Migration Letters

Volume: 19, No: S5 (2022), pp. 1327-1336

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Perceptions of Healthcare Professionals and Healthcare Users toward Electronic Medical Records and Data Confidentiality

Saad Saayd Ayad Alosaimi[1], Jehan Khelaif Alanazi[2], Mansour Sattam Nasser Al-Baqami3, Mohammed Ali Namshan Alkhathami[3], Mamdouh Abdullah Hudayb Al-Otaibi[4], Waad Saad Salem Allahyani5, Rajwa Abdulaziz Adam Hawsawi5, Reem Eqab Ayed Alharthi5, Sinah Awad safeer Aljauid5, Nahed Ahmad omar zabarmawi[5], Ohoud Abdullah Mohammad Almadani[6], Amani Salim Sahinqari[7], Bader Jaly Almutairi[8], Ebtesam Alruwaili[9]

Abstract

Background: Electronic Medical records (EMRs) can improve the quality and safety of care. However, the adoption and use of the EMR is influenced by several factors, including users' perception. Jeddah city made a major bound forward, which supports with the vision of leadership, in the region's electronic health services by adopting a unified electronic medical record system across the country. EMRs provide a better, more efficient standard of care and a vital database that will update the administrative process and promote better outcomes with less utilization of resources. MRs Form an essential part in patient management and include a diversity of patient data information that might be sensitive. Therefore, the primary challenge is to maintain data confidentiality of the EMRs. The study aims: To investigate the perceptions of healthcare professionals (HCPs) and healthcare users (HCUs) toward EMRs and data confidentiality in electronic healthcare facilities in Jeddah, KSA. Methods: A descriptive study was conducted on explored the perceptions towards EMRs and data confidentiality using an online survey as a data collection tool. Data collection was carried out over four weeks started from January 2022. The dependent variables were the user and provider perceptions, while the independent variables included gender, and age. A random sample of 201 electronic Healthcare facilities professionals and users was included. Results: The findings of the study revealed that most HCPs and users agreed on the presence of good electronic Health data protection practices and confidentiality principles. There was a statistical correlation between the surveyed confidentiality practice perceptions and gender. However, age had no statistically significant association. Conclusions: These research findings can influence policymakers and stakeholders when developing EMRs and data confidentiality policies and guidelines across

[1] Male health information technician, Dawadmi General Hospital, Saudi Arabia.
[2] Health informatics technician, National Guard Hospital, Saudi Arabia.
[3] Health Information Management, Al Quwayiyah General Hospital, Saudi Arabia.
[4] Healthcare management specialist and his services,Third Settlement, Riyadh - Halit Health Center, Saudi Arabia.
[5] Health informatics specialist, Maternity and Children's Hospital in makkah, Saudi Arabia.
[6] Health and hospital services management technician, Maternity and Children's Hospital in Makkah, Saudi Arabia.
[7] Health information systems technician, Maternity and Children's Hospital in Makkah, Saudi Arabia.
[8] Medical secretary, General Sajer hospital, Saudi Arabia.
[9] Second Health Cluster, Riyadh, Primary health Care Center Al-Naseem Al-Awsat Ministry of Health Riyadh13717, Saudi Arabia

the healthcare facilities, in particular, during the implementation of unified EMRs. Future research could investigate the effect of the specific demographic variables on the perception of confidentiality among electronic healthcare facility users that might influence EMRs and data confidentiality.

Keywords: *Electronic Health; Confidentiality; electronic medical records; healthcare professionals.*

Introduction

The implementation of health information technology (HIT) has been associated with improved quality of healthcare services, increased efficiency, and reduced costs of healthcare as well as provider satisfaction (1, 2). Electronic medical records (EMRs) and electronic health records (EHRs) are the most common e-health technologies used in many healthcare settings today (3). Lu et al., (2005) (4) noted that these computer-based record systems help healthcare professionals (HCPs) to manage patients' health information and improve care (4). The healthcare outcomes of EHR/EMR are mainly attributed to the systems' enormous benefits, including but not limited to the elimination of redundant paper-based processes (5, 6), elimination of time-consuming procedures in recording and retrieving patient data (7), easy access to patient information (8), and improved communication between the multidisciplinary teams (9, 10).

