

Evaluating Privacy and Security Requirements of the Electronic Prescribing System in Iran: A Qualitative Study

Mohamad Jebraeily¹ , Hero Khezri¹ , Bahlol Rahimi^{2,3} , Ghanbar Tavassoli⁴ , Tahereh Samimi⁴ 

Published: 30 February 2026

© The Author(s) 2026

Abstract

Background Electronic prescribing (e-prescribing) systems enable physicians to generate and transmit prescriptions electronically, improving accuracy, reducing medication errors, and supporting clinical decision-making. These systems also enhance communication between healthcare providers and pharmacies, contributing to safer and more efficient patient care. Because e-prescribing involves the exchange of sensitive patient information, ensuring data privacy, confidentiality, and cybersecurity is essential for the safe and effective use of these systems. The aim of this study is to identify and evaluate the privacy and security requirements of the electronic prescribing system in Iran from the perspectives of different stakeholders.

Methods A qualitative study was conducted in Urmia, Iran, in 2024. A total of 15 participants were recruited, including information technology specialists (n = 7), health information management professionals (n = 3), and physicians (n = 5). Data were collected through face-to-face, semi-structured interviews, each lasting approximately 30–40 minutes. The interview data were transcribed verbatim and analyzed using qualitative content analysis with MAXQDA software, and the coding process was independently reviewed by a second researcher to enhance the credibility and reliability of the findings.

Results Analysis identified three major themes and 15 sub-themes. Participants emphasized the importance of technical safeguards, including multi-factor authentication, robust password policies, role-based access control, encryption, real-time security alerts, and system protections against external threats. Managerial measures, such as audits, training, and standards-based security practices, together with user-related behaviors, including security awareness and responsible system use, were also considered critical.

Conclusion The e-prescribing system has positively influenced outpatient healthcare services in Iran. Ensuring privacy and security, however, depends on the implementation of robust technical safeguards, effective managerial strategies, and responsible user behavior. Future research should evaluate the nationwide implementation of the system and investigate opportunities to further optimize its performance and effectiveness.

Keywords Ambulatory care, Computer security, Electronic prescribing, Privacy

✉ Tahereh Samimi
samimi.ta@umsu.ac.ir

1. Department of Health Information Technology, School of Allied Medical Sciences, Urmia University of Medical Sciences, Urmia, Iran
2. Health and Biomedical Informatics Research Center, Urmia University of Medical Sciences, Urmia, Iran
3. Department of Medical Informatics, School of Allied Medical Sciences, Urmia University of Medical Sciences, Urmia, Iran
4. Student Research Committee, Urmia University of Medical Sciences, Urmia, Iran

1 Introduction

The integration of electronic prescribing (e-prescribing) systems into healthcare has transformed processes such as medication prescribing, clinical consultations, and diagnostic testing.^[1,2] Fundamentally, e-prescribing refers to a computer-based system that enables healthcare providers to electronically enter and transmit accurate prescription instructions.^[3] This approach minimizes prescribing errors and enhances patient safety by generating real-time alerts regarding potential drug allergies and drug interactions.^[4,5] Several studies have shown that e-prescribing systems improve the safety, quality, efficiency, and cost-effectiveness of healthcare delivery, while streamlining workflows and increasing accessibility for patients.^[1,6] Physicians generally report that e-prescribing enhances workflow efficiency and clinical decision-making; however, challenges such as internet connectivity, usability issues, and insufficient training persist.^[6] Intelligent Prescription Systems (IPS) integrate advanced algorithms, machine learning, and patient-specific data to optimize drug selection, dosing, and monitoring.^[7] Despite these advances, user perceptions highlight barriers such as system usability, workflow integration, and training requirements, especially in outpatient and community settings.^[8] Data privacy and security are critical challenges in implementing e-prescribing systems, requiring rigorous measures to ensure the confidentiality and integrity of patient health information.^[4,9,10] Secure management of protected health information and personally identifiable information is essential due to inherent privacy vulnerabilities.^[11,12] Threats such as unauthorized access, data breaches, and misuse of patient records within e-prescribing systems present significant risks, potentially resulting in identity theft, financial fraud, and erosion of patient trust.^[13-15] Security vulnerabilities, such as weak authentication, insufficient encryption, and susceptibility to cyberattacks, further compromise the confidentiality, integrity, and availability of prescription data.^[14,15] Additionally, while healthcare organizations may secure Protected Health Information (PHI) within internal systems, transmitting data to external entities introduces further risks when third parties fail to provide adequate safeguards.^[7,16,17] While safeguarding patient privacy remains paramount, successful adoption of e-prescribing systems requires strict adherence to healthcare data governance frameworks.^[16] Security can be significantly improved by incorporating privacy and security requirements early in the system design and implementation phases, ensuring the integrity, availability, and confidentiality of medical data.^[9] In Iran, e-prescribing systems are now widely implemented across healthcare centers. However, limited evidence exists regarding the adequacy of their privacy and security measures. The aim of this study is to identify

