JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2024, VOL 7, NO S10

EHR Adoption in Saudi Arabia: Privacy, Security, and Patient Trust

Naif Salah Alradadi[1], Mohammed Rageh Ahmad Abuallah[2], Hayat Nasser Mosa Maslom[3], Faisal Mohammed Ahmed Mudhawwi[4], Sarah Hamed Hamdan Alotaibi[5], Abeer Zakri Masoud Ruthan[6], Luliyyah Mukhdhari Maghfuri[7], Hadeel Mohammed Maghfori[8], Safa Abbas Alsaeed[9], Mohammed Ahmed Jaber Bakri[10], Ebrahim Saud Alotaybi[11], Mutaen Ibrahim Ahmed Faqih[12], Yousef Ibrahim Mohammed Alajam[13], Norah Mohammad Ali Hadadi[14], Yahya Ahmed Yahya Shajiri[15].

1. *Medical secretary, Nojoud Center, Ministry of Health, kingdom of saudi arabia. nalradadi@moh.gov.sa*
2. *Health Informatics Technician, Jazan, mrabuallah@moh.gov.sa*
3. *Medical secretarial, Abu Arish General Hospital, Ministry of health, kingdom of Saudi Arabia. Hmaslom@moh.gov.sa*
4. *Health Administration and Community Health, Damad General Hospital, Ministry of health, kingdom of Saudi Arabia. Fmudawi@moh.gov.sa*
5. *Health Informatics Technician, King Salman bin Abdulaziz Hospital, Ministry of health, kingdom of Saudi Arabia. shalotaiby@moh.gov.sa*
6. *Medical secretary, Al bead Primary Care Center, Ministry of health, kingdom of Saudi Arabia. azruthan@moh.gov.sa*
7. *Medical secretary, King Fahad central hospital in jazan, Ministry of health, kingdom of Saudi Arabia. lmmaghfuri@moh.gov.sa*
8. *Medical secretary, King Fahd Hospital, Ministry of health, kingdom of Saudi Arabia. hmaghfori@moh.gov.sa*
9. *Health informatics, Maternity and Children Hospital – Dammam, Ministry of health, kingdom of Saudi Arabia. Salsaeed5@moh.gov.sa*
10. *Medical secretary technician, King Fahad Central Hospital, Ministry of health, kingdom of Saudi Arabia. Moahbakri@moh.gov.sa*
11. *Health administration specialist, Maternity and Children's Hospital Alkharj, Ministry of Health, Kingdom of Saudi Arabia. hp200101@hotmail.com*
12. *Medical secretary, King Killed hospital Al-Kharj, Ministry of Health, Kingdom of Saudi Arabia. Mutaen_faqih@hotmail.com*
13. *Medical secretarial, Directorate of Health Affairs in Asir Region, Ministry of Health, Kingdom of Saudi Arabia. Y.alajam@hotmail.com*
14. *Medical Secretary, Hawtah Sudair Hospital, Ministry of health, Kingdom of Saudi Arabia. nohadadi@moh.gov.sa*
15. *Information health, Jazan health cluster. yshajiri@moh.gov.sa*

Abstract

The adoption of electronic health records (EHRs) in Saudi Arabia has gained significant momentum in recent years. However, concerns regarding privacy, security, and patient trust have emerged as critical challenges hindering the widespread implementation of EHRs. This study aims to identify and address these challenges based on a comprehensive review of relevant literature. The findings reveal that while Saudi Arabia has made notable progress in enhancing EHR security through privacy regulations and confidentiality guidelines, gaps persist in the implementation of advanced e-security features and policies across clinical and non-clinical electronic systems. Factors such as unauthorized access to patient records, resistance to change among medical staff, and inadequate training on secure EHR usage pose significant barriers to adoption. Additionally, the increasing frequency of cyberattacks targeting patient data in the Saudi health care system underscores the urgent need for robust cybersecurity measures. The study highlights the importance of patient trust and the role of social determinants in shaping health care consumers' intentions to adopt EHRs. Recommendations include launching public awareness campaigns, investing in advanced cybersecurity tools, providing mandatory EHR training for health care professionals, and addressing cultural and skill gaps. By implementing these strategies and fostering patient

trust, Saudi Arabia can overcome the challenges associated with EHR adoption and pave the way for a secure and confidential digital health care future.
Keywords: EHR, electronic health records, Saudi Arabia

