How to Cite:
Alsanad, I. S., Aldarbi, S. A., Aljohani, M. A., Alhejaili, M. A. M., Aldhahri, A. M., & Alarfi, M. D. M. (2023). Data security challenges in medical records: A comparative analysis of digital and paper systems. *International Journal of Health Sciences*, *7*(S1), 3813–3828. https://doi.org/10.53730/ijhs.v7nS1.15402

Data security challenges in medical records: A comparative analysis of digital and paper systems

Ibrahim Saud Alsanad
Ministry of National Guard Health Affairs

Salman Anber Aldarbi
Ministry of National Guard Health Affairs

Mohammed Abdulrahman Aljohani
Ministry of National Guard Health Affairs

Mazen Ayidh Muawwadh Alhejaili
Ministry of National Guard Health Affairs

Abdullah Mohammed Aldhahri
Ministry of National Guard Health Affairs

Mobarak Dakhelallah Meateq Alarfi
Ministry of National Guard Health Affairs

***Abstract*---Background**: This has become very important since health care is moving from paper-based systems to electronic systems. Each of them is exposed to various risks such as cyberrisks and physical losses which makes the issue of data security rather acute. **Aim**: The purpose of this work is to define the major issues related to the protection of the patient records and discover the differences in the risks associated with the digital and paper record management in healthcare organizations. **Methods**: A literature review and was done to compare the risks of using digital and paper medical record systems, with emphasis on data breaches, regulation, and security measures in the case studies. **Results**: The major drawbacks of the paperless systems include attacks on the digital records and system Compromised data on the other hand has high risks of being stolen, ripped, lost among other catastrophes. Both systems fail in compliance matters, as well as in sharing data securely. **Conclusion**: Medical facility data safeguarding is about both the paper and digital sides that are addressed by encryption, compliance with the law, or

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

staff education. Continual adaptation has been regarded as a key to successful protection of patient data.

***Keywords*---**Electronic health record, documentation, electronic systems, paper based systems, leakage of health information, security.

Introduction

Data security however has emerged as an even bigger issue in the healthcare industry, especially when the management of records, especially medical records is slowly shifting to more complex technology applications. As a result of recent changes in health care information technology moving from paper based systems, health care organizations are confronted with unprecedented challenges in protecting their patients' personal information from various risks. Electronical medical records are used for the delivery of health services, and at the same time they contain personal data, medical data, and even financial data that are attractive to cyber criminals. Guarding these records calls for handling of multiple and multiple layers of security risks including cyber security risks**.**, element large risks from insiders, supportive compliance, data encryption, and controlling third-party vendors. The idea that skirmish remains a prospective threat for health-care organizations is prime to maintaining an ethnical cognizance to strategic security, as organizations strive to manage merging healthcare systems and quantities of data. In this work, the major issues affecting the security of medical records as well as the impacts that are caused by technology and paper works have been discussed, and probable solutions for these impacts have also been provided.[1,2]

Learning about Data Security in Healthcare

Information management in health care refers to the security of data in today's practices for health affairs, this is under the facility that patient's information must be secure, updated and accessible only to the appropriate personnel. Under the healthcare industry there is a huge amount of data that contains personal records of individuals, diagnostic information, and financial data. This information is extremely important when it comes to delivering excellent quality of care, minimizing bureaucratic work and when carrying out investigations. But it also makes the healthcare industry a favorite among hackers to test their skills and for unauthorized access to sensitive data. Concatenating this information is not only an IT issue but also a legal and an ethical one as well. A violation of patient information can lead to so many losses, penalties, and already weakened trust of patients to doctors. Consequently, analyzing the concept of data security in this regard involves identification of the type of threats, mechanisms for preparing to address threats, security measures to put into place, the lessons to learn, and measures to adopt.[3,4] From experience, caretakers in healthcare organizations are in a peculiar position in ensuring data security, given the kind of organizations they work for. Patient data is sometimes located within Enterprise Information System (EIS), which include EHR and Patient Administration Systems (PAS), on mobile and cloud applications and even in paper records. The present advance in healthcare technology qua digitization has created increases in efficiency and access but with new risks. Risk of cyber attack including ransomware, phishing scams and data loss incidents have also escalated and become newer and more complex. In addition to violating the patient's right to privacy, these attacks can immune crucial healthcare delivery. However, physical threats within the same level which include loss or theft of paper-base files are also real threats. The problem of ensuring data availability while trying to enforce a fairly tight level of security is not easy and needs to be addressed constantly and flexibly.[5,6]