Therefore, electronic health information systems (HISs) are crucial for the sustainability of healthcare organizations as the provision of high-quality care services likely to attract more clients resulting in increased profitability and growth (11). Electronic Health is an inevitable, real-time technological advance that enhances patient-centered communication in the age of globalization. The use of EMR offers potential improvements in the legibility and accessibility of medical records among multiple HCP sites (12, 13). EMRs allow the immediate and complete exchange of patient health information. This property can improve the quality and safety of healthcare services, reduce healthcare costs and facilitate research. Electronic records also enhance the safety of healthcare services through strengthening the continuity of care and increasing the documentation accuracy, accessibility of test results and availability of online medication reordering with drug alerts and error notifications (13, 14).

However, successful digital healthcare infrastructure, created by an EMR system, requires a better understanding of the healthcare user's views, concerns and experiences, as healthcare professionals are using EMR daily to deliver the services (12). The benefits of an EMR system must be balanced against the possibility of a potential loss of information privacy and cyber-attacks, which are more prominent than for paper medical records. Patient health information is stored in the system of healthcare providers, insurance companies and government entities for record, references and research purposes. Storing sensitive patient information in the electronic health system can lead to unauthorized access and misuse (12-14).

Without the presence of legislation, electronic healthcare service users may fear unauthorized access to sensitive personal information and, thus, avoid the use of electronic health services. Therefore, the perception of users is critical to determine their behaviors and interactions with the system. Hence, it is the responsibility of the provider to maintain the confidentiality of the data through the implementation of proper privacy and liability mechanisms to increase trust in the electronic health system and services provided, including the internet of medical things (12, 15, and 16). Interviewing healthcare professionals in London showed that there is a superficial level of perception regarding the importance of healthcare system security, which

might significantly threaten the integrity of the healthcare system (17). A cross-sectional study conducted in New Zealand showed that 73.3% of participants were apprehensive regarding the privacy and security of their medical records (18).

A survey conducted in the United States on primary care physicians revealed that the majority of physicians perceived the benefit of EHRs. However, they reported a primary concern for the privacy and confidentiality of electronic Health services (19). A study conducted on the impact of health disclosure laws on health information exchanges showed that the presence of secure privacy and confidentiality laws that limit disclosure of health information data led to more significant health information exchanges between healthcare facilities (20, 21). Other studies focused on individual attitudes toward EHRs, indicating that privacy concern was reduced by the perceived effectiveness of regulatory mechanisms and the perceived effectiveness of technological mechanisms, where both showed a positive impact on the trust, while technological mechanisms positively impacted the perceived privacy control and trust (15, 22, and 23).

Electronic medical record users may experience serious financial, social and psychological problems if sensitive information and other determinants of health informatics adoption and diffusion are disclosed (21, 24). There is limited evidence regarding the current use and perception of electronic medical records and data confidentiality in KSA. In this study, we investigated the perception of healthcare professionals and healthcare users toward electronic medical records and data confidentiality in electronic Healthcare facilities after the implementation of electronic medical records for the most significant public healthcare service provider in Jeddah, KSA.

Methods

A descriptive cross-sectional study investigated the perceptions of healthcare users toward electronic Health data and record confidentiality in Jeddah in terms of user perceptions regarding the data protection practices of electronic Healthcare facilities in Jeddah as well as their understanding of the adoption of useful confidentiality measures. We also investigated the confidentiality and privacy principles offered by healthcare providers and users to maintain data privacy and measured their association with some demographic variables, including gender, age. The HCPs included physicians, nurses, paramedics and nutritionists, while the healthcare users represented the patients receiving care from such facilities. The survey inclusion criteria required literacy in Arabic or English. Users who did not speak either English or Arabic were excluded.

The data collection procedure was through a universal link sent by a convenient method through email and social media programs to the HCPs. At the same time, HCPs were contacted by the primary healthcare sector. Participation was entirely voluntary, and the participant could stop the survey based on their convenience at any time while answering the survey questionnaire. There was no identifiable information obtained from the participants, and the participants were anonymous. Data collection was carried out over four weeks started from January 2022. By the end date, the collection period survey was closed, and the data were downloaded from the survey platform.

The researchers used email, mobile phone and social media programs to recruit participants; the universal link was sent to different contacts, to reach a maximum number of users in the months of January-February of 2022. After data cleaning, the final number obtained from survey respondents for providers and users was 201. Similar to providers, the users' sampling method was based on volunteer sampling. The survey link had the same message sent to all

participants explaining the purpose of the study, the informed consent form and the survey questions.. Many types of research tackling the same topic area used the survey method, which made the cross-sectional survey approach the best to collect the required data (25-28).

The demographic variables obtained for both users and providers in the survey included gender, age, employment designation, length of service, and type of healthcare sector. The healthcare sector was divided into public, private and other, as public and private are the two main categories, while other will cover an additional minority if it exists.