Introduction

Electronic health records (EHRs) are described by Keshta and Odeh [1] as "an electronic version of a medical history of the patient as kept by the health care provider (HCP) for some time." Furthermore, they state that EHRs encompass all essential administrative and clinical data associated with the care provided to an individual by a specific HCP. These datasets typically include patient demographics, progress notes, diagnoses, medications, vital signs, medical history, immunization records, laboratory results, and radiology reports. EHRs are frequently referred to as electronic medical records (EMRs), a term that has gained prominence with the increasing global adoption of digital systems. However, it is crucial to differentiate between EMRs and EHRs. EMRs represent a digital version of all paper-based charts related to a patient that are maintained in a clinician's office. In contrast, EHRs contain all information included in EMRs along with additional datasets on the individual's overall health status, designed to be accessible to clinicians and specialists across different medical domains. EMRs are legal records generated at hospitals and serve as the primary source of data for EHRs (Keshta & Odeh, 2021).

Since their introduction in the late 1970s, EHRs have demonstrated a high global adoption rate (Evans, 2016). This adoption rate is influenced by the level of technological advancement within each country, as it is integral to achieving a competitive standard of care quality, patient safety, and satisfaction. EHR systems enable HCPs to monitor patients' health status in real time and store examination data digitally. These data include personal details, laboratory results, treatment plans, diagnoses, medications, vaccination history, and even multimedia files such as images and audio recordings. EHRs consolidate medical information from various independent HCPs, facilitating access within the same city, nation, or even across borders (Jabeen et al., 2018).

The exchange of personal and health information over the internet and via servers or clouds outside the secure environments of health care institutions has raised significant concerns regarding privacy, security, accessibility, and regulatory compliance (Keshta & Odeh, 2021). To maintain the trust between patients and HCPs, health care organizations must implement effective measures to secure EHRs (Evans, 2016). Trust, as highlighted by Jabeen et al., is a critical factor that indirectly influences the quality of health care. Patients' perceptions of HCPs and their ability to distinguish between health care providers significantly depend on the degree of trust established.

Confidential information is safeguarded by confidentiality, which prevents unauthorized access to sensitive data and ensures that personal information is protected. Breaches of confidentiality can lead to data loss and, in some cases, severe personal consequences for the patient, such as exposure of medical conditions like HIV or other sexually transmitted infections (Hameed et al., 2021). The collection of health information must adhere to legal and ethical privacy standards, including the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States (Hameed et al., 2021). These regulations aim to protect the confidentiality of patient data, prevent unauthorized disclosure, and secure institutional information (Masud et al., 2021).

According to the Cybersecurity Quarterly Bulletin for the fourth quarter of 2020, published by the Saudi National Cybersecurity Authority, the health care sector accounted for 14% of global cyberattacks, ranking it third among the most targeted industries. In Saudi Arabia (KSA), unauthorized activities were identified as the top threat, while information leakage was ranked fourth. The presence of sensitive health data in electronic systems poses risks to patient privacy and confidentiality. Rieder et al. underscored the necessity of maintaining information secrecy,

as its absence may lead patients to withhold critical details from their HCPs (Rieder et al., 2016). Such actions can impair physicians' ability to deliver effective care and may also allow political authorities to misuse administrative power by undermining medical confidentiality. Similarly, Samkari et al. emphasized the importance of the confidentiality, integrity, and availability (CIA) triad in health care systems (Samkari & Gutub, 2019). A data breach, as defined by the US Department of Health and Human Services, refers to the unauthorized use or disclosure of confidential health information that jeopardizes its privacy or security under the privacy rule, posing a significant risk of financial, reputational, or other harm to the affected individual (Seh et al., 2020). Schatz et al. defined cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and assets." (Schatz et al., 2017) KSA has demonstrated significant progress in cybersecurity, ranking second among the 193 members of the Global Security Index, a rise from 11th place within two years. According to the International Communication Union, it ranks first in both the Middle East and Asia.

