How to Cite:
Alhejaili, S. E. F., Alhejaili, A. R., Alyehya, A. A., Alharbi, F. S., Almotairi, M. M. H., Almutairi, M. S. M., Almutairi, N. S., Al Ahmadi, S. A. M., Almughathawi, A. S., Alraddadii, A. S., Alsuhaymi, F. G., Hazazi, M. M. M., & Alanazi, M. M. M. (2023). Challenges and solutions in medical record keeping and data security. *International Journal of Health Sciences*, *7*(S1), 3711–3721. https://doi.org/10.53730/ijhs.v7nS1.15326

Challenges and solutions in medical record keeping and data security

Salman Eid Fadhi Alhejaili
KSA, National Guard Health Affairs

Abdullah Raja Alhejaili
KSA, National Guard Health Affairs

Abeer Ali Alyehya
KSA, National Guard Health Affairs

Fayez Suliman Alharbi
Qassim Armed Forces Hospital

Mohammed Monawer H. Almotairi
Qassim Armed Forces Hospital

Muneer Shudayyid Muneer Almutairi
Qasim Aremed Forces Hospital

Nawaf Sakr Almutairi
National Guard Hospital

Sultan Abdulaziz Muhanna Al Ahmadi
KSA, National Guard Health Affairs

Abdulaziz Salman Almughathawi
KSA, National Guard Health Affairs

Abdlraheem Salem Alraddadii
KSA, National Guard Health Affairs

Fahad Ghali Alsuhaymi
KSA, National Guard Health Affairs

Mohammed Maqbul Mohammed Hazazi
Prince Sultan Air Base, Al-Kharj

International Journal of Health Sciences E-ISSN 2550-696X © 2023.
***Corresponding email**: akk29337@gmail.com*
Manuscript submitted: 01 Jan 2023, Manuscript revised: 09 Jan 2023, Accepted for publication: 15 Jan 2023

Mohammad Mamdouh Mohammed Alanazi
Prince Sultan Air Base, Al-Kharj

***Abstract*---**This literature review analyzes the challenges and solutions associated with the security and privacy of electronic health records (EHR). The extensive implementation of electronic health records (EHRs) provides advantages, including cost savings and enhanced quality of care, yet it also presents considerable vulnerabilities. Patient concerns regarding data protection are significant, driven by fears of unauthorized access and data breaches. This review examines the security risks associated with EHR systems, emphasizing three primary categories of safeguards: administrative, physical, and technical. This study examines the challenges presented by the Internet of Things (IoT) in relation to Electronic Health Records (EHRs), emphasizing the necessity for strong security protocols to manage heterogeneity, uncontrolled environments, and scalability requirements. This paper examines diverse security solutions, such as encryption and access control mechanisms, including Role-Based Access Control (RBAC), while emphasizing the significance of a multidisciplinary approach in the management of Electronic Health Record (EHR) systems. The rising frequency of cyberattacks on healthcare organizations highlights the necessity for proactive risk management strategies, which should encompass regular security audits, staff training, and the establishment of robust physical and technical safeguards. The review highlights the essential requirement for standardized protocols and strong security measures to safeguard patient privacy and maintain data integrity in the developing context of EHR systems.

***Keywords*---**Internet of Things (IoT), cybersecurity, data privacy, EHR security, and healthcare informatics.

1. Introduction

An electronic health record (EHR) is a digital representation of a patient's medical history, systematically maintained by a healthcare provider, encompassing essential clinical and administrative information pertinent to the patient's care. This includes demographic information, progress notes, medical conditions, prescribed medications, vital signs, immunization records, laboratory results, and radiology reports (1). The ongoing dependence on paper records in numerous healthcare facilities has resulted in substantial documentation, leading organizations to transition to electronic health records. Carey et al. (2) highlight that integrated health records provide substantial advantages, such as cost reduction, improved care quality, facilitation of evidence-based medicine, and enhanced record portability. For an EHR system to maintain effectiveness, it must fulfill specific criteria, including data completeness, fault tolerance, high availability, and compliance with security protocols (3). Despite the benefits,

various obstacles have impeded the broad adoption of electronic health records, encompassing financial, organizational, and attitudinal issues.