and evaluate the privacy and security requirements of the electronic prescribing system in Iran from the perspectives of different stakeholders.

2 Methods

Study Design

This study employed a qualitative research design using the conventional content analysis method to explore the privacy and security requirements of the national e-prescribing system.

Setting and Participants

The study was conducted in Urmia, Iran, from February to May 2024, aligning with the timeframe mentioned in the abstract. A total of 15 participants were recruited, including physicians ($n = 5$), information technology specialists ($n = 7$), and Health Information Management (HIM) professionals ($n = 3$). Participants were selected based on their professional experience and direct involvement with the design, implementation, or use of the e-prescribing system.

Sampling Strategy

A purposive sampling strategy with maximum variation was used to capture diverse perspectives and experiences. Recruitment continued until data saturation was reached, when no new codes or themes emerged. Participants were informed about the study objectives, and interviews were scheduled at convenient times and locations.

Data Collection

Data were collected through face-to-face, semi-structured interviews, each lasting approximately 30–40 minutes. Interviews were conducted in private rooms at participants' workplaces to ensure confidentiality and comfort. An interview guide, based on the study objectives and relevant literature, focused on privacy and security requirements of the e-prescribing system. Key questions included:

- Main privacy and security challenges encountered
- Essential technical and managerial measures
- Impact of user behaviors, such as password sharing or ignoring security alerts

Follow-up questions were asked for clarification or elaboration. All interviews were audio-recorded with participants' permission, and field notes were taken.

Data Analysis

Interviews were transcribed verbatim and analyzed using qualitative content analysis with MAXQDA software, with coding independently reviewed by a second researcher to ensure accuracy, consistency, and rigor. Analysis was performed in several steps: repeated

reading of transcripts to obtain a sense of the whole, identification of semantic units relevant to the study objectives, coding of both manifest and latent content, grouping codes into categories, and abstraction of categories into main themes and sub-themes. Codes and categories were reviewed multiple times to ensure internal consistency and conceptual clarity. To ensure the rigor of the study, Lincoln and Guba's criteria were applied. Credibility was enhanced through member-checking with participants and peer debriefing with qualitative experts. Dependability was supported by maintaining an audit trail, including transcripts, coding frameworks, and analytical notes. Confirmability was established through reflexive journaling and independent review of coding by a second researcher. Finally, transferability was facilitated by providing detailed contextual descriptions of participants, settings, and procedures.

3 Results

Demographic Characteristics of Participants

In this qualitative study, 15 participants from Urmia University of Medical Sciences were interviewed. The mean duration of the interviews was 32 minutes. Table 1 presents the demographic characteristics of the participants.

According to Table 1, the majority of participants were

Table 1 Demographic characteristics of study participants

Variable		Frequency (Percentage)
Sex	Male	9 (60.0)
	Female	6 (40.0)
Age	30-40	5 (33.3)
	40-50	10 (66.7)
Specialty	Information technology	7 (46.7)
	Physician	5 (33.3)
	HIM	3 (20.0)
Work experience with the system	> 3 years	4 (26.7)
	< 3 years	11 (73.3)

male ($n = 9$, 60.0%) and belonged to the age group of 40–50 years ($n = 10$, 66.7%). Nearly half of the respondents specialized in information technology ($n = 7$, 46.7%), followed by physicians ($n = 5$, 33.3%) and HIM specialists ($n = 3$, 20.0%). Furthermore, most participants reported having less than three years of work experience with the e-prescribing system ($n = 11$, 73.3%).

Themes and Sub-Themes: Privacy and Security Requirements

In total, after several iterations of review, the contents of interviews were categorized into three main themes

and 15 sub-themes (Table 2). These themes highlighted the impact of the e-prescribing system on patient safety, quality of care, user and patient satisfaction, and healthcare workflows.