Long-term studies on data breaches by Seh et al. have shown that health care records are compromised due to both internal and external breaches, including hacking, theft or loss, unauthorized internal disclosure, and improper disposal of sensitive information (Seh et al., 2020). Unauthorized sharing or transfer of sensitive health data without proper authorization can lead to serious consequences, including permanent harm to patients if the compromised data affects their medical treatment (Hameed et al., 2021). It is essential that EHRs are retained only as long as necessary for their intended purpose. Additionally, stored, transferred, and utilized data must be protected from compromise. The health care sector must incorporate robust cybersecurity measures to safeguard patient safety and collaborate to prevent cybercrime and unauthorized access to patient information. While cryptography is commonly used to protect EHRs, advancements have been made by combining cryptography with steganography for enhanced security (Samkari & Gutub, 2019).

A study conducted in Malaysia by Dong et al. highlighted that health institutions need to strengthen their efforts to monitor human-related security breaches to achieve effective information protection (Dong et al., 2021). The authors identified that major security breaches often result not only from technological flaws but also from inadequate security culture, awareness, and management within organizations. The implementation of a comprehensive information security policy compliance framework is crucial for all sectors.

In the KSA, the Personal Data Protection Law was introduced in September 2021, requiring organizations to make significant adjustments to their daily operations to ensure compliance. This law, enforceable from March 2023, mandates the registration of data controllers, maintenance of processing records, strengthened governance over personal data, limitation of data transfers (especially outside KSA), enforcement of individual consent for handling and sharing personal data, enhanced impact assessments, implementation of breach notification protocols, and heightened regulation over sensitive data, including health-related information. This project seeks to identify and address the challenges associated with protecting patient confidentiality in EHRs in the KSA based on a comprehensive review of relevant literature.

Literature review

1 Confidentiality Compliance of HCPs and Driving Factors of Data Breaching

Almulhem conducted a descriptive study examining the access privileges of medical interns from various Saudi Arabian medical colleges. The study revealed that 62.8% of participants had access to medical records, 66.1% had access to EHRs, and 83.27% had read-only access. These interns could perform quick searches for patient records, with 70.1% of those accessing

EHRs and 67.1% of those accessing paper medical records reporting this capability. Of the eleven studies reviewed, three focused on analyzing factors contributing to breaches of information security policies (ISPs) by health care professionals (HCPs). These studies explored determinants of compliance and noncompliance, employing various behavioral theories with minor variations (Alshahrani et al., 2021).

Two studies conducted by Altamimi et al., concentrated on non-malicious breaches of ISPs by medical interns in academic hospitals. The findings indicated that interns often justified their noncompliance behaviorally, citing reasons such as personal comfort in disregarding ISPs. The researchers demonstrated that neutralization theory could explain these deviations from expected norms and predict the likelihood of medical interns breaching hospital privacy regulations (Altamimi et al., 2018). In another study, Alanazi et al. investigated the efficacy of a theory-based model for predicting information security compliance behavior (ISCB) among HCPs in Saudi government hospitals. The study revealed that moderating and unconventional factors, such as morality and religion, influenced ISCB, whereas demographic factors such as marital status, job experience, and age had no significant effect (T. Alanazi et al., 2020).