The dependent variables (DVs) were obtained through posing three questions; the first was about how the user feels while using the electronic Healthcare facility regarding their rights, data record accuracy and protection and if they trust and feel comfortable while using the EMRs. The second DV question was regarding the seven privacy principles used to measure the degree of privacy and confidentiality offered by healthcare providers to maintain data privacy. The seven principles are the notice principle, choice principle, disclosure principle, security principle, data integrity principle, access principle and enforcement principle. The third DV question was regarding the perception of healthcare users of the right adoption of data privacy measures by HCPs. The dependent variables were measured against a Likert scale.

The data collected were exported to Microsoft Excel in both forms as coded values and coded text and then exported into Statistical Package for the Social Sciences (SPSS) version 28. Data cleaning and screening procedures were applied to the exported SPSS data. After cleaning, a codebook was generated for all variables, the data entry was performed using the codebook, and descriptive tables for demographic data were generated.

Three domains of perceptions were investigated. This was carried out using 25 questions, with 6 for healthcare professional and user feelings regarding data privacy while using the electronic Health facility in Jeddah, seven for privacy principles and 12 for good provision of privacy and confidentiality of healthcare providers when dealing with patient data. Each question had seven options ranging across Strongly Disagree, Somewhat Disagree, Slightly Disagree, Slightly Agree, Somewhat Agree, Strongly Agree, and Not Applicable. They were given scores of 1, 2, 3, 4, 5, 6, and 7, respectively.

After applying the percentage score, descriptive tables were generated; cross tables regarding the correlations between demographic variables and the principle domains were also generated using SPSS. The statistical significance was calculated, and a p-value of less than 0.05 was considered the cut-off point of significance.

Results

Table (1) shows 78% of the survey respondents were HCPs, while 22% (n = 44) represented healthcare users. The description of demographic characteristics of the participants shows that 82% of the respondents were female while there were 18% male respondents. Approximately 86% of the respondents were 30 years of age or above. Approximately 90% of the respondents (n = 180) utilized the private healthcare sector, as compared to 21 respondents (10%) who used the public healthcare sector (Table 1).

Table (2) shows that the healthcare users who reported that the purpose of the last visit to the healthcare institution or clinic included medical follow-up constituted 41%. In comparison, 27.3% used it for medical tests, 18% for emergency visits and 13.6% for regular check-ups (Table 2).

On the other hand, healthcare professionals were 62.4% doctors, 27.4% nurses, 2.5% medical assistants, and 1.3% dieticians and nutritionists, while 6.4% were reported as other health-allied

professionals; including pharmacists, radiographers and speech therapists. Forty-eight percent of the survey healthcare professionals had more than ten years of working experience within their respective designations (Table 3).

Perception of the Participant on electronic Health Privacy

Our findings of the perception of the data protection practice of the electronic Healthcare provider showed that more than 93% of the survey respondents reported that they were "comfortable when using electronic Health services", "the data collected are recorded accurately and precisely" and "they could trust the electronic Health services systems offered". Ninety-one percent of the survey respondents reported that "they felt secured when using electronic Health services". We found that 90% of the user respondents felt that their "data collected are protected" and 89% felt that "their right has not been violated".

Findings of the data privacy principles from the perspective of service providers were as follows:

1. Notice principles: This principle explains that the data user must inform the individual that their data are being collected; they also must provide their contact details, the type of disclosed data and if the third party will use the data. (90 %) of the respondents agreed that this principle was evident.

2. Choice principle: This principle empowers individuals to have the authority to limit the usage of their data to only the collected purpose. (83%) percent of the respondents agreed that this principle was evident.

3. Disclosure principle: Data disclosure to the third party must be ensured after informing the subjects, and data should be transferred according to the purpose for which it was initially collected. (87%) percent of the respondents agreed that this principle was evident.

4. Security principle: This principle protects the data from misuse, abuse, unauthorized access and disclosure while dealing with collected data. (92%) percent of the respondents agreed that this principle was evident.

5. Data integrity principle: According to this principle, the collected data should be accurate and consistent at all stages; during collection, usage and disclosure. (92%) percent of the respondents agreed that this principle was evident.

6. Access principle: According to this principle, the data should be accessible by an authorized individual to amend, delete and modify the data if required, in addition to tracking modification history. (86%) percent of the respondents agreed that this principle was evident.

7. Enforcement principle: This principle requires that the data user should provide a precise, transparent mechanism to ensure compliance with data principles. (92%) percent of the respondents agreed that this principle was evident.

