JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2024, VOL 7, NO S12

Privacy Issues Hindering Implementation and Use of Electronic Health Records in the Middle East

Asaad Nasser Izzuldeen Qasimi[1],Saeed Ali Saeed Alzahrani[2],Muath Musaad Mutain Tumyhi[3],Musaed Hameed Almuqati[4],Bashair Mohamed Hezam[5]

Introduction

Electronic health records are a radical advancement in the current society especially in the delivery of health care since it brings efficiency in the management of healthcare records as well as improvement of patients' health. However, certain challenges have risen in the Middle East specifically concerning EHR implementation which is privacy. Based on these antecedents and acknowledgments of differences in cultural, religious, and regulatory aspects in the Middle Eastern countries, the following specific challenges are postulated as specific to the Middle Eastern Region in the implementation of EHR. To this end, the current systematic review seeks to explore the complex array of privacy issues that underlie the effective adoption and usage of EHR systems in MEHI (Heston, 2024). The healthcare sector of Middle Eastern countries has been through a process of sharp recent years, and many countries have increased investment in digital healthcare systems. However, the diffusion of EHR systems still lacks a more integrated and coherent approach and it is still considered rather fragmented and problematic in nature because of privacy issues, which can be technical, cultural, and regulatory. Awareness of these challenges is essential for future healthcare managers, authorities, and IT developers dedicated to improving IT-based healthcare in the area.

Data Security and Encryption Challenges in Middle Eastern Healthcare Systems

The deployment of sound protection measures and encryption, however, remains an area of concern in Middle Eastern healthcare systems. Hospitals and other healthcare centers in the area have to deal with constantly evolving and more complex cyber threats while trying to protect and secure users' information. The primary concerns are technical in nature, and consequently, predominant solutions are also largely technical, but several factors suggest that protection must be considered from technical and operational viewpoints in parallel. One of these major issues is in the choice and application of suitable encryption algorithms. As there are technologies for high-level encryption, their integration with existing healthcare structures is challenging (Zanaboni et al., 2020). Primary data collection showed that the use of legacy systems in many healthcare facilities in the Middle East renders inadequate encryption of patient data. However, investment into the most advanced encryption techniques that are employed in the system is costly for the implementation and regular maintenance and this is difficult on the smaller end of the spectrum within the healthcare industry.

One of the questions that arise is that of data protection in transit: Data security during transfer poses another vital question. Because data is now shared across networks, as healthcare providers engage with other networks, end-to-end encryption becomes a priority. However, due to the differences in terms of technical solutions implemented throughout levels of hi, the technical preparedness of various healthcare centers can vary significantly; optimal measures coincide with discrepancies in security; thus, introducing potential vulnerabilities in the chain. Further, advancement in Mobility, particularly for the management of health applications and timely access to patient records, brings new kinds of risk to light that have to be managed. Another major issue is the encryption key and access management area. Security-conscious patient data demands in healthcare organizations need to be addressed while accommodating the practical necessity of medical teams needing ready access to patient data, particularly during emergencies.

Legislative and Regulatory Framework for Health Data Privacy

Middle Eastern countries' legislation and regulations concerning the protection of health data are still undefined and changing. Some nations are gradually formulating elaborate policies for data protection and personal information, but others remain unrecognized in establishing valid procedures for managing e-health data. Thus, such differences in 'regulatory maturity' prove disadvantageous for the healthcare companies practicing across several jurisdictions within the region. A vast number of Middle Eastern nations are in the process of regulating data privacy and protection to meet the global market requirements, including the GDPR policy from the EU community (Mesquita et al., 2025). Nevertheless, enforcement of these regulations is a challenge since the ability to implement measures to protect the privacy of patients is constrained by resources, and there are differing institutional viewpoints about what privacy entails, and since privacy protection has to be achieved while at the same time facilitating the provision of efficient health care services in the health information system. The lack of similar rules of protection for the patients' data throughout the region also presents difficulties in cross-border healthcare services provision and exchange of data.