2 Challenges of Confidentiality and Security of EHRs

Mishah et al. assessed e-security in Saudi hospitals and found that while health information technology departments were well-established in most hospitals, health information management departments were less prepared. The security of server rooms, data centers, and IT networks were identified as fundamental components of hospital e-security platforms. However, the study also highlighted contradictory practices regarding e-security. For instance, antivirus software was available in 93.75% of hospitals, but only 33.33% of these hospitals maintained updated versions. Similarly, while 83.3% of hospitals had established IT departments, 83.3% lacked designated e-security officers. Additionally, 62.5% of hospitals did not have an intrusion prevention system. Although 67% of hospitals' networks were internet accessible, only 33.33% of these networks were secured by firewalls. Remote backups, crucial for data recovery in cases of natural disasters or fires, were unavailable in 66.66% of the hospitals. Furthermore, only 4% of the hospitals had implemented a digital disaster recovery plan that included system restoration testing (Mishah et al., 2019).

Chikhaoui et al. explored privacy and security concerns related to cloud computing. Their findings revealed that more than half of the respondents believed patient medical records were at risk when stored in cloud environments. While 40% of participants stated that the data was secure, 10% declined to comment. A comparative analysis with bank data security showed that many respondents considered hospital data as secure as bank account data, expressing minimal concern over security. However, several respondents raised concerns about hospital data security, particularly regarding the transfer of patient information between hospitals. The majority (85%) believed that patient privacy was compromised during such transfers, while 5% disagreed, and 10% abstained from responding (Chikhaoui et al., 2017).

Almuayqil et al. investigated the barriers to e-health care and the adoption of EHRs in Saudi Arabia. The study identified that while citizens and IT professionals generally reported no concerns about security and privacy, health care professionals expressed significant apprehensions. Most health care professionals reported unauthorized access to patient EHRs, with 52.9% (n = 9) stating that they had experienced such incidents. Additionally, approximately one-third (41.2%, n = 7) reported cases where their patients' EHRs were not only accessed but also updated without their consent. Half of the respondents (47.1%, n = 8) indicated an inability to control access to their patients' EHRs, while the same proportion reported having unauthorized access to other patients' records. Over half (52.9%, n = 9) could not determine who had access to their patients' EHRs, leading to widespread dissatisfaction among 64.7% (n = 11) of the health care professionals due to their inability to regulate access. Moreover, 37.5% (n = 6) of the respondents indicated they could access the health records of

other patients. Among the three groups surveyed, citizens demonstrated the highest mean score for perceived security (mean = 3.5), followed by health care professionals (mean = 3.2) and IT specialists, who reported the lowest score (mean = 2.2) (Almuayqil et al., 2016).

3 Influence of Confidentiality on EHR Adoption

Research by Alsahafi et al. revealed that participants perceived security concerns as having a significant negative impact on their behavioral intention to adopt the National Electronic Health Records (NEHR) system in Saudi Arabia (beta = -0.22; P = 0.001). This finding indicates that concerns about unauthorized access to personal health information may discourage health care consumers from utilizing the NEHR system. The study also found that trust had a statistically significant positive effect on the behavioral intention of Saudi health care consumers to use the NEHR system (beta = 0.22; P = 0.001). These results suggest that trust in government e-health initiatives, along with health practitioners' confidentiality in managing sensitive health-related information, plays a critical role in shaping the intentions of Saudi health care consumers to adopt the NEHR system. Furthermore, trust was shown to have a substantial negative effect on perceived security concerns (beta = -0.39; P = 0.001). These data imply that Saudi health care consumers who perceive the NEHR system and its administrators as trustworthy are likely to experience reduced privacy and security concerns, thereby increasing their willingness to use the system (Alsahafi et al., 2020).

A study by Jabali and Jarrar in 2018 evaluated the operational challenges of EHR systems in 15 hospitals located in the Eastern Province of Saudi Arabia. Their survey indicated that approximately seven hospitals (46.6%) had implemented or were in the process of implementing an EHR system. In this region, EHR systems were primarily used for order entry (51.11%) and chart review (41.11%), with notable barriers to their application for documentation, decision support, and communication tools. The results suggested that despite the presence of "secure" EHR systems, the existing security mechanisms were not sufficiently robust to protect against all types of threats (Jabali & Jarrar, 2018).