In recent years, numerous governments have acknowledged the significance of integrated electronic health records (EHRs) in enhancing healthcare delivery. In 2004, the U.S. government established a goal to connect the majority of Americans to an electronic health record (EHR) system by 2014 (4). The American Recovery and Reinvestment Act of 2009 designated $19 billion for the digitization of healthcare records (5). In 2010, European Union countries proposed a plan to create a unified health system by 2015, with the objective of enhancing the sharing of patient data across borders to improve healthcare quality and efficiency (5). Nonetheless, there has been minimal advancement in resolving privacy concerns related to the shift from paper to digital records, especially within integrated EHR systems (6). The swift progress in information and communication technologies has generated apprehensions regarding security and privacy. Data security and patient privacy present significant challenges to the implementation of electronic health records, underscoring the necessity for healthcare organizations to formulate robust data protection strategies (7).

2. Electronic health records

Electronic health records, or electronic medical records (EMRs), have become increasingly significant in the e-health sector (8). Electronic Medical Records (EMRs), which encompass patient health information, are essential to e-health and are legally recorded in hospital environments. These records function as primary data sources for electronic health records. Healthcare professionals may exhibit mistrust towards EMR systems in daily hospital operations, stemming from their experiences with traditional methods. Albahri (9) discusses the emergence of e-health in the early 21st century, highlighting its utilization of information and communication technologies for the provision of healthcare services. Effective management of e-health necessitates a multidisciplinary approach that encompasses telecommunications, computer science, and instrumentation to enable the exchange of medical data over extensive geographic regions (10). E-health enhances the ability of healthcare providers to connect effectively, thereby improving the quality and operational efficiency of services delivered to patients.

The terms "electronic medical record" and "electronic health record" denote systems that store patient health information and underpin e-health applications (11). Electronic Health Records facilitate the efficient exchange of medical information among stakeholders and permit the updating of patient data as treatment advances. Alsalem et al. (12) highlight that health information technology can markedly improve efficiency, patient safety, and healthcare outcomes, while also reducing costs. EHRs provide cost-saving advantages through the digitization of data and the centralization of medical information. Historically, healthcare data was primarily recorded on paper; however, the past three decades have witnessed substantial adoption of health information technology. Many physicians continue to express concerns regarding unauthorized access to patient information in EMRs, apprehensive about potential misuse and the legal ramifications of confidentiality breaches. Wikina

(13)observed that physicians place a higher emphasis on security and confidentiality compared to patients, with numerous doctors continuing to favor paper records due to perceived security benefits. This concern highlights the significance of privacy in electronic medical record systems, as patients may refrain from disclosing information if their privacy is not guaranteed (14).

This research may provide important insights for healthcare stakeholders and other agencies concerning the selection, development, and implementation of EHRs that emphasize patient privacy and security. This paper functions as a resource for information custodians tasked with managing security in healthcare, as well as for scholars focused on improving patient privacy and security in electronic health record systems.

3. Privacy concerns regarding electronic health records

Numerous surveys have reported privacy and security concerns regarding electronic health records (EHRs), indicating substantial patient anxiety about data protection. Shi et al. (15) reported that around two-thirds of patients were concerned about the privacy of their health records, while only 39% expressed confidence in the security of their data. In certain instances, respondents expressed a lack of trust in the safety of their data and doubted its adequate protection (16). Akhlaq et al. (17) conducted a study indicating that 50% of participants expressed concerns regarding data security related to internet transmission. Almost fifty percent of participants in a study conducted by Ancker et al. (18) expressed concerns that sharing health information might jeopardize their privacy. Research highlighting individual concerns regarding data privacy emphasizes its significance in the successful adoption of electronic health records (EHR).

4. Challenges related to privacy and security in the context of the Internet of Things

Challenges related to privacy and security that are specific to the Internet of Things (IoT) stem from its unique characteristics, including heterogeneity, an uncontrolled environment, limited resources, and scalability demands. Small IoT devices are equipped with advanced cryptographic engines and adequate memory to implement essential security measures. Razmak and Bélanger (19) identified essential IoT security requirements, categorizing them into identity management, network security, resilience and trust, and privacy. The study analyzed multiple proposed IoT architectures and concluded that, although certain security needs are met, no singular architecture satisfies all security requirements comprehensively.