Currently, some of the countries have adopted specific HC data protection laws but these do not contain elaborate implementation procedures and measures. Meantime, healthcare providers have to work in those gray areas while trying to meet high expectations for patient data protection. This state of affairs is made even worse given the fact that there are both local and extra-regional privacy laws especially where patients are from other countries or where participating in intercontinental research programs. Data retention, disposal, and notification in case of breach are mandatory legal standards that also differ from one country to another in the region. This variation poses several difficulties for healthcare organizations that are in many different states and it also makes it more difficult to set a common standard for privacy.

Cultural and Religious Considerations Affecting Health Information Privacy

Due to cultural and religious factors, Middle Eastern patients and healthcare providers have different perspectives regarding health information privacy for use in EHR. A brief look at Islamic practices of privacy and confidentiality is enough to show that factors governing acceptable practices in handling special health information emanate from established religious practices. These cultural and religious considerations must be taken into consideration while designing and implementing EHR systems in the region as well. Privacy pervades most aspects of Middle Eastern societies and most of the time family and community values are highly considered. This collective approach to privacy can also influence the use and disclosure of health information often in situations having to do with special health needs or genetic predisposition.

Clinicians can hardly avoid these cultural factors while also remaining HIPAA compliant (Bajnaid & Aljasir, 2025). Gender segregation practiced in most Middle Eastern countries also affects the manner in which information relating to health is addressed. That is why healthcare facilities need to attend to these cultural needs when activating EHR systems without compromising the proper organization of healthcare. This may involve providing or denying gender based access controls, formulating procedures for dealing with records concerning females. The roles religious beliefs play also affect perceptions of some forms of medical content and how they require treatment. For example, the records of a patient’s mental health or information on reproductive health can deserve special considerations relative to privacy owing to cultural taboos or religious beliefs.

Patient Consent Management and Access Control Issues

Enforcement of patient autonomy and patient control of e-health records are difficult issues to address in Middle Eastern healthcare organizations. The procedure of acquiring, recording, and sustaining a patient's consent must meet legal and cultural aspects and not interfere with the effectiveness of the healthcare service provision. This raises even further challenges when working with different types of medical information and different levels of access to the same (Grzenda &

Widge, 2024). There remain issues regarding the use of some new approaches to the consent model and flexible management that would be required to address situations like managing EMR access under circumstances like emergent conditions, other access by family members, or other different consent levels for different types of medical information. An additional level of complication lies in regularly creating audit trails for changes in consent decisions or in access to the patient record.

The use of role-based access control systems is faced with technical and operational issues. Various types of employees will require different types of access to patients' records and healthcare organizations must determine who may have what type of access while at the same time maintaining the open availability of all medical information as it may be needed at any one time. This becomes especially difficult, especially in teaching hospitals or research facilities where other consumers of information may include other people. Also, a decision in this area is focus on how to address the patient's preferences regarding the disclosure of information to either the family members or multiple providers. Family-centered decision-making is another typical feature of Middle Eastern populations, which demands efficient solutions concerning their values as well as adequate protection of patients' privacy.

Healthcare Provider Training and Compliance Barriers

Health IT infrastructure can only support fully privacy-preserving EHR systems if healthcare providers have sufficient training and are willing to adhere to privacy safeguards. However, in many healthcare organizations in the Middle East training related difficulties and maintaining consistent privacy compliance pose major problems to the provision of effective training. Adding to these: are high staff turnover rates and variability of education among people employed in the sphere of healthcare. ConcerningIMP-software, training has to be in place, and sustained by healthcare providers in the use of EHR and privacy laws (Alhur, 2024). They must serve surveys for staff who may have diverse technical literacy and assume that all the staff know their obligations to patients' privacy. Because of the time and money that has to be invested in framing such a practice, added to which is the fact that there are inherent costs associated with the undertaking which are oftentimes stressful to a health care system.