Discussion

The confidentiality and security of EHRs are fundamental to ensuring patient satisfaction. Saudi Arabia has made significant advancements in enhancing EHR security through the implementation of privacy regulations and confidentiality guidelines. However, as highlighted by Mishah et al., only a limited number of clinical and non-clinical electronic systems incorporate advanced or moderately advanced e-security features, tools, and established policies to safeguard patient confidentiality. With an increasing number of cyberattacks targeting patient data in the Saudi health care system, the evaluation and strengthening of e-security measures in Saudi hospitals are essential to mitigate potential threats to patient data integrity and safety. Enhancing e-security protocols and developing stringent data security regulations are therefore critical to safeguarding patient information (Mishah et al., 2019).

Saudi Arabia's health care system is characterized by its reliability and its ability to foster trust and build positive relationships, which are vital for creating a confident and dependable public health care framework. Effective management of patient data requires understanding the motivations and factors that drive security compliance or breaches. Altamimi et al. identified various motivations that influence the use of management information systems (MIS) under conditions where ISP requirements are not fully adhered to. However, compliance with ISPs by employees cannot always be assumed, especially when they are dissatisfied with existing rules. In such cases, employees often adopt neutralization strategies to rationalize their behavior. These strategies include denial of responsibility, denial of injury, appeal to higher loyalties, the metaphor of the ledger (justifying negative actions by referencing past positive actions), defense of necessity, and condemnation of condemners (Altamimi et al., 2020).

While these neutralization approaches may mitigate some challenges, they are insufficient to fully protect privacy and comply with regulatory standards. To address these limitations, Altamimi et al. recommended adopting preventive strategies such as awareness campaigns and training programs (e.g., face-to-face sessions, online courses, and seminars) as operational health care measures to discourage noncompliant behavior. Implementing these strategies could strengthen safety measures by creating psychological barriers to inappropriate actions, complementing advancements in technological systems. The influence of social norms, particularly descriptive norms, has also been shown to reinforce compliance, as individuals are more likely to respond positively to descriptive norms compared to injunctive norms.

Additionally, factors influencing ISCB are critical for maintaining the confidentiality of EHRs. Alanazi et al. described various factors that impact ISCB, including psychological behaviors, cultural and religious beliefs, personality traits, compliance costs, social norms, technology awareness, and legal considerations. Their findings indicated that ISCB is influenced by uncommon factors such as religion and morality, while demographic factors, such as work experience, were found to have no significant effect (T. Alanazi et al., 2020).

Alsahafi et al. highlighted that several influential factors, particularly social determinants, could impact the confidentiality of electronic health records (EHRs). They emphasized that aspects such as the perspectives of health care consumers significantly influence policy makers' decisions in planning and enhancing the acceptance and implementation of the National Electronic Health Records (NEHRs) in Saudi Arabia (KSA). Consequently, the trust of health care consumers in the government's ability to maintain confidentiality and adhere to established standards for accessing patient data is a critical factor in ensuring the confidentiality of EHRs (Alsahafi et al., 2020).

Almulhem [15] reported that participants were granted unrestricted access to medical records. Their responses to open-ended questions revealed the necessity for appropriate regulations governing such access. Compared to traditional paper-based medical records, medical students reported a more favorable experience with EHRs. Furthermore, various essential skills could be acquired by medical students through interacting with medical records, which would benefit their future professional practice. However, the educational experiences of medical students were constrained when they were provided with read-only access. Almulhem also stressed the importance of adequate EHR training for medical students prior to granting them access, as this training facilitates their ability to practice and use EHR systems effectively.

Despite the potential benefits of EHRs, the health care system in the KSA faces numerous challenges in adopting these systems, particularly concerning privacy concerns. For instance, Jabali and Jarrar identified resistance to change among some medical staff as a significant barrier to implementing EHR systems and ensuring data security. Additionally, certain medical personnel exhibited reluctance to adopt information technologies designed to mitigate patient data breaches. The study also noted that insufficient funding strategies hindered the development of robust confidentiality programs for EHRs, and that inadequate training for medical staff on the proper and secure use of EHR systems posed further obstacles (Jabali & Jarrar, 2018).