It is noteworthy that the strategy of utilizing data protection regulation as a dominant pattern of response is initiated by various regulatory authorities across the world as a crucial component of the solution. Current legal regulations such as Health Insurance Portability and Accountability Act (HIPAA) in USA and General Data Protection Regulation (GDPR) in European Union set rules and put into place punitive measures on data utilizing organizations. These regulations place stress on an organization to have a security policy in place and enforce it, conduct security audits, and continuously educate employees on the issues of data security. But, don't be confused, compliance alone is not enough. Today's cyber threats are rapidly developing, and they require organizations to implement measures, like encryption, two-factor authentication, constant monitoring of systems and etc. In addition to this, there is the need to create a security awareness culture in the healthcare organizations where user at all levels will be in a position to understand their responsibilities towards patients' information security.[7]data security in healthcare cannot be perceived as a single component part, more about technology, rules, or people, it's about all of these combined. In the future, growing of the industry it is evident that security of patient's information is a crucial factor. Besides, protection of individual data and privacy is very important and it improves the level of confidence as well as functionality of healthcare sectors. By identifying the key and significant issues, which are found in the model, healthcare organizations can improve their ability to mitigate current threats and to cope with potential future threats.[8,9]

The Protection of Patient Records in the Line of Lyme Disease

Protecting patients' medical data is one of the crucial concerns of contemporary healthcare organizations because such data is extremely personal. Medical records contain nearly every type of data that an individual may provide to the health care provider – from identity numbers or names to the medical history, diagnostic test results, patient's and physician's future plans, and even the patient's financial information. Although EHR data are unlikely to be manipulated, the integration, confidentiality, and availability of this data are vital to the improvement of patient care and to the development of trust with patients. If this information falls into the wrong hands, those people who depend on these records for diagnosis can be misdiagnosed, fraudsters can defraud such individuals, or someone's identity can be stolen. Therefore, medical record protectionism is as much an operational imperative as it is a moral and regulatory requirement for care organizations.[10,11]This means that data protection carries with it an emphasis not necessarily only on the needs of the patient, but also on the healthcare organization as a whole. Medical records help in advancement of continuity of care and avoid repetition of history by providing secure, advance, and accurate records for the healthcare providers to share.. For example, a treating physician when having a chronic illness depends on the accuracy of the records of past treatment to formulate the next course of action. The problem circumventing these breaches or loss would disrupt this continuum in a manner capable of compromising the patient's health. Moreover, the increase in the usage of EHRs and telemedicine platforms increased the necessity for protection of data. New technologies help to increase availability and productivity but bring new threats – hackers, intruders, etc. The present day health care organizations must pay close attention to the security of their data in order to safeguard both the interest of the patients as well as the health care entity itself. [12,13]

Laws and regulations emphasize securing medical records and establish very high protection requirements. HIPAA for example in the United States requires that all healthcare providers should ensure that their patients' information is protected from such things as hacking and theft. Similarly, across the European Union, medical information is considered personal information that is now protected under the General Data Protection Regulation. Violation of these regulations is liable to attract severe penalties, loss of reputation, and patient trust. In addition to meeting the legal and wholesome standards of care, patients' data also deserve moral protection. People go to health care workers with their bodies wide open, naked in a sense, with the assumption of trust being there that personal information that they reveal will not be disclosed to others or used inappropriately. Such violation has potential severe negative effects, not only for the deceived persons, but also for the very idea of healthcare in society.[14]

Confidentiality of patients' records is important not only for clinical medical inventory but also for future surveys and investigations. identified patient information is commonly appropriate for use in medical research, epidemiological investigations, and legislation formulation. Protecting this data, ensures that it is not used by other unauthorized parties and thus increases the faith of the public in such programs. For instance, throughout global health emergencies such as the emerging coronavirus illness (COVID 19), accurate and contained records offered useful information on the affected population to inform the interventions necessary in containing the illness. Any undo exposure of data could have negatively impacted on these efforts, with potential dire consequences to public health.[15,16]it can be realized that protection of medical records is a critical concern that should receive a lot of attention. That is why ensuring the patient anonymity, the overall quality and the ethical standards of health care organizations are of great significance. Given the fact that the amount of medical data is increasing year by year as well as their variability, it is crucial for health care organizations to apply the increased levels of security and engage their personnel in data safety. In this way, they can ensure confidentiality about each patient but also other's information and confidence, and efficiency of the whole healthcare system.[17,18]

