*Med. J. Cairo Univ., Vol. 90, No. 9, publication: 15 jan 2022*
*2865-2871*
https://www.medicaljournalofcairouniversity.net
https://mjcu.journals.ekb.eg

# Security and Privacy of Healthcare Records

MOHAMMED FARHAN ALDHAFIRI, ALMATRAFI JABER SADI, ALI MUTALEQ ALSUBAIE, ABDULKARIM SHUNAYN ALANAZI, SAYEL SALEH ALRASHIDI and MOHAMMED MESFER MUSAED AL KHATHAMI Faisal Barjas AlHarbi and Manar Ibrahem Al Wehaibi and Fahad Husayyan Al Enazi and Amani Mohammad Al Mubarak And Iman Olayan Al Mutairi And Enass Mohammed Almetery And MAHA MOSLEH ALBUGAMI And LILA MUTEB Almutairi And Amani Abdulmohsen Alshammari

*Medical Records KSA*

## Abstract

The transition from paper-based to electronic health records (EHRs) has revolutionized healthcare delivery, offered numerous benefits while introduced significant security challenges. This paper explores strategies for securing EHRs, focusing on the importance of physical, technical, and administrative safeguards. Key topics include the role of legislative initiatives like the ARRA/HITECH Act in driving EHR adoption, the impact of cyber threats on healthcare security, and the implementation of encryption and digital signature technologies to protect patient information. The discussion also addresses unintended consequences of EHR implementation, such as system design flaws and information sharing vulnerabilities. Recommendations for mitigating security risks include the use of firewalls, data encryption, and stringent access control measures. Additionally, the paper highlights the importance of staff training and compliance with HIPAA regulations to ensure the confidentiality and integrity of health records. By adopting a comprehensive approach to EHR security, healthcare providers can safeguard patient information, maintain trust, and enhance the efficiency of healthcare delivery systems.

**Key Words:** *Electronic Health Records (EHRs) – Security – Encryption – HIPAA compliance – Cyber threats – Data privacy – Healthcare delivery.*

## Introduction

Paper health records have given way to electronic health records (EHRs) in the US. Widespread technological use, its perceived utility, and legislative actions have all contributed to this change. The American Recovery and Reinvestment Act (ARRA) and Health Information Technology for Economic and Clinical Health (HITECH Act) of 2009 included financial incentives, which, when combined with the Federal Health Information Technology Strategic Plan, have greatly increased the adoption of EHRs **[1]**. Approximately 75% of physician offices and 92% of hospitals obtained financial incentives for implementing EHRs between the Act's enactment in 2009 and 2014 **[1]**. According to Bowman **[2]**, implementing EHRs and health information technology (HIT) is crucial to changing the US healthcare system so that it can provide high-quality treatment more reliably, safely, and efficiently.

In addition to improving healthcare quality, lowering costs, and supporting evidence-based practice and record-keeping, integrated health records also make information sharing easier **[3]**. EHRs need to comply with safety and security regulations and provide complete data in order to continue being effective. But as EHRs are used more often, a lot more data is being available to both authorized and illegal users **[4]**. One of the biggest obstacles to the implementation of health records databases is the current state of serious concerns regarding the security and privacy of healthcare data kept in electronic databases. In order to secure EHRs and stop unwanted third-party access, healthcare organizations must devise security measures. This review of the literature focuses on examining security risks associated with the use and deployment of EHRs as well as countermeasures.

The electronic form of patient records that healthcare professionals have on file is called an EHR. Patients' personal information, a list of symptoms, diagnoses, vaccination records, medication histories, allergies, test findings, and radiological results are all kept in electronic health records (EHRs) **[4]**. Health information on patients can be gathered and stored by EHR systems, and then shared with healthcare providers. Software programs called electronic medical records (EMRs) are used to exchange data regarding patient medical histories, medical treatments, and laboratory test results **[5]**. These apps give healthcare professionals rapid access to patient data, regardless of their location or

***Correspondence to:*** Mohammed Farhan Aldhafiri,
Medical Records KSA

schedule, and provide the assistance they need to make better clinical decisions [6]. But more accessibility also means a higher chance of security lapses that jeopardize patient confidentiality and privacy.