Table 2 Themes and sub-themes related to privacy and security requirements of the e-prescribing system

Themes	Sub-themes
Technical	Lack of authentication methods
	System downtimes and slow internet
	Implementing strong security measures
	Role-based access
	Security alerts
Management	Insufficient training
	Audits and monitoring
	Risk management
	Standards-based security requirements
	Separate insurance system
User's behaviour	Service disruption during e-prescribing downtime
	Lack of awareness
	Sharing usernames and passwords
	Accountability issues
	Disregard for security alerts

Technical Mechanisms of Privacy and Security in the E-Prescribing System

Participants highlighted several technical mechanisms implemented to ensure privacy and security within the e-prescribing system (Table 2). Regarding authentication, an IT professional stated, “existing privacy and security mechanisms are not adequate, and many challenges remain. It is better to apply multi-factor authentication to prevent any illegal access” (IT 3), which corresponds to the sub-theme Lack of authentication methods. Similarly, a HIM professional emphasized password management, noting that “users of the e-prescribing system have to use strong passwords with complexity and are required to change them regularly” (HIM 1). Several participants highlighted role-based access control as a key security measure. For example, one Physician explained, “Users have access to electronic prescriptions based on their primary role and perform necessary transactions according to their duties (e.g., Physicians can prescribe, pharmacists can dispense, but not modify prescriptions)” (Physician 7), linked to the sub-theme Role-based access. Other technical safeguards included antivirus and firewall use to protect against external threats (IT 2), encryption of communications and storage between prescribers, pharmacies, and other healthcare providers (IT 5), and real-time alerts to detect and notify suspicious activities, such as unauthorized access attempts, corresponding to implementing strong security measures and security alerts.

The separate insurance system directly affects the privacy and security of electronic prescriptions. System performance issues, such as downtimes and slow internet, were also highlighted as technical barriers under the sub-theme System downtimes and slow internet. “When the e-prescribing system goes down, we cannot access or process prescriptions, which delays patient care and creates confusion in the pharmacy” (Physician 5).

Managerial Issues of Privacy and Security in the E-Prescribing System

Participants emphasized several managerial issues directly related to privacy and security (Table 2). Proper training on the correct use and handling of PHI was recommended to reduce data breaches caused by employee errors. One physician highlighted the lack of training, stating, “I received no training about privacy and security requirements of e-prescribing” (Physician 4), which aligns with the sub-theme Insufficient training. Regular audits were also considered essential to ensure compliance with security policies, corresponding to the sub-theme Audits and monitoring. Furthermore, the fragmentation arising from the existence of multiple insurance systems has significantly undermined the privacy and security of electronic prescription processes. As one physician observed, “Each insurance organization in Iran developed its own electronic prescription platform, creating considerable challenges in maintaining uniform access controls and safeguarding data privacy” (Physician 5). In alignment with this perspective, a HIM professional emphasized that “the separation of insurance systems introduces substantial challenges concerning access control, encryption, and data protection, fundamental technical mechanisms that underpin the privacy and security of e-prescribing systems.” (HIM 3).

Furthermore, participants emphasized the absence of standardized privacy and security requirements or guidelines, a finding that aligns with the sub-theme Standards-Based Security Requirements. This lack of consistent standards further exacerbates the vulnerabilities of systems, highlighting the need for unified governance and interoperable security frameworks within the national e-prescription infrastructure.

User-Related Behaviors Affecting Privacy and Security in the E-Prescribing System

Participants highlighted several user behaviors that influence privacy and security within the e-prescribing system (Table 2). One physician noted, “Some physicians give their username and password to secretaries to enter orders into the e-prescribing system,” (Physician 4), reflecting the sub-theme Sharing usernames and passwords. Most interviewees agreed that due to the lack of electronic signatures, unauthorized access by secretaries

or other staff, and insufficient authentication methods, the security of the e-prescribing system is inadequate. Digital signatures were recommended to ensure prescriptions are securely signed and to prevent tampering. Several participants also reported that some physicians delegated e-prescribing tasks to their assistants, which complicated the supervision of medications dispensed to patients. One participant emphasized the challenge of balancing access with patient privacy: “When we want to view a patient’s previous records, a confirmation code must be sent, which can cause issues if the patient doesn’t have their phone with them. We need to access these records in the patient’s presence for their benefit, not to misuse their medical history” (Physician 3). Another participant noted operational issues, stating, “System downtimes and slow internet are our biggest problems. When a patient comes to the pharmacy, we can’t access their prescription or dispense their medication” (IT 7). Sometimes we receive security warnings in the system, but due to workload or urgency, we often ignore them and proceed with the prescription” (Physician 5).