The survey also included questions related to the providers' perception of the adoption and maintenance of ethical electronic Health data privacy standards and practices by the electronic Health service provider. The results showed that 95% of the respondents agreed that the service providers, in general, were following the data protection principles to: "maintain personal information", "continuously improve the process of collecting patients' information", "continuously update and enhance the networks to the latest technology available" and "record all data and information precisely and accurately". In addition, 94% agreed to the notion of "maintain personal privacy", 93% agreed on "reassure patients that privacy is at its highest", "avoid being the violators of user trust" and implementation of the privacy policy. Over 89% of respondents agreed to statements such as "avoid being the worst privacy offenders", "store all patients' information and data in safe networks" and "have encrypted networks". We found

that 84% agreed to the statement, “Educate the patients on the standard privacy rules and procedures in place”.

Table (4) shows that there was no statistically significant association between age and gender (users and providers) for all privacy statements.

Table (1): The demographic characteristics of the study

Variable		n	%
Gender	Female	165	82
	Male	36	18
Age (years)	Below 20	5	2.5
	20–29	24	12
	30–39	86	42.8
	40–49	63	31.3
	Above 50	23	11.4
Respondent	Healthcare user	44	22
	Healthcare professional	157	78
Healthcare sector	Public	180	90
	Private	21	10

Table (2): Healthcare user purpose of the last visit to the healthcare facility

Variable		n	%
Purpose of the last visit	Medical follow-up	18	41
	Medical test	12	27.3
	Emergency visit	8	18.1
	Regular check-up	6	13.6

Table (3): Length of service and designation of healthcare professionals

Variable		n	%
Length of service	Less than 5 years	45	28
	5–10 years	37	24
	More than 10 years	75	48
Designation	Doctors	98	62.4
	Nurse	43	27.4
	Medical assistant	4	2.5
	Dietician	2	1.3
	Other health allied	10	6.4

Table (4): Statistical associations between the perceptions of participants on privacy principles and the practice of providers and users and selected demographic variables

	Age	Gender
Notice principle	0.706	0.524
Choice principle	0.736	0.762
Disclosure principle	0.662	0.495
Security principle	0.710	0.752
Data integrity principle	0.509	0.081
Access principle	0.337	0.926
Enforcement principle	0.776	0.684

* p-value: significance less than 0.005.

Discussion

The massive volume of clinical data, new knowledge and advanced clinical tools, as well as integrated and coordinated patient clinical information, created the need for electronic Health (EH) and electronic medical records (EMRs). Patient health record data and information are crucial in the healthcare sector. EMRs help to achieve massive cost savings, improve the efficiency and quality of care by increasing accessibility, aid in the provision of coordinated and comprehensive care and reduce medication error (29). This study showed that there is an increased level of agreement on the data protection practice by an electronic Healthcare provider as indicated in the results achieved on 11 of the statements measured after EMR was implemented. This was true except for the "rights have not been violated" statement, which showed a similar level of privacy perception before and after EMRs implementation according to "privacy protection laws and public perception of data confidentiality, the case of electronic healthcare services (24)".

A study on the perception of EMRs by nursing staff in a teaching hospital in India showed that 75% of the nurses were comfortable using the EMRs (30) while the results in this study showed a higher level of agreement particularly after the implementation of EMRs. The rated data confidentiality principles showed an overall reduction in the level of agreement on the presence of privacy principles except for the data integrity and enforcement principle, which increased from 84% to 90% after EMRs implementation. A study carried out in the United States (n = 30) with mixed cultures to assess patients willingness to share their information showed that individuals with highly sensitive data were less likely to share their information unconditionally (31, 32), especially if there was a lack of consent before data usage (23). This might provide an insight into the reason behind the reduction in the notice, choice, and disclosure principle levels of agreements.

When the results of this survey were compared with the earlier study that was conducted before EMR implementation (24), the survey findings regarding the providers' opinions on the motives for adopting ethical Health data privacy principles by electronic Health service providers showed an increased level of agreement, except for statements such as "educate the patients of the standard privacy rules and procedures in place", which remained the same before and after EMR implementation. A study by Gupta et al. (2016) (22) showed that a user's trust could be positively impacted by the perceived effectiveness of the technological and regulatory mechanisms. Respondent perceptions in this study might reflect the level of trust toward

electronic Healthcare facility EMR confidentiality measures.