Digital Systems: Redding the Error But Increasing Efficiency

In this paper, we will discuss how the advance use of technology in healthcare has transformed one of the most important areas that is recording some of the best reform in efficiency, accessibility and information management. With EHRs, those in the telemedicine platforms, and the availability of cloud storage solutions, the path through which patient data flows has become much more efficient, hence improving the decision-making process since all the parties in a patient's medical decision-making process have access to the data. This makes it possible to note changes in real time and not only different physicians providing care to a patient to have information from the patient's record updated by other providers no matter the geographical location. Furthermore, population health management has been enhanced through the use of digital tools as it answers questions regarding population based on Big Data which includes trend identification, risk assessment as well as determination of optimum solution to be taken in order to address the area's health challenges. However, the replacement of original paper-based systems with digital ones has led to the appearance of numerous additional threats and susceptibilities, creating the problem of data protection, which plays an important role in healthcare organizations.[19,20] Cyber risk is one of the most well-known risks related to the implementation of digital systems. New Account Data Healthcare data has always been a commodity that's hot property at the black market since it tends to combine details that are personal, medical, and financial. This makes healthcare organizations sit as easy targets for hackers who use different tactics like ransomware, phishing, and malware to penetrate health organizations security. An example of this is ransom ware which holds essential health records hostage through encryption until the attacker receives a ransom. The working and the financial costs of such attacks are high; it is not only the overview of the provision of immediate care but also the organization's reputation which becomes questionable. Also, violation of digital systems may pose patients to risk and identity theft, fraudsters, which is why health facilities deserve effective cybersecurity systems.[21,22]

Digital systems have their own problems that arise from user error and system susceptibilities. Holders of paper-based systems know how easy it is to coordinate and manage them, but with digital systems, they know that constant updating is essential for security and functioning. Misconfigured servers, aged software, and feeble passwords can provide entry points for use by hackers to access the systems. Individual mistakes for instance communicating wrong data to the wrong person or even not logging off an account correctly also results to leakage. Moreover, acquisitions of other firms or third-party vendors using digital interfaces cause additional application-to-application connections, which make protection of the whole chain challenging. Coordination of the implementation of these standards for every participant of the supply chain is not an easy process, but without it, all these risks have to be faced routinely.[23,24]However, there are some difficulties in realizing the usage of digital systems to improve the data security as follows In spite of these challenges digital systems have certain advantages if effectively used. Additionally practices like encryption, use of multiple authentication factors as well as block chain that enhances security to higher levels will make it hard for the intruders to get access to the information. Another way to lower exposure to user error is to enhance security for personnel including employees dealing with cyber issues by conducting periodic security sensitization for healthcare staff. Also, digital systems provide enhanced ability to control and audit data access in real-time which help the healthcare organizations to prevent and identify breaches faster in future. As is evident in the advanced adoption of various technologies and practices, health care organizations reap maximum from the systematic systems without facing many challenges.[25]

Altogether, it can be concluded that digital systems facilitated the enhancement of performance and capabilities of healthcare management, though they obviate certain critical risks. These systems are easy to use and offer great functionality, however they pose a major threat to patients' data and privacy which must be well guarded. Due to these risks, healthcare organizations have to ensure they put adequate measures of cybersecurity, train employees on them, and always conduct vulnerability assessments. With this way, they will be able to achieve optimal usage of digital systems in performing their functions to protect the trust and health of patients. [26,27]

Paper-Based Systems: Traditional Methods and Their Vulnerabilities

Manual paper based systems have traditionally dominated healthcare record management, providing concrete and recognizable means as to where patient information is stored. For several decades, doctors, nurses and other health care providers have been using hand written paper records, charts and folders for creating patient records, medical histories, diagnoses, prescriptions, and sometimes even emergency instructions. These traditional techniques offer healthcare professionals tangible forms of patient information that were very accessible in clinics and hospitals. In most regions of the globe and especially in those regions that have not embraced modern technology paper-based systems of work are still popular when it comes to managing medical records. Nonetheless, conventional paper-based systems are accompanied by numerous other drawbacks, which stem from pressing security issues, increasing errors, and decreasing medical records' accessibility.[28,29]The first weakness of paper based systems is that the paper may be misplaced, torn, or lost entirely. Papers lead to many issues such as fire outbreaks, floods, or any other natural disasters that are likely to destroy all medical documents. In healthcare settings, medical records are very important because patient information is very important to continued care of the patient, therefore, loss of medical records can cause one to suffer negative consequences such as misdiagnosis, delayed treatments among others or even probable medical errors among patients. Paper records on the other hand cannot be easily duplicated or replicated as with digital systems' backups stored in other physical locations. Moreover, hard copies take a lot of storage space and over time it becomes difficult organize or even manage high number of documents that may be in store. Paper records occupy the valuable space and resources of the hospitals, clinics or other health care centers; managing paper records will always impose certain amount of inefficiency that can be managed by employing effective paperless solution.