4 Discussion

The confidentiality and security of patient information are critical components of electronic prescribing systems, as they directly affect patient safety, trust, and the overall quality of care.^[9] Despite their benefits, e-prescribing systems continue to face significant challenges related to security protocols and the lack of standardized privacy measures, which remain concerns for both patients and healthcare providers.^[19] Based on our findings, issues related to confidentiality can be categorized into three main themes: technical mechanisms, managerial measures, and user-related behaviors. These themes not only reflect the perceptions of Iranian healthcare professionals but also align with global evidence on safeguarding patient information in e-prescribing systems. Maintaining technical safeguards is essential for protecting sensitive patient data. In our study, participants highlighted several measures, including multi-factor authentication, strong password policies, role-based access, encryption of communications, real-time security alerts, and system defenses against external threats. These findings align with Norouzi Aval et al., who identified seven core technical components user authentication, confidentiality, licensing, integrity, non-repudiation, and protection of data in storage and transit as essential for securing e-prescribing systems.^[9] Similarly, Moghani et al. emphasized that the absence of digital signatures and insufficient adherence to e-prescribing standards increase the risk of unauthorized access to patient information. Their recommendations for digital signatures, role-based access controls, and practical user training correspond closely with the technical safeguards identified in our

study, underscoring the universal importance of robust technical infrastructures.^[20] Furthermore, Bouraghi et al. reported that poor system design, unresolved technical issues, and insufficient user training could exacerbate risks related to unauthorized access and mishandling of sensitive data. These findings collectively reinforce that secure system architecture and compliance with standards are critical for protecting patient information.^[21] In addition to technical safeguards, managerial measures such as structured training programs, regular audits, and adherence to privacy standards are essential. Our findings revealed that insufficient user training and lack of standardized policies were major gaps in the Iranian system. Moghani et al. also highlighted the importance of practical training for healthcare staff to ensure secure handling of patient data. Regular audits and monitoring were emphasized by participants as crucial strategies to detect potential breaches early and ensure compliance with privacy requirements.^[20] User behaviors significantly influence the effectiveness of privacy and security measures. In our study, participants noted that sharing usernames and passwords, ignoring security alerts, and a lack of awareness of privacy requirements increased the risk of unauthorized access. These behaviors echo concerns in the literature regarding the need for a culture of accountability and awareness among healthcare staff to prevent insider threats.^[9,19] To address these challenges, participants emphasized training programs to ensure users handle PHI correctly and reduce breaches caused by employee errors. The implementation of role-based access controls, encryption technologies, real-time alerts for suspicious activities, and regular audits were also highlighted as essential strategies to maintain system security and protect patient privacy. Finally, participants stressed the importance of promoting a culture of awareness and accountability among healthcare staff to mitigate insider threats.

In addition, interoperability in modern healthcare systems necessitates secure data exchange protocols to enable seamless information sharing while safeguarding privacy. Beyond privacy and security, e-prescribing systems influence workflow efficiency, patient safety, and satisfaction. Porterfield et al. demonstrated in a systematic review that these systems significantly reduce medication errors, enhance workflow, improve patient safety, and increase both patient and provider satisfaction. Integration with electronic health records allows access to complete patient information, supporting clinical decision-making and reducing reliance on handwritten prescriptions.^[22] Our study in Iran corroborates these benefits, showing improvements in workflow, physician satisfaction, and the quality of outpatient services. Similarly, Ambaye et al. highlighted that healthcare professionals perceive e-prescriptions as effective tools for saving time and reducing errors, with positive perceptions influenced by

work experience and prescription volume. These findings complement our results, emphasizing that optimizing e-prescribing systems can simultaneously enhance workflow, user satisfaction, and the overall quality of care.^[23]

These findings suggest that while technical safeguards and managerial strategies are essential, their effectiveness heavily depends on user compliance and behavior. For instance, even well-designed systems can be compromised if security alerts are ignored or access credentials are shared. Therefore, optimizing e-prescribing systems requires an integrated approach that addresses technology, governance, and human factors simultaneously.