In the study conducted by Sarabdeen and Moonesar, (2018) (24), the majority of respondents were from healthcare users, and there was no significant association between all the demographic variables and the privacy principles in the study. In this study, the majority were from the healthcare professional categories that are using electronic medical records to manage the patients. In this study, age had no statistically significant association with the different studied elements of privacy. There were statistically significant associations between the gender of the electronic medical record providers and "educate the patients of the standard privacy rules and procedures in place", "continually improve the process of collecting patient's information" and "the gender relationship needs to be further studied to understand how it affects users' and providers' perceptions".

Privacy principle applications at various healthcare institutions must be encouraged by policymakers. The presence of EMR data protection, confidentiality, and privacy law will strengthen patient rights. Reserving patient and healthcare professional rights will increase satisfaction. Different areas of data protection and privacy adopted from the study conducted by Sarabdeen and Moonesar, (2018) study provide a baseline for healthcare leaders and policymakers (24, 32).

Conclusions

The policy implications of those are as follows: Perception of the data protection practices of electronic Healthcare providers: This provides insights regarding healthcare users' perceptions of electronic Health facility practices, and how users and healthcare professionals feel with regard to facility data protection and their rights. The majority of respondents agreed on all statements. Perception of participants on adopting good Health data privacy practices by electronic Healthcare providers: This provides an insight into the motives for selecting ethical electronic Health data privacy principles by the electronic Health service provider. The variables that were associated were gender. This can be advised by the policymakers to invite and involve both genders to address any issues related to data protection before the implementation of the electronic medical records system.

Perception of participants on the privacy principle practices of electronic Healthcare providers: Although most participants agreed on the privacy principle practices by electronic Health providers. Future studies are required to investigate the further effects of specific demographic variables on the perception of privacy among electronic Healthcare facility users. Additionally, participant responses could be influenced by the questionnaire items, resulting in commonly biased answers. Future researchers should include an in-depth interview method and add the perception of non-electronic Health facility users to compare the knowledge of both groups.

References

1. Abdulla AE, Ahmed SY, Alnoaimi MA, Ali H. Users' satisfaction with the electronic health record (EHR) in the Kingdom of Bahrain. Consumer-driven technologies in healthcare: breakthroughs in research and practice: IGI Global; 2019. p. 319-44.
2. Buntin MB, Burke MF, Hoaglin MC, Blumenthal D. The benefits of health information technology: a review of the recent literature shows predominantly positive results. Health Aff (Millwood) 2011. Mar;30(3):464-471. 10.1377/hlthaff.2011.0178
3. Amatayakul MK. Electronic health records: A practical guide for professionals and organizations: American Health Information Management Association Chicago; 2009.

4. Lu Y-C, Xiao Y, Sears A, Jacko JA. A review and a framework of handheld computer adoption in healthcare. Int J Med Inform 2005. Jun;74(5):409-422. 10.1016/j.ijmedinf.2005.03.001

5. Li J, Talaei-Khoei A, Seale H, Ray P, Macintyre CR. Health care provider adoption of eHealth: systematic literature review. Interact J Med Res 2013. Apr;2(1):e7. 10.2196/ijmr.2468

6. Al-Harbi A. Healthcare providers' perceptions towards health information applications at King Abdul-Aziz Medical City, Saudi Arabia. International Journal of Advanced Computer Science and Applications 2011;2(10):10-13 . 10.14569/IJACSA.2011.021003

7. El Mahalli A. Electronic health records:Use and barriers among physicians in eastern province of Saudi Arabia. Saudi J Health Sci 2015. Jan;4(1):32-41 . 10.4103/2278-0521.151407

8. Silow-Carroll S, Edwards JN, Rodin D. Using electronic health records to improve quality and efficiency: the experiences of leading hospitals. Issue Brief (Commonw Fund) 2012. Jul;17:1-40.

9. King J, Patel V, Jamoom EW, Furukawa MF. Clinical benefits of electronic health record use: national findings. Health Serv Res 2014. Feb;49(1 Pt 2):392-404. 10.1111/1475-6773.12135

10. O'Malley AS, Grossman JM, Cohen GR, Kemper NM, Pham HH. Are electronic medical records helpful for care coordination? Experiences of physician practices. J Gen Intern Med 2010. Mar;25(3):177-185. 10.1007/s11606-009-1195-2

11. Alkraiji A, Osama E-H, Fawzi A. Health informatics opportunities and challenges: preliminary study in the cooperation council for the Arab States of the Gulf. J Health Inform Dev Ctries 2014;8(1).