EHR systems utilize three main categories of security safeguards: physical, technical, and administrative. Each category includes strategies employed by healthcare organizations to protect sensitive health information. Administrative safeguards encompass audits, the appointment of a chief information security officer, and contingency planning to ensure adherence to security policies and procedures (15). Physical safeguards consist of measures designed to prevent unauthorized physical access to health information systems, including restricted

access to hardware and software to mitigate misuse or tampering (16). Research indicates that violations of physical safeguards are a primary factor in security incidents (20). Technical safeguards, the third category, serve to protect entire information systems through the implementation of firewalls, encryption, antivirus software, and authentication measures, addressing the frequent vulnerabilities to electronic breaches via computers and other portable devices (20). Els and Cillier's research (21) concluded that firewalls and cryptographic techniques are among the most commonly implemented technical safeguards, whereas other security measures, such as antivirus software and cloud computing, are contingent upon organizational budgets (22).

Liu et al. (20) emphasized that physical access controls, including the locking of computer systems, serve to enhance technical measures such as firewalls and encryption in the protection of patient data. Amer (23) conducted a study on the ethical use of genomic data and electronic health records (EHRs), concluding that encryption serves as a reliable technical safeguard, whereas administrative safeguards involve techniques such as de-identifying samples. Technical safeguards are enhanced by implementing firewalls and encryption, whereas administrative protections encompass extensive training and security plans. Shi et al. (13) observed that administrative safeguards encompass management approvals for the release of paper records and staff training on responding to incidents involving missing records. Physical safeguards may include the implementation of security cameras to prevent unauthorized access.

Advancements in technology have led to an increase in security breaches targeting healthcare organizations, necessitating the adoption of contemporary risk management practices. Organizations like the Clinical Engineering Information Technology Community, the American College of Clinical Engineering, and the Healthcare Information and Management Systems Society play a crucial role in assisting healthcare facilities in improving EHR security. Implementing risk assessment and management strategies, along with partnerships with prominent organizations, enhances the security of patient information within electronic health record systems. Healthcare providers have implemented Radio Frequency Identification (RFID) technology to store data in RFID tags and limit access, enhancing privacy and allowing only authorized personnel to access the information. The appointment of a Chief Information Security Officer can facilitate the effective coordination of all security practices within electronic health records (19).

Firefox serves as a technology for safeguarding healthcare organizations' information systems, providing network security and ensuring data protection against internal and external threats. However, the Infosec Institute has indicated that the increase in EHR adoption has not consistently matched by robust cybersecurity measures, resulting in heightened vulnerability to cyberattacks within the healthcare sector. Research indicates that security breaches in healthcare incur significant costs, with data breaches potentially resulting in settlement expenses for hospitals ranging from $250,000 to $2.5 million. Enhancing IT security and privacy protocols in healthcare environments is crucial for delivering safe and effective care (20).

5. Security incidents related to information technology in healthcare environments

The swift integration of electronic health records (EHRs) in recent years has led to notable advancements in healthcare, while simultaneously increasing the industry's vulnerability to cybersecurity threats (24). The Infosec Institute indicates that the extensive adoption of EHRs has not been accompanied by sufficient cybersecurity measures, resulting in increased vulnerability of healthcare organizations to cyber threats and related damages (2021). This issue is reflected in various reports detailing numerous IT-related security incidents in hospitals and other healthcare environments (25). A 2014 report by the Information Security Media Group indicated that 75% of surveyed U.S. healthcare organizations encountered at least one security breach affecting fewer than 500 individuals, whereas 21% reported breaches impacting over 500 individuals (26). A survey conducted by the Healthcare Information and Management Systems Society (HIMSS) in 2015 indicated that 68% of U.S. healthcare organizations faced significant security incidents, with threats arising from internal sources (53.7%) and external sources (63.6%) (27).

IT security breaches in healthcare are likely underreported or inadequately documented, indicating that the true incidence of such events may exceed reported figures. Numerous breaches remain undetected, and organizations may be reluctant to disclose them due to concerns regarding reputational damage or potential legal repercussions (28). The financial consequences of these breaches can be significant; for example, Absolute Software Corporation estimated that healthcare data breaches may result in settlement payments for hospitals ranging from $250,000 to $2.5 million. This reflects only a portion of the financial implications, as expenses also encompass operational disruptions, regulatory penalties, and erosion of patient trust (29).