Overall, the study emphasizes that technical safeguards, managerial strategies, and user-related behaviors collectively determine the effectiveness of privacy and security measures in e-prescribing systems, highlighting areas for improvement in implementation and training.

Given the widespread use of electronic prescribing in healthcare provision and the need to maintain patient confidentiality, it seems necessary to conduct further research on improving the security of electronic prescribing systems. Also, additional research should be conducted to evaluate system performance and the behavior of system users in maintaining confidentiality.

This study has several limitations that should be considered. First, the small sample size (15 participants) may not capture the full diversity of perspectives, despite purposive sampling with maximum variation and data saturation. Second, the study was conducted only in one city (Urmia), which may limit the generalizability of the findings to other regions of Iran.

5 Conclusion

The study highlights that implementing an electronic prescribing system requires careful attention to technical, managerial, and user-related aspects to ensure patient privacy and data security. Addressing infrastructure limitations, standardizing processes, providing practical training, and fostering a culture of privacy awareness are essential for successful implementation. Compliance with security protocols, continuous monitoring, and promoting transparency and accountability can mitigate risks and enhance the system's effectiveness. These findings provide a roadmap for healthcare institutions seeking to optimize e-prescribing systems while safeguarding sensitive patient information.

Declarations

Acknowledgments

The authors express their gratitude and appreciation to all the participants in this study.

Artificial Intelligence Disclosure

The authors used Grammarly for editing the English section of the manuscript. All edited content was reviewed and approved by the authors.

Authors' Contributions

Mohamad Jebraeily and Tahereh Samimi designed the study. Mohamad Jebraeily, Hiro Khezri, Ghanbar Tavasoli and Tahereh Samimi collected the data. Analysis and interpretation of the data were done by Mohamad Jebraeily and Balol Rahimi. All authors have written and approved the manuscript.

Availability of Data and Materials

The data used in this study are available from the corresponding author upon reasonable request via email.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript.

Consent for Publication

Not applicable.

Ethical Considerations

This research study was approved by the ethics committee of Urmia University of Medical Sciences under the Code of Ethics IR.UMSU.REC.1401.408.

Funding

The present study was supported by the Research Council of Urmia University of Medical Sciences (project code: 3158).

Open Access

This article is licensed under a Creative Commons Attribution-Noncommercial 4.0 International License, which permits any non-commercial use, sharing, adaptation, distribution, and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third-party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by-NC/4.0/>.