Chikhaoui et al. focused on the challenges associated with EHR adoption, specifically in the context of cloud computing. They highlighted risks such as hackers potentially accessing sensitive patient data and computer viruses compromising the integrity of patient records. Furthermore, the portability of data enabled by cloud computing presents additional challenges for EHR implementation in the KSA. Despite these concerns, cloud computing was recognized for enhancing the efficiency of health care processes by enabling centralized data storage and processing (Chikhaoui et al., 2017).

Similarly, Alqahtani et al. emphasized that patient involvement is key to improving EHR adoption. Their study revealed that patients asserted their right to make decisions based on the

medical care they receive, including the right to accept or refuse treatment and the right to establish advance directives. As such, patient awareness plays a pivotal role in facilitating the adoption of EHRs, enabling them to make timely decisions regarding privacy and confidentiality in their health care.

Almuayqil et al. identified major challenges in ensuring data integrity and security during EHR adoption, with connectivity issues between information systems being a primary concern. Other barriers included cultural obstacles related to technical expertise and limited computer skills. Health care professionals ranked security and privacy as the third most significant barrier, citing concerns such as unauthorized access to medical records without patient or physician consent. Additionally, IT experts stressed the importance of implementing robust security and privacy measures to safeguard patient information. Addressing these challenges is essential for smooth EHR adoption and maintaining confidentiality (Almuayqil et al., 2016).

The perspectives of physicians regarding EHR privacy in the KSA were examined by Alshahrani et al. The study found that physicians considered EHR systems protected by password-protected software to be more secure and private than paper-based records. They agreed that the advantages and utility of EHRs outweighed potential risks. Moreover, the use of computers in health care was deemed highly beneficial, contributing to the widespread adoption of EHRs in the largest institutions in the KSA. These insights can guide policy makers in advocating for the broader deployment of EHRs while ensuring that privacy, security, and confidentiality of patient information remain uncompromised (Alshahrani et al., 2021).

The limitations of this study included the limited availability of relevant publications in the KSA, a lack of original findings, and potential biases in the methodology. Conversely, the strengths of the study were the systematic review of articles published within the last five years, which are considered relatively recent. Additionally, the study's focus on the Saudi population provided more targeted and relevant results.

Recommendations

- Launch public awareness campaigns to educate patients about the benefits of EHR systems and their privacy safeguards.
- Ensure patients have access to information about their rights to data privacy and control over their medical records.
- Invest in advanced cybersecurity tools, such as encryption combined with steganography, to enhance data security.
- Regularly update and test security systems, including intrusion detection and prevention tools.
- Provide mandatory EHR training for health care professionals, emphasizing privacy and secure system usage.
- Design initiatives to bridge cultural and skill gaps, such as workshops focused on digital literacy for health care professionals.
- While leveraging the efficiency of cloud computing, implement robust data protection strategies to address portability and access risks.

Conclusion

The adoption of electronic health records (EHRs) in Saudi Arabia offers immense potential to revolutionize the health care sector by improving efficiency, accessibility, and patient outcomes. However, challenges such as privacy concerns, resistance to change, and insufficient training for health care professionals continue to hinder full-scale implementation. Addressing these issues requires a multifaceted approach, including enhanced cybersecurity measures, comprehensive training programs, and fostering patient trust. By overcoming these barriers,

Saudi Arabia can achieve a robust and secure EHR system, ensuring confidentiality and building a solid foundation for the future of digital health care.