Concerns regarding security and privacy represent a substantial obstacle to the adoption of advanced information technology within the healthcare sector. Concerns regarding liability and breaches inhibit numerous healthcare providers from completely adopting IT solutions in their services, notwithstanding the possible enhancements to patient care and operational efficiency. Enhancing IT security and privacy protocols in healthcare facilities is essential for providing safe and effective care. Liu et al. (30) assert that healthcare organizations can mitigate these concerns through the implementation of comprehensive security measures that are aligned with their IT development plans. Addressing insider threats, which are breaches caused by authorized personnel, continues to pose a significant challenge. Insiders possess access to sensitive data, complicating the detection and attribution of malicious actions to particular individuals (31).

Information and Communication Technologies (ICT) have enabled patients to engage actively in their healthcare. Modern patients differ from traditional, passive healthcare recipients in that they can access their health records, make informed choices, and engage in treatment decisions. Increased engagement has, however, introduced challenges related to data access and privacy. Maintaining data security and privacy necessitates a balance between the freedoms afforded to data issuers, such as healthcare providers, and data subjects, namely patients.

Addressing these challenges requires the implementation of robust privacy measures, stringent security protocols, and effective key management practices within EHR systems (32).

Privacy and security concerns have emerged as significant obstacles to the implementation of electronic health records in recent years. Healthcare organizations advancing in digitization must prioritize both patient care and the safeguarding of sensitive health information. Implementing advanced encryption, access controls, and continuous monitoring enables healthcare facilities to enhance the security of EHR systems and mitigate vulnerabilities. Furthermore, educating personnel on cybersecurity best practices and establishing incident response protocols are critical for ensuring a secure healthcare environment. Effective cybersecurity in healthcare necessitates a comprehensive strategy that considers both technological and human elements, allowing healthcare providers to deliver secure, efficient, and reliable digital services to patients (34-36). Table 1 provides a summary of key areas, associated threats, and proposed solutions.

Table 1. Summary of IT Security Challenges and Solutions in Healthcare

Category	Key Challenges	Common Threats	Proposed Solutions
Electronic Health Records (EHRs)	High vulnerability due to widespread adoption, lack of robust security	Data breaches, unauthorized access	Enhanced encryption, access controls, staff training on data privacy
Insider Threats	Difficult to detect due to authorized access	Malicious actions by internal personnel	Role-based access control (RBAC), continuous monitoring, auditing, and administrative safeguards
External Threats	Cyber-attacks from hackers and malware targeting sensitive health data	Phishing, ransomware, data theft	Firewalls, antivirus software, regular security audits, incident response protocols
Patient Privacy Concerns	Anxiety over data security, potential breaches in EHR and IoT usage	Lack of trust in EHR, reluctance to share data	Transparent privacy policies, patient education on data usage, secure transmission methods
IoT Integration	Heterogeneous devices with variable security levels, high scalability demands	Unauthorized access to IoT devices, limited security	Implementation of secure IoT protocols, identity management, and privacy measures
Financial Impact of Breaches	High costs from data breaches, fines, loss of patient trust	Financial losses, liability costs	Risk management plans, comprehensive cyber insurance, and adoption of strong organizational security

Category	Key Challenges	Common Threats	Proposed Solutions
			protocols
Legal and Compliance Issues	Need for compliance with regulations (e.g., HIPAA) and evolving cybersecurity standards	Non-compliance penalties, regulatory fines	Adherence to HIPAA guidelines, regular policy updates, training on regulatory requirements
User Training and Awareness	Lack of awareness among staff regarding IT security practices	Human error leading to breaches	Regular cybersecurity training, awareness campaigns, and establishment of clear IT security guidelines

6. Conclusion

This literature review discusses EHR security and privacy, including the advantages of exchanging medical data across healthcare providers and possible remedies. EHRs make patient data easier to access and update, but also present security risks. Harmonization is essential to address disputes between rules and standards. EHRs should use efficient encryption and RBAC access control. Effective management needs a multidisciplinary team with communications, instrumentation, and computer science to communicate data across areas.