By decreasing medical errors, encouraging collaboration and communication, offering real-time patient health information, facilitating information sharing among clinicians, and gathering health data for clinical decision-making and research, the implementation of EHRs aims to improve the delivery of high-quality care [7,4]. EHRs improve patient data access, retrieval, and portability, among other benefits [8]. Electronic charts, in contrast to paper records, are easily retrievable and can be consulted concurrently by several people. Furthermore, analysis of individual patient data can be used to pinpoint risk factors and direct treatment in accordance with accepted guidelines.

Enacted in 2009, the HITECH Act aims to advance health information technology (HIT), with a particular focus on electronic health records (EHRs). Additionally, it reinforced the HIPAA Act of 1996's enforcement by enacting harsher sanctions for non-compliance. In 2008, just 10% of hospitals had EHRs in place prior to HITECH. Healthcare providers are required to implement EHRs in order to facilitate information exchange among various entities, progress healthcare, and improve care coordination. HITECH established incentives to promote the use of EHRs because the costs associated with switching from paper to electronic records were prohibitive. As a result, from 3.2% in 2008 to 14.2% in 2015, EHR usage increased. 86% of doctors who practice in offices by 2017 had adopted electronic health records [9]. The use of electronic records has increased significantly since the Act's enactment in 2009. EMRs were used in 95% of clinical decision-making and healthcare delivery in the US by 2017 [10]. The imperative to enhance healthcare quality, attain efficiency, and tackle mounting budgetary strains has propelled this expansion.

### *Security of Medical Records:*

The three key elements of EHR systems are privacy, security, and confidentiality [11]. People have the moral right to privacy, which allows them to decide when and how their personal information is accessed and shared. As part of EHR security, data and security resources are safeguarded, including data storage and transit between computer systems [12]. Upholding rules for the sharing and archiving of personal data with other parties is a component of protecting privacy, which is a subset of security. Data security is the process of limiting access to private patient information by unauthorized personnel. Conversely, information leaks to unauthorized parties may result in data breaches. It's important to recognize that there are numerous ways in which privacy and security can be compromised, including the inevitable systemic identification that occurs through electronic health infrastructure and technology. Moreover, the government, healthcare providers, pharmaceutical companies, and laboratories might need access to patient health records; all of these entities run the risk of unintentionally or intentionally breaching data security and privacy [4].

Safeguarding data against unwanted access during transmission, storage, and patient care is all part of maintaining confidentiality. Password-controlled system access and data encryption are two ways to achieve confidentiality. A privacy concern is confidentiality, which makes sure that medical records are shielded from unwanted additions or deletions [13]. Data availability, which describes the capacity of an authorized user to access a system and perform all system functions, including accessing all required information at all times, is another crucial phrase in EHR data security and privacy. Because they help patients have faith in their physicians' ability to make decisions, electronic health records' privacy and security are essential [14]. Patients are more likely to divulge information to their clinicians when they feel that the electronic health information they have access to is accurate and private [14]. Because of this transparency, medical professionals can obtain all the data they need to comprehend a patient's general health and make better judgments [15]. On the other hand, if patients feel that the confidentiality and privacy of their information is being jeopardized, they can refuse to provide information or postpone getting treatment [16]. Many patients have serious concerns about the security of their medical data because they fear that a hospital may lose their trust if confidential patient information is compromised [17].

A federal statute known as HIPAA protects patient health information across the country by prohibiting its disclosure to other parties without the patient's permission. HIPAA comprises national guidelines for the protection of electronic Protected Health Information (ePHI) and a Privacy Rule that safeguards patient-identifiable health information [17]. The law also mandates that covered businesses and business affiliates notify patients in the case of a security breach. This is known as the breach notification regulation. HIPAA's regulations regarding security, privacy, and breach notification must be followed by healthcare providers. A past, present, or future payment for healthcare services; the provision of treatment; demographic information pertaining to a mental or physical health condition; and other individually identifiable health information, such as medical records, laboratory results, or hospital bills, are among the details covered by HIPAA [18]. Health plans, healthcare clearinghouses, and healthcare providers who conduct routine transactions electronically are among the entities obligated to adhere to HIPAA regulations.