Other factors include the following; compliance monitoring and enforcement. This means that healthcare organizations have to find ways of tracking compliance with privacy protocols while at the same time continuing to deliver efficient healthcare. This involves performing periodic reviews on accesses that exist in the system, tracking the violation of privacy incidents, and taking appropriate action when called for (Alhitmi et al., 2024). Lack of language interpreters among healthcare attendants or even cultural differences among trainers, facilitators, or assessors can also affect the success of training programs and compliance activities. In view of these differences, organizations need to develop methods and training aids that address the differences yet provide uniformity to other organizational policies such as privacy protection.

Cross-border Health Data Exchange Challenges

Cross-border flows of health data within the Middle East region raise specific confidentiality and security concerns. Due to the trends like going international and patients traveling across borders for treatments, the need for effective and secure transmission of information across borders is becoming even more important. However, the privacy requirements, technical specifications, and confidentiality expectations differ from country to country, organization to organization, or culture to culture, which acts as a brake on free information exchange (Aldughayfiq & Sampalli, 2021). One really big issue applies to the fact that there are a number of national data protection laws, and they may be mutually contradictory so compliance with them can be problematic. It presents great challenges because objective data have to be exchanged between health care providers but at the same time the legal requirements that have to be followed are quite intricate.

Technical integration is another crucial factor that affects cross-border health data transfer, they include; There are various systems in use across countries and healthcare organizations, and the platform, and terminology may also differ, hence information exchange is not easy while respecting privacy concerns. Stating that it is necessary to translate medical terminology as well as documents being used at that moment complicates the matter even more (Chilunjika & Uwizeyimana, 2024). Some of the more sensitive data are most likely to cause concern when shared across different borders especially due to the fact that not all countries around the globe could have put in place adequate measures to protect such data. Healthcare providers have to ensure that the information is secure during transmission and on the same note, it must be available to the intended users regardless of the physical location.

Technical Infrastructure and System Interoperability Concerns

The technical infrastructure supporting EHR systems in the Middle East faces numerous challenges related to system interoperability and infrastructure reliability. Most are challenged with old hardware, inadequate telecommunications, and unstable power, all of which are potential risks to EHI. As is the case with the Surescripts message, there is still a question of the compatibility of EHR systems used by different healthcare organizations (Sheikh et al., 2021). This absence of common features poses privacy concerns whenever exchanging data and can lead to latency of information or the development of a partial picture of the patient. One cannot overemphasize the need for healthcare organizations to continue to invest in solutions that allow for the transparent exchange of data while at the same time preserving the privacy of any data that is shared across the various platforms that exist.

Availability of technical infrastructure for the delivery of online classes is inconsistent across the region: there may be regular power outages or/and very low Internet speed at home. These infrastructure challenges can lead to the prevalence of EHR system availability issues and put patient data at risk in data system outages or when data is being recovered. The availability of backup systems and contingency plans becomes necessary for healthcare providers to ensure patients' data during any technical disruptions (Aboalsamh et al., 2023). Organizational adoption of cloud technologies provides both pros and cons to EHR deployment. Although the use of cloud solutions can increase scalability and accessibility, the major concerns have been on sovereignty and security.

Role of International Standards and Best Practices in Middle Eastern Context

International standards and best practices have to be incorporated into EHR privacy protection but at the same time have to be tailored to the Middle Eastern setting. Though the adopted global standards offer relevant conceptual foundations for protecting individual's privacy, their adoption must be done with consideration to the local laws and norms, as well as technology infrastructure. Assessment and management of privacy information have become more important to healthcare organizations in the Middle East, as they seek international standards like ISO 27701 and HL7 (Katoue et al., 2022).

However, meeting these standards is not an easy task since it carries along with it a great deal of resources and professional implications that cannot be available to many health organizations. This paper examined the various advantages associated with international certification, necessary for organizations to take cognizance of the other crucial side, which relates to the effective implementation of the certification systems. Privacy protection measures should be standardized but the implementation processes should take into consideration the regional issues of concern that should not contradict the global policies on the same. This involves creating a PIA approach that takes into consideration the civil rights of the local populace and biomining of local healthcare delivery models to accommodate PBD solutions.

