. 2024;9(1):e41. https://doi.org/10.1016/j.glohj.2024.08.002
9. Sheikhtaheri A, Taheri Moghadam S. Challenges and facilitators of using smartphones in educational activities: medical and nursing students' perspective. Studies in Health Technology and Informatics. 2022;293:234-241. https://doi.org/10.3233/SHTI220375
10. Byambasuren O, Sanders S, Beller E, Glasziou P. Prescribable mHealth apps identified from an overview of systematic reviews. NPJ Digital Medicine. 2018;1:12. https://doi.org/10.1038/s41746-018-0021-9
11. Dennison L, Morrison L, Conway G, Yardley L. Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study. Journal of Medical Internet Research. 2013;15(4):e86. https://doi.org/10.2196/jmir.2583
12. Fadaizadeh L, Sanaat M, Yousefi E, Alizadeh N. Mobile health: a comparative study of medical and health applications in Iran. Biomedical and Biotechnology Research Journal (BBRJ). 2022;6(2):249-54. https://doi.org/10.4103/bbrj.bbrj_31_22

13.Sun L, Yang B, Kindt E, Chu J. Privacy barriers in health monitoring: scoping review. Journal of Medical Internet Research Nursing. 2024;2(1):e53592. https://doi.org/10.2196/53592.

14.Rachayu I, Riyanto Y, Dewi U, Maiziani F, Ramazan R, Perwitasari S, Wulandari R. Implementation security and privacy in the era of industry 4.0 to protect digital attacks on health profession students: SOAR analysis. Journal of Posthumanism. 2025;5(2):487-501. https://doi.org/10.63332/joph.v5i2.434

15.Alipour J, Mehdipour Y, Zakerabasali S, Karimi A. Nurses' perspectives on using mobile health applications in southeastern Iran: Awareness, attitude, and obstacles. PloS One. 2025;20(3):e0316631. https://doi.org/10.1371/journal.pone.0316631

16.Ghaddaripouri K, Mousavi Baigi SF, Abbaszadeh A, Mazaheri Habibi MR. Attitude, awareness, and knowledge of telemedicine among medical students: a systematic review of cross-sectional studies. Health Science Reports. 2023;6(3):e1156. https://doi.org/10.1002/hsr2.1156

17.Zhou L, Bao J, Watzlaf V, Parmanto B. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. JMIR mHealth and uHealth. 2019 Apr 16;7(4):e11223. https://doi.org/10.2196/11223

18.Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;3(2):77–101. https://doi.org/10.1191/1478088706qp063oa.

19.Atienza AA, Zarcadoolas C, Vaughon W, Hughes P, Patel V, Chou WY, Pritts J. Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study. Journal of Health Communication. 2015;20(6):673-9. https://doi.org/10.1080/10810730.2015.1018560

20.Peng W, Kanthawala S, Yuan S, Hussain SA. A qualitative study of user perceptions of mobile health apps. BMC Public Health. 2016;16:1-1. https://doi.org/10.1186/s12889-016-3808-0

21.Prasad A, Sorber J, Stablein T, Anthony D, Kotz D. Understanding sharing preferences and behavior for mHealth devices. In Proceedings of the 2012 ACM workshop on Privacy in the electronic society 2012 Oct 15 (pp. 117-128). https://doi.org/10.1145/2381966.2381983

22.Mousavi Baigi SF, Mousavi AS, Kimiafar K, Sarbaz M. Evaluating the cost effectiveness of tele-rehabilitation: a systematic review of randomized clinical trials. Frontiers in Health Informatics. 2022;11. https://doi.org/10.30699/fhi.v11i1.368

23.Swain S, Muduli K, Kumar A, Luthra S. Analysis of barriers of mHealth adoption in the context of sustainable operational practices in health care supply chains. International Journal of Industrial Engineering and Operations Management. 2024;6(2):85-116. https://doi.org/10.1108/IJIEOM-12-2022-0067

24.Simblett S, Greer B, Matcham F, Curtis H, Polhemus A, Ferrão J, Gamble P, Wykes T. Barriers to and facilitators of engagement with remote measurement technology for managing health: systematic review and content analysis of findings. Journal of Medical Internet Research. 2018;20(7):e10480. https://doi.org/10.2196/10480

25.Aljedaani B, Ahmad A, Zahedi M, Ali Babar M. Security awareness of end-users of mobile health applications: an empirical study. InMobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services 2020 Dec 7 (pp. 125-136). Available form: https://arxiv.org/abs/2008.13009

26.Breitinger F, Tully-Doyle R, Hassenfeldt C. A survey on smartphone user's security choices, awareness and education. Computers & Security. 2020;88:101647. https://doi.org/10.1016/j.cose.2019.101647

27.Aval RN, Baigi SF, Sarbaz M, Kimiafar K. Security, privacy, and confidentiality in electronic prescribing systems: A review study. Frontiers in Health Informatics. 2022;11(1):115. https://doi.org/10.30699/fhi.v11i1.374

28.Nasiri S, Sadoughi F, Tadayon M H, Dehnad A. Security and privacy mechanisms of internet of things in healthcare and non-healthcare industry. Journal of Health Administration. 2019; 22 (4):86-105 [In Persian]. Available form: http://jha.iums.ac.ir/article-1-3233-en.html

29.Rezaee R, Khashayar M, Saeedinezhad S, Nasiri M, Zare S. Critical criteria and countermeasures for mobile health developers to ensure mobile health privacy and security: mixed methods study. JMIR mHealth and uHealth. 2023;11:e39055. https://doi.org/10.2196/39055