*Vulnerabilities of HER:*

*The Increasing Prowess of Attackers:*

The risk of unauthorized access to information by third parties is becoming more sophisticated and dangerous. Cyber-attacks are on the rise, increasingly evasive, and almost undetectable **[18]**. The tactics and intentions of attackers are evolving, shifting from seeking fame to pursuing financial gains. This means attackers are now more interested in stealing identities and banking or credit information from EHRs for financial profit. A concerning trend in cyberattacks involving EHRs is the use of evasive technologies by hackers, which makes detecting security breaches challenging. With these technologies, hackers can execute attacks to their fullest extent, causing maximum damage. Additionally, the expansion of vendors' cloud-based services likely means an increase in cyberattacks **[19]**.

*The Increasing Use of "Off-the-Shelf" Software Options:*

As the use of EHRs grows, there is a higher demand for ready-made EHR systems by healthcare providers. To meet this demand, vendors are increasingly using off-the-shelf operating systems such as Windows, Linux, Unix, and similar third-party software. Vockley notes that medical devices such as patient monitors, MRI scanners, X-ray machines, and similar equipment commonly used in healthcare delivery share many interface similarities, resembling regular desktops and laptops **[20]**. This is because they use the same operating systems that are vulnerable to the same attacks. Consequently, all devices using these operating systems can be infected with the same viruses, increasing the scope of security risks. The rise in networked medical equipment and devices means that a security breach, such as hacking, can slow down network traffic and interfere with healthcare service delivery. Additionally, the use of mobile devices to access patient health information complicates security issues **[20]**. The risk of patient or user harm in the case of a security breach often depends on the type of hazard. For instance, medical devices accessing real-time patient data through a network are more vulnerable to network disruptions.

Using off-the-shelf items increases the risk of unintentional harm from security breaches. Software patches and upgrades are frequently applied to commercial operating systems, browsers, and databases to guard against the most recent malware and security flaws. While companies and people can immediately install these upgrades and get back to work, producers of medical technology are required to go through an FDA approval process before recommending these changes to their clients. This guarantees that the security and operation of the health databases and EHRs are not compromised by the upgrades **[21]**. EHRs are therefore more susceptible to attacks since the operating systems and other software that enable them frequently lag behind in terms of security. When a security lapse occurs, this vulnerability may permit unauthorized access by someone with bad intentions. Malware can enter healthcare systems through a number of channels, such as shared networks on desktops, mobile devices, and laptops. Medical equipment that is vulnerable to malware can readily become infected with viruses, which has the ability to completely shut down a hospital's operating system. Software defects and viruses, according to Bowman, can jumble data, erase information, or put it in the wrong place, all of which can affect data integrity **[3]**. Service delivery may be disrupted by doctors finding vital patient information slowly due to disorganized data.

*Unintended Consequences:*

Unintended consequences are another source of security concerns regarding EHRs. Graber et al. highlight that system design issues such as software design flaws, routing of electronic data, system malfunctions, and integration problems pose significant threats to the security of EHRs and can adversely affect patient health outcomes **[1]**. For instance, a system malfunction that prevents a healthcare provider from accessing patient radiology studies or delays the upload of pathology reports of adenocarcinoma can threaten patient outcomes. These examples illustrate how safety and security can be compromised when a component of the EHR system malfunctions **[21]**.

*Information Sharing Concerns:*

Security breaches may also occur unintentionally when clinicians share information. Harman et al. report that approximately 73% of physicians text other physicians about patient interactions and care practices **[22]**. Securing such information is challenging since there is no control over what is shared via texting or whether third parties can intercept this information. Mobile phones, designed for individual use, often lack the security features of desktops that are part of an organization's network. Additionally, mobile phones can be easily misplaced or stolen, allowing third parties to access protected information.

*Impacts of Data Security Breaches:*

Data security breaches can have significant financial and organizational repercussions, affecting individual hospitals, providers, business associates, and patients. These breaches threaten the entire healthcare industry and undermine the success of EHRs **[23]**. Common causes of security breaches involving health records databases include the loss of unencrypted laptops and mobile phones containing patient health information. Chenthara et al. note that cyberattacks, such as ransomware, have impacts that extend beyond financial loss and privacy breaches. For example, when hackers accessed the Community Health Systems (CHS) database, they retrieved personal information, including the social security numbers of up to a million patients. There is also an incident where Anonymous, an internet vigilante group, launched a Distributed Denial-of-Service (DDoS) attack on several hospital websites, crippling medical services [24]. To prevent such attacks, healthcare providers must implement adequate safeguards in their electronic databases.