References

Almuayqil, S., Atkins, A. S., & Sharp, B. (2016). Ranking of E-Health Barriers Faced by Saudi Arabian Citizens, Healthcare Professionals and IT Specialists in Saudi Arabia. *Health*, *08*(10), 1004–1013. https://doi.org/10.4236/health.2016.810104

Alsahafi, Y. A., Gay, V., & Khwaji, A. (2020). *The Acceptance of National Electronic Health Records in Saudi Arabia: Healthcare Consumers' Perspectives*. ACIS. https://www.semanticscholar.org/paper/The-Acceptance-of-National-Electronic-Health-in-Alsahafi-Gay/db8431f1454a816bcfa77483bb4b953537db8dca

Alshahrani, A., Jamal, A., & Tharkar, S. (2021). How private are the electronic health records? Family physicians' perspectives towards electronic health records privacy. *Journal of Health Informatics in Developing Countries*, *15*(1), Article 1. https://www.jhidc.org/index.php/jhidc/article/view/298

Altamimi, S., Renaud, K., & Storer, T. (2020). Correction to: "I do it because they do it": Social-Neutralisation in Information Security Practices of Saudi Medical Interns. In S. Kallel, F. Cuppens, N. Cuppens-Boulahia, & A. Hadj Kacem (Eds.), *Risks and Security of Internet and Systems* (Vol. 12026, pp. C1–C1). Springer International Publishing. https://doi.org/10.1007/978-3-030-41568-6_25

Altamimi, S., Storer, T., & Alzahrani, A. (2018). The role of neutralisation techniques in violating hospitals privacy policies in Saudi Arabia. *2018 4th International Conference on Information Management (ICIM)*, 133–140. https://doi.org/10.1109/INFOMAN.2018.8392823

Chikhaoui, E., Sarabdeen, J., & Parveen, R. (2017). Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia. *Communications of the IBIMA*, 1–18. https://doi.org/10.5171/2017.369309

Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. *Sustainability*, *13*(5), 2800. https://doi.org/10.3390/su13052800

Evans, R. S. (2016). Electronic Health Records: Then, Now, and in the Future. *Yearbook of Medical Informatics*, *25*(S 01), S48–S61. https://doi.org/10.15265/IYS-2016-s006

Hameed, S. S., Hassan, W. H., Abdul Latiff, L., & Ghabban, F. (2021). A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science*, *7*, e414. https://doi.org/10.7717/peerj-cs.414

Jabali, A. K., & Jarrar, M. (2018). Electronic Health Records Functionalities in Saudi Arabia: Obstacles and Major Challenges. *Global Journal of Health Science*, *10*(4), 50. https://doi.org/10.5539/gjhs.v10n4p50

Jabeen, F., Hamid, Z., Akhunzada, A., Abdul, W., & Ghouzali, S. (2018). Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues. *IEEE Access*, *6*, 17246–17263. https://doi.org/10.1109/ACCESS.2018.2810337

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Masud, M., Gaba, G. S., Choudhary, K., Alroobaea, R., & Hossain, M. S. (2021). A robust and lightweight secure access scheme for cloud based E-healthcare services. *Peer-to-Peer Networking and Applications*, *14*(5), 3043–3057. https://doi.org/10.1007/s12083-021-01162-x

Mishah, N., Bukhari, A., AlMutairi, B., & Mohreq, M. (2019). Status of e-security and privacy protection in Saudi hospitals. *Computer Methods and Programs in Biomedicine*, *171*, 5–6. https://doi.org/10.1016/j.cmpb.2018.12.012

Rieder, P., Louis-Courvoisier, M., & Huber, P. (2016). The end of medical confidentiality? Patients, physicians and the state in history. *Medical Humanities*, *42*(3), 149–154. https://doi.org/10.1136/medhum-2015-010773

Samkari, H., & Gutub, A. (2019). *Protecting Medical Records against Cybercrimes within Hajj Period by 3-layer Security*. https://doi.org/10.5281/ZENODO.3543455

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

T. Alanazi, S., Anbar, M., A. Ebad, S., Karuppayah, S., & Al-Ani, H. A. (2020). Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. *Symmetry*, *12*(9), 1544. https://doi.org/10.3390/sym12091544