Conclusion

Privacy-preserving EHR systems in the Middle Eastern region have several barriers that need addressing from the aspect of stakeholders within the players such as the healthcare organizations,

policy makers, and technology firms. Although much progress has been made in addressing these challenges further research has to be conducted to come up with all-inclusive approaches to solving the challenges with a focus on both the protection of patients' privacy while at the same time seeking to enhance health care delivery systems. Based on the findings of the study, future research regarding the strengthening of EHR privacy should concentrate on the creation of nation-specific structures that reflect the philosophies of the Middle East as well as referring to global guidelines. Such as reinforcing the legal architecture, enhancing the subordinate technological structures, and creating mechanisms with regard to ethical and religious aspects of a person's privacy. The accomplishment of these challenges is still a long shot, especially with continuous investment towards availing of better technologies, training of human resources, and protection of privacy.

References

Aboalsamh, H. M., Khrais, L. T., & Albahussain, S. A. (2023). Pioneering perception of green fintech in promoting sustainable digital services application within smart cities. *Sustainability*, *15*(14), 11440. https://www.mdpi.com/2071-1050/15/14/11440

Aldughayfiq, B., & Sampalli, S. (2021). Digital health in physicians' and pharmacists' office: a comparative study of e-prescription systems' architecture and digital security in eight countries. *Omics: a journal of integrative biology*, *25*(2), 102-122. https://www.liebertpub.com/doi/full/10.1089/omi.2020.0085

Alhitmi, H. K., Mardiah, A., Al-Sulaiti, K. I., & Abbas, J. (2024). Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions. *Cogent Business & Management*, *11*(1), 2393743. https://www.tandfonline.com/doi/full/10.1080/23311975.2024.2393743#abstract

Alhur, A. (2024). Overcoming electronic medical records adoption challenges in Saudi Arabia. *Cureus*, *16*(2). https://pmc.ncbi.nlm.nih.gov/articles/PMC10924290/

Bajnaid, W., & Aljasir, S. (2025). Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region. *Journalism and Media*, *6*(1), 8. https://www.mdpi.com/2673-5172/6/1/8

Chilunjika, S. R., & Uwizeyimana, D. E. (2024). Blockchain technology for health information management: a case of Zimbabwe. *Insights into Regional Development*, *6*(1), 59-73. https://www.researchgate.net/profile/Sharon-Chilunjika/publication/379430106_Blockchain_technology_for_health_information_management_a_case_of_Zimbabwe/links/66093dc5b839e05a20b26739/Blockchain-technology-for-health-information-management-a-case-of-Zimbabwe.pdf

Grzenda, A., & Widge, A. S. (2024). Electronic health records and stratified psychiatry: bridge to precision treatment?. *Neuropsychopharmacology*, *49*(1), 285-290. https://www.nature.com/articles/s41386-023-01724-y

Heston, T. F. (2024). Prespective chapter: Integrating large language models and blockchain in telemedicine. https://www.intechopen.com/chapters/1176440

Katoue, M. G., Cerda, A. A., García, L. Y., & Jakovljevic, M. (2022). Healthcare system development in the Middle East and North Africa region: challenges, endeavors and prospective opportunities. *Frontiers in public health*, *10*, 1045739. https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.1045739/full?amp%3Bamp

Mesquita, S., Perfeito, L., Paolotti, D., & Gonçalves-Sá, J. (2025). Epidemiological methods in transition: Minimizing biases in classical and digital approaches. *PLOS Digital Health*, *4*(1), e0000670. https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000670

Sheikh, A., Anderson, M., Albala, S., Casadei, B., Franklin, B. D., Richards, M., ... & Mossialos, E. (2021). Health information technology and digital innovation for national learning health and care systems. *The Lancet Digital Health*, *3*(6), e383-e396. https://www.thelancet.com/journals/landig/article/PIIS2589-7500(21)00005-4/fulltext

Zanaboni, P., Kummervold, P. E., Sørensen, T., & Johansen, M. A. (2020). Patient use and experience with online access to electronic health records in Norway: results from an online survey. *Journal of medical Internet research*, *22*(2), e16144. https://www.jmir.org/2020/2/e16144/