*Recommendations for Reducing the Security Risks of Electronic Health Records:*

To ensure the security of health records databases, healthcare providers should implement physical, technical, and administrative strategies. According to Keshta and Odeh [4], administrative safeguards include performing system audits, appointing an officer in charge of information technology, and developing contingency plans in case of a breach. Administrative safeguards are crucial as they establish security procedures and policies that guide the use of information technology, thereby enhancing the security of EHRs. Physical safeguards involve protecting health information physically to prevent unauthorized access to software and hardware [25]. Examples of physical safeguards include setting security roles and securing places where servers are stored.

Technical safeguards are aimed at protecting the information systems and networks of a healthcare institution. Compared to physical and administrative safeguards, technical safeguards are vital because most security breaches occur through electronic media such as computers and mobile phones [25]. Common technical safeguards include firewalls, data encryption, antivirus software, and cloud computing. Implementing physical, administrative, and technical safeguards together can enhance the security of health records databases. Physical safeguards, such as restricting physical access to servers and installing security cameras, can prevent theft. Technical safeguards, like firewalls and encryption, can prevent electronic breaches even if physical safeguards are compromised [4]. Administrative safeguards, such as comprehensive education, security plans, and appointing a chief information security officer, can improve the overall security of EHR systems and databases. Additionally, administrative measures like requiring manager approval for data release and training employees on handling missing data can further bolster the security of health records databases.

To enhance the security of electronic health records (EHR) databases, healthcare providers should implement a combination of physical, technical, and administrative strategies.

*1- Physical Safeguards:*

Physical safeguards involve protecting the physical aspects of EHR systems to prevent unauthorized access to hardware and software [25]. This can include secure storage for servers, restricted access areas, and surveillance systems.

*2- Technical Safeguards:*

*Technical safeguards are crucial for protecting the information systems and networks of healthcare institutions. These include:*

- Firewalls: Essential for blocking unauthorized access and protecting the organization's network.
- Data Encryption: Ensures that data is unreadable to unauthorized users.
- Antivirus Software: Protects against malware and other malicious software.
- Cloud Computing: Provides secure data storage and access management [25].

Specific recommendations include the use of level gateway firewalls, which act as gatekeepers to the organization's network, preventing unauthorized external access. Network address translators (NAT) can also be used to hide intranet IP addresses, creating a barrier for external users. Implementing these technologies requires a thorough needs assessment, threat assessment, and budgetary planning to identify the best options [27].

Firefox has been recommended as an effective tool for securing an organization's network, ensuring comprehensive protection both inside and outside the network [4].

*3- Administrative Safeguards:*

Administrative safeguards focus on policies and procedures that govern the use of information technology within healthcare organizations. These include:

- System Audits: Regularly reviewing and assessing the security measures in place.
- Information Technology Officer: Appointing a dedicated individual to oversee IT security.
- Contingency Plans: Developing plans for responding to security breaches [4].
- Education and Training: Comprehensive training for employees on handling EHRs and understanding security protocols.
- Policies for Data Release: Requiring manager approval for data release and ensuring accurate patient identification during system shutdowns [26].

*4- Duplication and Backup Strategies:*

Collier [26] recommends duplicating all critical hardware to enhance the security of electronic health databases. Backup generators should be in place to support electronic systems during power outages, ensuring continuous access to patient records and preventing downtime. Comprehensive testing and monitoring strategies are essential to ensure the availability of patient records when needed. In the event of a system shutdown, having paper records as a backup and effective communication systems that do not rely on electronic systems are crucial. By implementing these physical, technical, and administrative safeguards, healthcare providers can significantly enhance the security of EHR systems and protect patient data from unauthorized access and cyber threats.

### *5- Cryptography as a Strategy for Securing EHRs:*

One approach to securing electronic health records (EHRs) is through cryptography or encryption. This technique involves encoding data to ensure the protection of health records during information exchange. Cryptography is a method of covert writing that establishes protocols to prevent unauthorized individuals from reading confidential messages **[28]**. The exchange of health information must adhere to specific policies and specifications, with all exchanges being documented when encryption is activated or deactivated. HIPAA provides guidelines on using encryption to secure health information, particularly during the creation, receipt, storage, and sharing of such information. For example, digital signatures can mitigate the risk of breaches when patients access their health information. However, the unfamiliarity with digital signatures among many people results in their underutilization **[29]**. The use of usernames and passwords also constitutes a form of cryptography. Users are advised to frequently update passwords and avoid using easily guessable names and birthdates to reduce the likelihood of password breaches **[30]**. Nonetheless, this method does not protect against internal threats. Therefore, employees should log out after completing procedures to prevent unauthorized access to patient information. Additionally, employees must refrain from sharing their identification (ID) with others and always log off when leaving a computer unattended **[31]**.