12. Alkureishi, M.A.; Lee, W.W.; Lyons, M.; Press, V.G.; Imam, S.; Nkansah-Amankra, A.; Werner, D.A.; Arora, V.M. Impact of Electronic Medical Record Use on the Patient–Doctor Relationship and Communication: A Systematic Review. J. Gen. Intern. Med. 2016, 31, 548–560.

13. White, A.; Danis, M. Enhancing Patient-Centered Communication and Collaboration by Using the Electronic Health Record in the Examination Room. JAMA 2013, 309, 2327.

14. Heurix, J.; Karlinger, M.; Neubauer, T. PERiMETER—Pseudonymization and personal metadata encryption for privacy-preserving searchable documents. Health Syst. 2012, 1, 46–57.

15. Mou, J.; Shin, D. Effects of social popularity and time scarcity on online consumer behaviour regarding smart healthcare products: An eye-tracking approach. Comput. Hum. Behav. 2018, 78, 74–89.

16. Shin, D.; Biocca, F. Health experience model of personal informatics: The case of a quantified self. Comput. Hum. Behav. 2017, 69, 62–74.

17. Ondiege, B.; Clarke, M. Health care professionals’ perception of security of personal health devices. Smart Homecare Technol. TeleHealth 2017, 4, 35–42.

18. Prajesh Chhanabhai, A. Consumers Are Ready to Accept the Transition to Online and Electronic Records If They Can be Assured of the Security Measures. 2007. Available at: https://www.ncbi.nlm.nih.gov/pmc/ articles/PMC1924980/

19. Anderson, J.G.; Balas, E.A. Computerization of Primary Care in the United States. Int. J. Health Inf. Syst. Inform. 2006, 1, 1–23.

20. Idris Adjerid, R. Impact of Health Disclosure Laws on Health Information Exchanges. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3243116/

21. Shin, D.-H.; Lee, S.; Hwang, Y. How do credibility and utility play in the user experience of health informatics services? Comput. Hum. Behav. 2017, 67, 292–302.

22. Gupta, A.; Patel, V.; Greenes, R. Advances in Healthcare Informatics and Analytics, 19th ed; Springer International Publishing: Cham, Switzerland, 2016.

23. Whetten-Goldstein, K.; Nguyen, T.Q.; Sugarman, J. So much for keeping secrets: The importance of considering patients' perspectives on maintaining confidentiality. AIDS Care 2001, 13, 457–465.

24. Sarabdeen, J.; Moonesar, I.A. Privacy protection laws and public perception of data privacy. Benchmarking Int. J. 2018, 25, 1883–1902.

25. Papoutsi, C.; Reed, J.E.; Marston, C.; Lewis, R.; Majeed, A.; Bell, D. Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: Results from a mixed methods study. BMC Med. Inform. Decis. Mak. 2015, 15, 1–15.

26. O'Donnell, H.C.; Patel, V.; Kern, L.M.; Barron, Y.; Teixeira, P.; Dhopeshwarkar, R.; Kaushal, R. Healthcare Consumers' Attitudes Towards Physician and Personal Use of Health Information Exchange. J. Gen. Intern. Med. 2011, 26, 1019–1026.

27. Lakbala, P.; Dindarloo, K. Physicians' perception and attitude toward electronic medical record. SpringerPlus 2014, 3, 63.

28. Rutten, L.J.F.; Vieux, S.N.; Sauver, J.L.S.; Arora, N.K.; Moser, R.P.; Beckjord, E.B.; Hesse, B.W. Patient perceptions of electronic medical records use and ratings of care quality. Patient Relat. Outcome Meas. 2014, 5, 17–23.

29. Wang, S.J.; Middleton, B.; Prosser, L.A.; Bardon, C.G.; Spurr, C.D.; Carchidi, P.J.; Kittler, A.F.; Goldszer, R.C.; Fairchild, D.G.; Sussman, A.J.; et al. A cost-benefit analysis of electronic medical records in primary care. Am. J. Med. 2003, 114, 397–403.

30. Pera, N.K.; Kaur, A.; Rao, R. Perception of electronic medical records (EMRs) by nursing staff in a teaching hospital in India. Int. J. Adv. Med. Health Res. 2014, 1, 75.

31. Caine, K.; Hanania, R. Patients want granular privacy control over health information in electronic medical records. J. Am. Med. Inform. Assoc. 2013, 20, 7–15.

32. Shin, D.; Hwang, Y.; Cheung, C. Integrated acceptance and sustainability evaluation of Internet of Medical Things. Internet Res. 2017, 27, 1227–1254.