Comparative Analysis: Advantages and Disadvantages of Information Technology Paper and Electronic Documents

Electronic records system is one of the major revolutionary changes in health care facilities in the recent past and each of the system has its traditional and conventional merits and demerits. A comparison between using digital and paper-based systems to store medical records outlines the effects of both methods on healthcare service provision, productivity, safety and patients. Although digital formats offer immense and easy ways of storing, retrieving and sharing data in healthcare management, paper based records are still in use widely, especially in the developing countries. However, awareness of both systems' capabilities and vulnerabilities becomes important for healthcare organizations that are to choose between classic approaches and innovations.[28,29]

Some of the advantages of records in the category of Digital records include;

An important advantage of manuscript records is the ability to improve access and transfer of information in electronic format. Through the use of electronic systems including EHRs the providers gain access to patient data in a convenient way without regard to location hence increasing the convenience of care. General practitioners, specialists as well as other care givers in a particular healthcare facility may monitor the record of a patient in real time thus reducing chances of incorrect analysis and decision making. Records are also digital to ensure smooth transition and exchange of information such as health records of a patient transfer from one hospital to the other or from one clinician to another. This connectedness lowers the probability of the patient receiving care in silos and guarantees to any provider who seeks it, an all-encompassing view of the patient. [30,31]

The other major benefit of digital records is the flexibility that allows record creators to integrate new technologies into record keeping in a bid to improve security. The information kept in the digital systems can be encrypted, protected by password and can be preserved and easily retrieved unlike the paper records. Multi-factor authentication, user access control, and audit trails help the healthcare organization to identify exactly who is accessing patient's data and ensure that patient's data will not be accessed by unauthorized people. Also, digital systems are better from the standpoint of storage and retrieval of information. Compared to paper records which needs space and physical filing, and records are easily accessed digitally in secure databases or the cloud. It also cuts down on paperwork and frees up healthcare organizations' time and money for more important tasks patient care. [32,33]

Digital Records: Their Strengths and Weaknesses

Thus, there are also multiple issues concerned with the digital records, first of all, security issues and dependence on certain technologies. Some of the emerging risks that have been increasingly turning hostile towards healthcare organizations are: Healthcare data is considered to be of great value and is usually involves personal information, thereby has becomes a prime area where hackers use either ransomware, phishing or a data breach with an intention to steal or corrupt patient's data. As much as organizations try to implement sound security measures on the digital systems, no system can be said to be fully safe and a leakage is catastrophic. Furthermore, as digital systems networks grow sophisticated; healthcare organizations have to update software, maintain infrastructure as well as train staff on how to address security issues. This is a continuing requirement that can add pressure on the available resources, especially in institutions that have limited financial might or IT personnel.[34,35]

Advantages of Paper Based Records

As much as paper-based systems are inefficient in almost all aspects of record keeping, they have advantages that are hard to mimic in digital systems. There is a certain convenience and safety of paper charts, for example. Unlike the digital systems, paper records can be hindered by technical problems, but they can be accessed without electricity or other digital amenities. If the electronic records are hacked, or the system crashes, at least the patient's paper records can be used as a reference for managing the patient's condition. Furthermore, some patients and caretakers and even some healthcare providers may grasp the paper documents fully than the electronic documents in settings where the use of technology is not well enhanced. In some health facilities particularly in rural areas or developing world, paper based system still holds the day as they offer simple ways of handling patient's data with out compromising on the technology aspect.[36,37]