### *Conclusion:*

The transition from paper to electronic health records (EHRs) in the United States, driven by the widespread use of technology and legislative initiatives like the ARRA/HITECH Act, has revolutionized healthcare delivery. EHRs offer numerous advantages, including improved healthcare quality, reduced costs, enhanced information sharing, and support for evidence-based practices. However, this transition also introduces significant challenges, particularly concerning the privacy, security, and confidentiality of patient information. One of the critical aspects of securing EHRs involves adhering to the guidelines established by the Health Insurance Portability and Accountability Act (HIPAA), which sets national standards for the protection of electronic Protected Health Information (ePHI). Despite these regulations, the increasing sophistication of cyber-attacks poses substantial risks, with attackers often motivated by financial gains. The use of off-the-shelf software in medical devices exacerbates these risks, as these systems may lag in security updates, making them vulnerable to malware and other security breaches.

Moreover, unintended consequences arising from system design flaws, such as software malfunctions and integration issues, can adversely affect patient outcomes. Information sharing among clinicians, particularly through unsecured means like texting, further complicates the security landscape, increasing the likelihood of data breaches. To mitigate these risks, healthcare providers must implement a comprehensive strategy encompassing physical, technical, and administrative safeguards. Physical safeguards include secure storage and restricted access to hardware, while technical safeguards such as firewalls, encryption, and antivirus software protect against electronic threats. Administrative measures, including regular system audits, staff training, and the appointment of dedicated IT security officers, are essential for maintaining robust security protocols. Cryptography, particularly through data encryption and digital signatures, plays a pivotal role in safeguarding health information. However, to be effective, these measures must be widely understood and utilized. Additionally, the frequent updating of passwords and stringent access control practices are necessary to prevent unauthorized access, both from external threats and internal negligence. In conclusion, the effective security of EHRs requires a multifaceted approach that integrates physical, technical, and administrative safeguards. By addressing the evolving nature of cyber threats and ensuring strict adherence to HIPAA guidelines, healthcare providers can protect patient information and maintain the integrity and trustworthiness of their healthcare systems.

## References

1- GRABER M.L., SIEGAL D., RIAH H., JOHNSTON D. and KENYON K.: Electronic health record-related events in medical malpractice claims. J Patient Saf., 15: 77-85, 2019. 10.1097/PTS.0000000000000240.

2- BOWMAN S.: Impact of electronic health record systems on information integrity: quality and safety implications. Perspect Health Inf Manag., 10: 1c, 2013.

3- KESHTA I. and ODEH A.: Security and privacy of electronic health records: concerns and challenges. Egypt Inform J., 22: 177-83, 2021. 10.1016/j.eij.2020.07.003

4- SHER M.L., TALLEY P.C., YANG C.W. and KUO K.M.: Compliance with electronic medical records privacy policy: an empirical investigation of hospital information technology staff. Inquiry, 54: 0046958017711759.10.1177/0046958017711759, 2017.

5- WIKINA S.B.: What caused the breach? An examination of use of information technology and health data breaches. Perspect Health Inf Manag., 11: 1h, 2014.

6- AYATOLLAHI H., MIRANI N. and HAGHANI H.: Electronic health records: what are the most important barriers?. Perspect Health Inf Manag., 11: 1c, 2014.

7- MCBRIDE S., TIETZE M., ROBICHAUX C., STOKES L. and WEBER E.: Identifying and addressing ethical issues with use of electronic health records. Online J Issues Nurs., 23: 10.3912/OJIN.Vol23No01Man05, 2018.

8- DE RUITER H.P., LIASCHENKO J. and ANGUS J.: Problems with the electronic health record. Nurs Philos., 17: 49-58, 2016. 10.1111/nup.12112

9- What is the HITECH Act?. (2018). Accessed: September 15, 2022: https://www.hipaajournal.com/what-isthe-hitech-act/.