References

1. Kim SH, Kwon J. How do EHRs and a meaningful use initiative affect breaches of patient information? Information Systems Research. 2019;30(4):1184-202.
2. Carey DJ, Fetterolf SN, Davis FD, Faucett WA, Kirchner HL, Mirshahi U, et al. The Geisinger MyCode community health initiative: an electronic health record–linked biobank for precision medicine research. Genetics in medicine. 2016;18(9):906-13.
3. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021;22(2):177-83.
4. Ahmad KAB, Khujamatov H, Akhmedov N, Bajuri MY, Ahmad MN, Ahmadian A. Emerging trends and evolutions for smart city healthcare systems. Sustainable Cities and Society. 2022;80:103695.
5. Walid R, Joshi KP, Choi SG, Kim D-y, editors. Cloud-based encrypted ehr system with semantically rich access control and searchable encryption. 2020 IEEE international conference on big data (Big Data); 2020: IEEE.
6. Acquisti A, Brandimarte L, Loewenstein G. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. Journal of Consumer Psychology. 2020;30(4):736-58.
7. Lemke J. Storage and security of personal health information. OOHNA J. 2013;32(1):25-6.
8. Achampong EK. Electronic health record (EHR) and cloud security: the current issues. International Journal of Cloud Computing and Services Science. 2013;2(6):417.

9. Albahri OS, Albahri AS, Mohammed K, Zaidan A, Zaidan B, Hashim M, et al. Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: Taxonomy, open challenges, motivation and recommendations. Journal of medical systems. 2018;42:1-27.
10. Kiah MLM, Zaidan B, Zaidan A, Nabi M, Ibraheem R. MIRASS: Medical informatics research activity support system using information mashup network. Journal of medical systems. 2014;38:1-15.
11. Miotto R, Li L, Kidd BA, Dudley JT. Deep patient: an unsupervised representation to predict the future of patients from the electronic health records. Scientific reports. 2016;6(1):1-10.
12. Alsalem M, Zaidan A, Zaidan B, Hashim M, Albahri OS, Albahri AS, et al. Systematic review of an automated multiclass detection and classification system for acute Leukaemia in terms of evaluation and benchmarking, open challenges, issues and methodological aspects. Journal of medical systems. 2018;42:1-36.
13. Wikina SB. What caused the breach? An examination of use of information technology and health data breaches. Perspectives in health information management. 2014;11(Fall).
14. Hussain M, Al-Haiqi A, Zaidan AA, Zaidan BB, Kiah M, Iqbal S, et al. A security framework for mHealth apps on Android platform. Computers & Security. 2018;75:191-217.
15. Shi S, He D, Li L, Kumar N, Khan MK, Choo K-KR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & security. 2020;97:101966.
16. Lafky DB, Horan TA. Personal health records: Consumer attitudes toward privacy and security of their personal health information. Health Informatics Journal. 2011;17(1):63-71.
17. Akhlaq A, McKinstry B, Muhammad KB, Sheikh A. Barriers and facilitators to health information exchange in low-and middle-income country settings: a systematic review. Health policy and planning. 2016;31(9):1310-25.
18. Ancker JS, Silver M, Miller MC, Kaushal R. Consumer experience with and attitudes toward health information technology: a nationwide survey. Journal of the American Medical Informatics Association. 2013;20(1):152-6.
19. Razmak J, Bélanger C. Using the technology acceptance model to predict patient attitude toward personal health records in regional communities. Information Technology & People. 2018;31(2):306-26.
20. Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. Jama. 2015;313(14):1471-3.
21. Els F, Cilliers L, editors. Improving the information security of personal electronic health records to protect a patient's health information. 2017 Conference on Information Communication Technology and Society (ICTAS); 2017: IEEE.
22. Gupta B, Agrawal DP. Handbook of research on cloud computing and big data applications in IoT: IGI global; 2019.
23. Amer K. Informatics: Ethical Use of Genomic Information and Electronic Medical Records. Online Journal of Issues in Nursing. 2015;20(2).
24. Paganini P. Risks and cyber threats to the healthcare industry. Infosec Institute. 2014.
25. Uwizeyemungu S, Poba-Nzaou P, Cantinotti M. European hospitals' transition toward fully electronic-based systems: do information technology security