References

- Williams J, Malden S, Heeney C, Bouamrane M, Holder M, Perera U, et al. Optimizing Hospital Electronic Prescribing Systems: A Systematic Scoping Review. *J Patient Saf.* 2022;18(2):e547-e62. doi:10.1097/PTS.0000000000000867.
- Grammatikopoulou M, Zachariadou M, Zande M, Giannios G, Chytas A, Karanikas H, et al. Evaluation of an electronic prescription platform: Clinicians' feedback on three distinct services aiming to facilitate clinical decision and safer e-prescription. *Res Social Adm Pharm.* 2024;20(7):640-7. doi:10.1016/j.sapharm.2024.04.004.
- Alinejad A, Nourani A, Jebraeily M. Usability evaluation of the user interface in electronic prescribing systems of Iran Health Insurance Organization and Social Security Organization. *Journal of Health Administration.* 22;25(88):78 to 94.
- Alshahrani F, Marriott JF, Cox AR. A qualitative study of prescribing errors among multi-professional prescribers within an e-prescribing system. *Int J Clin Pharm.* 2021;43(4):884-92. doi:10.1007/s11096-020-01192-0.
- Cassidy CE, Boulos L, McConnell E, Barber B, Delahunty-Pike A, Bishop A, et al. E-prescribing and medication safety in community settings: A rapid scoping review. *Explor Res Clin Soc Pharm.* 2023;12:100365. doi:10.1016/j.rcsop.2023.100365.
- Alipour J, Payandeh A, Hashemi A, Aliabadi A, Karimi A. Physicians' Perspectives with the E-prescribing System in Five Teaching Hospitals. *Appl Clin Inform.* 2024;15(3):428-36. doi:10.1055/s-0044-1786872.
- Tantray J, Patel A, Wani SN, Kosey S, Prajapati BG. Prescription Precision: A Comprehensive Review of Intelligent Prescription Systems. *Curr Pharm Des.* 2024;30(34):2671-84. doi:10.2174/013816128321623240719104337.
- Sudarsono J, Satibi S, Lazuardi L, Widayanti AW. Healthcare professionals' perceptions of electronic prescription systems in outpatient services: a qualitative study at UNS hospital. *Cost Eff Resour Alloc.* 2025;23(1):31. doi:10.1186/s12962-025-00639-3.
- Norouzi Aval R, Fatemeh S, Baigi M, Sarbaz M, Kimiafar K, Mousavi F. Security, Privacy, and Confidentiality in Electronic Prescribing Systems: A Review Study. *Frontiers in Health Informatics.* 2022;11(1):115 doi:10.30699/fhi.v11i1.374.
- Datta A, Sen S. A Security and Privacy Validation Methodology for E-Health Systems Using Cloud Storage. *Network and Human Security, Social Media, and Devices* 2024. p. 173-92. doi:10.4018/979-8-3693-9235-5.ch009.
- Amato F, Casola V, Cozzolino G, De Benedictis A, Mazzocca N, Moscato F. A security and privacy validation methodology for e-health systems. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM).* 2021;17(2s):1-22. doi:10.1145/3412373.
- Oktarlina RZ. E-prescribing: benefit, barrier, and adopting challenge in electronic prescribing. *Journal of Medicine.* 2020;21(2):98-101. doi:10.3329/jom.v21i2.50213.
- Rodrigues H, Correia ME, Antunes L. A secure electronic prescription system. *International Journal for Infonomics.* 2013;6(3/4):780-7. doi:10.20533/iji.1742.4712.2013.0091.
- Abusal S, Alsarayra K, Alyabroodie Z. Designing a standard-based approach for security of healthcare systems. *J Stat Appl Pro.* 2024;13(1):419-34. doi:10.18576/jsap/130129.
- Hoffman SAE. Cybersecurity threats in healthcare organizations:: exposing vulnerabilities in the healthcare information infrastructure. *World Libraries.* 2020;24(1).
- Naghizadeh S, Farshid S, Rahimi B, Jebraeily M. Determining minimum data set for implementation of a ureteral stent registry system. *Health Science Monitor* 2024; 3 (3) :252-260. doi:10.61186/hsm.3.3.252.
- Fathi B, Alinejad V, Moslehi S, Marouzi P. Prevalence of the Common Cancers by Gender using GIS System in Razavi Khorasan Province. *Health Science Monitor* 2023; 2 (1) :21-29. doi:10.52547/hsm.2.1.21.
- Parv L, Kruus P, Mõtte K, Ross P. An evaluation of e-prescribing at a national level. *Inform Health Soc Care.* 2016;41(1):78-95. doi:10.3109/17538157.2014.948170.
- Alkathiri S, Alothman R, Ata S, Alruthia Y, editors. Evaluating the Wasfaty E-Prescribing Platform Against Best Practices for Computerized Provider Order Entry. *Healthcare*; 2025; 13(18):

- 946 MDPI. doi:10.3390/healthcare13080946.
20. Moghani NB, Hooshmand E, Zarqi M, Meraji M. Challenges and solutions in implementing electronic prescribing in Iran's health system: a qualitative study. *BMC Med Inform Decis Mak.* 2024;24(1):393. doi:10.1186/s12911-024-02737-3.
21. Bouraghi H, Imani B, Saeedi A, Mohammadpour A, Saeedi S, Khodaveisi T, Mehrabi T. Challenges and advantages of electronic prescribing system: a survey study and thematic analysis. *BMC Health Serv Res.* 2024 May 30;24(1):689. doi:10.1186/s12913-024-11144-3.
22. Porterfield A, Engelbert K, Coustasse A. Electronic prescribing: improving the efficiency and accuracy of prescribing in the ambulatory care setting. *Perspect Health Inf Manag.* 2014;11(Spring):1g.
23. Ambaye AS, Kassa MT, Ejigu YW, Tadesse GT, Siraj EA, Endalifer BL. Perception of health professionals towards electronic prescription in a teaching hospital. *Sci Rep.* 2025;15(1):31781. doi:10.1038/s41598-025-14919-8.