10- COLICCHIO T.K., CIMINO J.J. and DEL FIOL G.: Unintended consequences of nationwide electronic health record adoption: Challenges and opportunities in the post-meaningful use era. J Med Internet Res., 21: e13313.10.2196/13313, 2019.

11- SEIEDFARAJOLLAH S., SAFDARI R., GHAZISAEEDI M. and KEIKHA L.: Key security and privacy issues from implementing the National Electronic Health Record in the Islamic Republic of Iran. East Mediterr Health J., 25: 656-9, 2019. 10.26719/emhj.19.006.

12- AL-ISSA Y., OTTOM M.A. and TAMRAWI A.: eHealth cloud security challenges: a survey . J Healthc Eng., 2019: 7516035, 2019. 10.1155/2019/7516035.

13- HASSAN M., BUTT M.A. and ZAMAN M.: Privacy protection and security challenges in electronic healthcare records . Int J Adv Res Sci Engg., 7: 1525-34, 2018.

14- KISEKKA V. and GIBONEY J.: The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. J Med Internet Res., 20, 2018.

15- HealthIT.gov. Guide to privacy and security of electronic health information. The office of the national coordinator for health information technology. (2015). Accessed: September 15, 2022: https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

16- PAPOUTSI C., REED J.E., MARSTON C., LEWIS R., MAJEED A. and 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., 15: 86, 2015. 10.1186/s12911-015-0202-2.

17- GARIÉPY-SAPER K. and DECARIE N.: Privacy of electronic health records: A review of the literature. J Can Health Libr Assoc., 42: 74-84, 2021. 10.29173/jchla29496.

18- VOCKLEY M.: Safe and secure? Healthcare in the cyberworld. Biomed Instrum Technol., 46: 164-73, 2012. 10.2345/0899-8205-46.3.164.

19- LIU V., MUSEN M.A. and CHOU T.: Data breaches of protected health information in the United States. JAMA, 313: 1471-3, 2015. 10.1001/jama.2015.2252.

20- ACHAMPONG E.K.: Electronic health record (EHR) and cloud security: The current issues . Int J Cloud Comput Serv Sci., 2: 417-20, 2013.

21- SITTIG D.F. and SINGH H.: Electronic health records and national patient-safety goals. N Engl J Med., 367: 1854-60, 2012. 10.1056/NEJMsb1205420.

22- HARMAN L.B., FLITE C.A. and BOND K.: Electronic health records: privacy, confidentiality, and security . Virtual Mentor., 14: 712-9, 2012. 10.1001/virtualmentor.2012.14.9.stas1-1209.

23- COLLIER R: New tools to improve safety of electronic health records . CMAJ, 186: 251, 2014. 10.1503/cmaj.109-4715.

24- CHENTHARA S., AHMED K., WANG H. and WHITTAKER F.: Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access., 7: 74361-82, 2019. 10.1109/ACCESS.2019.2919982.

25- TEJERO A. and DE LA TORRE I.: Advances and current state of the security and privacy in electronic health records: Survey from a social perspective. J Med Syst., 36: 3019-27, 2012, . 10.1007/s10916-011-9779-x.

26- COLLIER R.: US health information breaches up 137%. CMAJ, 186: 412, 2014. 10.1503/cmaj.109-4731.