and privacy practices follow?. JMIR medical informatics. 2019 Mar 25;7(1):e11211.
26. Healthcare Information Security. Princeton, NJ: ISMG; 2014. The State of Healthcare Information Security Today. Update on HIPAA Omnibus Compliance, Protecting Patient Data URL: https://www.healthcareinfosecurity.com/surveys/state-healthcare-information-security-today-s-23 [accessed 2019-02-04]
27. HIMSS. Chicago, IL: HIMSS; 2015 Jun. 2015 HIMSS Cybersecurity Survey URL: https://www.himss.org/2015-cybersecurity-survey/full-report [accessed 2019-02-04]
28. Theodos K, Sittig S. Health information privacy laws in the digital age: HIPAA doesn't apply. Perspectives in health information management. 2020 Dec 7;18(Winter):1l.
29. Ahmad A, Desouza KC, Maynard SB, Naseer H, Baskerville RL. How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology. 2020 Aug;71(8):939-53.
30. Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. Jama. 2015 Apr 14;313(14):1471-3.
31. Donnelly R, Johns **J.** Recontextualising remote working and its HRM in the digital economy: An integrated framework for theory and practice. The International Journal of Human Resource Management. 2021 Jan 2;32(1):84-105.
32. Ganiga R, Pai RM, Sinha RK. Security framework for cloud based electronic health record (EHR) system. International Journal of Electrical and Computer Engineering. 2020 Feb 1;10(1):455.
33. Shamshad S, Mahmood K, Kumari S, Chen CM. A secure blockchain-based e-health records storage and sharing scheme. Journal of Information Security and Applications. 2020 Dec 1;55:102590.
34. Mayer AH, da Costa CA, Righi RD. Electronic health records in a Blockchain: A systematic review. Health informatics journal. 2020 Jun;26(2):1273-88.
35. Fennelly O, Cunningham C, Grogan L, Cronin H, O'Shea C, Roche M, Lawlor F, O'Hare N. Successfully implementing a national electronic health record: a rapid umbrella review. International Journal of Medical Informatics. 2020 Dec 1;144:104281.
36. Dubovitskaya A, Baig F, Xu Z, Shukla R, Zambani PS, Swaminathan A, Jahangir MM, Chowdhry K, Lachhani R, Idnani N, Schumacher M. ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. Journal of medical Internet research. 2020 Aug 21;22(8):e13598.

التحديات والحلول في حفظ السجلات الطبية وأمان البيانات

الملخص

تحلل هذه المراجعة الأدبية التحديات والحلول المرتبطة بأمان وخصوصية السجلات الصحية الإلكترونية .(EHR) توفر السجلات الصحية الإلكترونية (EHRs) تنفيذًا واسع النطاق فوائد، بما في ذلك توفير التكاليف وتحسين جودة الرعاية، ومع ذلك، فإنها تقدم أيضًا ثغرات كبيرة. إن مخاوف المرضى بشأن حماية البيانات هي قضايا مهمة، مدفوعة بمخاوف من الوصول غير المصرح به وانتهاكات البيانات. تستعرض هذه المراجعة مخاطر الأمان المرتبطة بأنظمة السجلات الصحية الإلكترونية، مع التركيز على ثلاث فئات رئيسية من التدابير الوقائية: الإدارية، والبدنية، والتقنية. كما تتناول هذه الدراسة التحديات التي يطرحها إنترنت الأشياء (IoT)فيما يتعلق بالسجلات الصحية الإلكترونية(EHRs) ، مع التأكيد على ضرورة وجود بروتوكولات أمان قوية لإدارة التنوع والبيئات غير المحكومة ومتطلبات التوسع. تبحث هذه الورقة في حلول أمان متنوعة، مثل التشفير وآليات التحكم في الوصول، بما في ذلك التحكم القائم على الدور(RBAC) ، مع التأكيد على أهمية نهج متعدد التخصصات في إدارة أنظمة السجلات الصحية الإلكترونية .(EHR) تسلط الزيادة المتكررة للهجمات السيبرانية على المؤسسات الصحية الضوء على ضرورة وجود استراتيجيات استباقية لإدارة المخاطر، والتي يجب أن تشمل تدقيقات أمان دورية، وتدريب الموظفين، وإنشاء تدابير وقائية بدنية وتقنية قوية. تبرز المراجعة الحاجة الأساسية لبروتوكولات موحدة وتدابير أمان قوية لحماية خصوصية المرضى والحفاظ على سلامة البيانات في سياق تطور أنظمة السجلات الصحية الإلكترونية.

الكلمات المفتاحية: إنترنت الأشياء (IoT)، الأمن السيبراني، خصوصية البيانات، أمان السجلات الصحية الإلكترونية، والمعلوماتية الصحية.