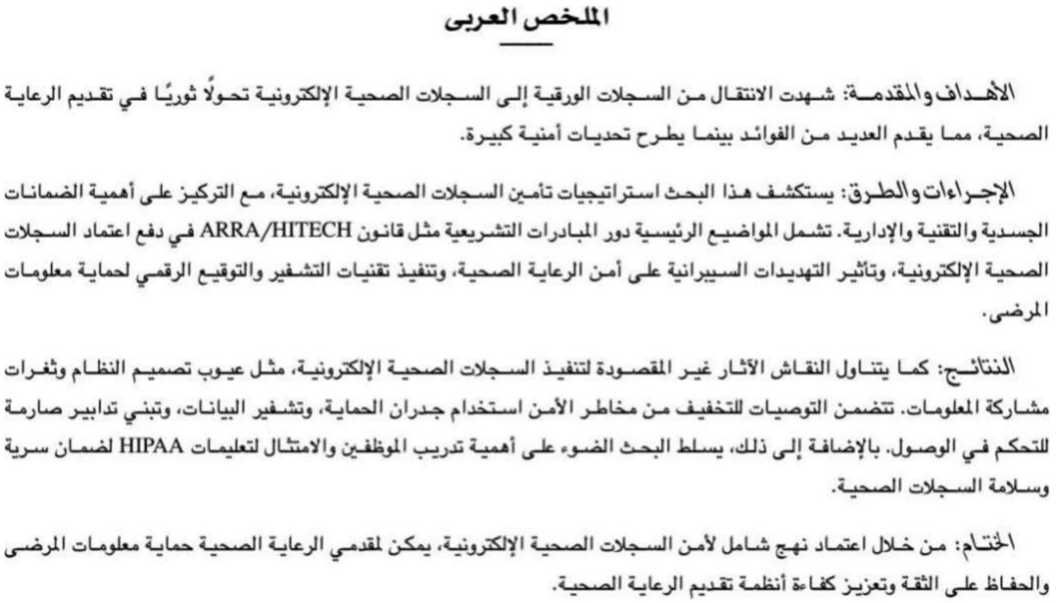
27- KRUSE C.S., SMITH B., VANDERLINDEN H. and NEALAND A.: Security techniques for the electronic health records . J Med Syst., 41: 127, 2017. 10.1007/s10916-017-0778-4.

28. CHENTHARA S., AHMED K., WANG H., WHITTAKER F. and CHEN Z.: Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS One, 15: e0243043, 2020. 10.1371/journal.pone.0243043.

29- ALAQRA A.S., FISCHER-HÜBNER S. and FRAMNER E.: Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: qualitative study of perspectives by medical professionals and patients. J Med Internet Res., 20: e10954, 2018. 10.2196/10954.

30- U.S. Department of Health and Human Services. Cybersecurity: 10 best practices for the small healthcare environment. (2010). Accessed: September 15, 2022: https://www.healthit.gov/sites/default/files/basicsecurity-for-the-small-healthcare-practice-checklists.pdf.

31- OZAIR F.F., JAMSHED N., SHARMA A. and AGGARWAL P.: Ethical issues in electronic health records: A general overview . Perspect Clin Res., 6: 73-6, 2015. 10.4103/2229-3485.153997.



## الملخص العربى

**الأهــداف والمقدمــة:** شـهدت الانتقـال مـن السـجلات الورقيـة إلـى السـجلات الصحيـة الإلكترونيـة تحـولًا ثوريًـا فـي تقـديم الرعايـة الصحيـة، ممـا يقـدم العديـد مـن الفوائـد بينمـا يطـرح تحديـات أمنيـة كبيـرة.

**الإجـراءات والطـرق:** يستكشـف هـذا البحـث اسـتراتيجيات تأمـين السـجلات الصحيـة الإلكترونيـة، مـع التركيـز علـى أهميـة الضمانـات الجسـدية والتقنيـة والإداريـة. تشـمل المواضيـع الرئيسـية دور المبـادرات التشـريعية مثـل قانـون ARRA/HITECH فـي دفـع اعتمـاد السـجلات الصحيـة الإلكترونيـة، وتأثيـر التهديـدات السـيبرانية علـى أمـن الرعايـة الصحيـة، وتنفيـذ تقنيـات التشـفير والتوقيـع الرقمـي لحمايـة معلومـات المرضـى.

**النتائــج:** كمـا يتنـاول النقـاش الآثـار غيـر المقصـودة لتنفيـذ السـجلات الصحيـة الإلكترونيـة، مثـل عيـوب تصميـم النظـام وثغـرات مشـاركة المعلومـات. تتضمـن التوصيـات للتخفيـف مـن مخاطـر الأمـن اسـتخدام جـدران الحمايـة، وتشـفير البيانـات، وتبنـي تدابيـر صارمـة للتحكـم فـي الوصـول. بالإضافـة إلـى ذلـك، يسـلط البحـث الضـوء علـى أهميـة تدريـب الموظفـين والامتثـال لتعليمـات HIPAA لضمـان سـرية وسـلامة السـجلات الصحيـة.

**الختـام:** مـن خـلال اعتمـاد نهـج شـامل لأمـن السـجلات الصحيـة الإلكترونيـة، يمكـن لمقدمـي الرعايـة الصحيـة حمايـة معلومـات المرضـى والحفـاظ علـى الثقـة وتعزيـز كفـاءة أنظمـة تقديـم الرعايـة الصحيـة.