Pitfalls of Paper Records

Even so, paper records have considerable drawbacks that make them unsuitable for use in contemporary healthcare organizations. Another disadvantage that is often attributed to this kind of marketing is non scalability. Paper documentation occupies a lot of physical space and a lot of time and energy is used in the filing, sorting and retrieving. While healthcare organizations expand in size and collect more patients' records, paper-based processes become more and more cumbersome and ineffective. Trying to pull record of a single patient may take as short a time as minutes or as long as hours depending on the quantity of records in the large hospitals or clinics, say hundreds or thousands of files. This inefficiency make it difficult in the diagnosis and treatment of the disease hence affecting the patients. [38,39]Besides, paper based health records are subject to physical damage or loss due physical calamities such as fire, water, disasters among others. As many people know, the digital records can be copied and stored in different locations so it is possible to have a guarantee that they will be protected, however the paper records cannot be replicated in the same way. Also, there is a huge problem with the enforcement of security of paper based records. As we all know, paper files can be locked in cabinets or even locked in rooms where nobody can access them but then again theft is not an exception. Yet, paper records cannot identify who accessed the information, a situation that makes it hard to identify or investigate cases of a security breach .Accordingly, the advantages of both digital and paper systems are apparent, and which to use is dependent on the characteristics of a given healthcare organization. Digital records, despite the advantages of being more efficient, accessible and secure when managed properly, listed here below has its own disadvantage which is the risk of hacking into the system and a system breakdown. There are some advantages and disadvantages for using paper records to capture information within some healthcare centers as a type of computerized system: This paper puts emphasis in understanding the changing landscape within the healthcare systems and coming up with the appropriate means of managing the record keeping systems involved; whether it has to do with an integration of the paper based record keeping and the digital based record keeping or even adoption of the digital only record keeping systems. [38,39]

Main Problems of Ensuring Data Security of Medical Records

Protection of medical records is an essential issue in the healthcare because people's personal data can be vulnerable to various threats, including hacking. Since health records are now increasingly being stored and managed using technology, healthcare organizations encounter the following major tasks to keep this information secure. These challenges are further exacerbated by the healthcare setting, evolving and increasingly complex cyber threats, and the ever expanding amount of data produced and transferred in the field. Below are the key challenges that healthcare organizations must address to safeguard medical records:

- **Cybersecurity Threats and Hacking**

The fact that cybercrime is becoming increasingly prevalent in the US is one of the most significant trends currently facing medical records' data security. The Increased number of patients with their records also make healthcare facilities being at the frontline of hackers. Through hacking techniques like phishing, ransomware, and malware attacks, cybercriminals get unauthorized access to patient's personal data, steal it or lock it within the healthcare system for a ransom. The healthcare sector is the most affected due to the sensitivity of the patient information that includes;; their personal details, their medical records as well as their insurance details can easily be sold on the black market. Using number firewalls and other security measures in place, it has been found that threats are constantly evolving therefore the healthcare organizations have to be on the lookout on how they can strengthen their security measures. [40,41]

- **Insider Threats**

Besides the external threats that are usually hackers, there is another threat that is insiders threats. Anyone who has legitimate access to the medical records of their employer's clients can abuse the privilege, whether out of malice or through negligence. Others may be healthcare workers who may hack their patient's data out of curiosity, or due to revenge or for monetary benefit, a mistake like sending data to a wrong recipient, or failing to adhere to the recommended security measures. Medical records are accessed not only by practitioners, but by nurses, technicians and administrative workers and because of that, the task of controlling access becomes a challenge. To Address insider threats, healthcare organizations should ensure the following control: Access controls should be stringent; audits should be routinely done; and awareness should be created frequently among the staff.[42]

Meeting the regulatory requirement

It is noteworthy that the healthcare organizations are challenged by the strict requirements and mandatory guidelines governing patient's data, including the HIPAA in United States, and GDPR in the Europe. Such regulations require particular security solutions for protecting patients' information such as cryptographic, authorization, and risk management measures. Nonetheless, it remains difficult to meet these regulations as it relates to both the dynamic landscape in terms of regulation and cybersecurity threats. It is a challenge for healthcare organizations to monitor current legislation and policy while also maintaining security while enhancing work, productivity, and patient well-being. Penalties for non-compliance are severe, legal and financial, which means that protecting sensitive Information remains crucial.[43]

- **Data Encryption and Privacy**

Encryption is one of the most effective ways of safeguarding the records but when it comes to implementation, it is faced with some of the following; Data encryption makes it impossible for an unauthorized person to read any information about patients, while data masking makes information partly invisible and readable only by authorized personnel. But encryption keys should be properly managed and encryption should be implemented on all levels where an organization's medical records may be stored or transferred. This can be especially challenging at a time when patient data is handled by many healthcare organizations or third-party individuals. Also, data that is encrypted is still at risk if keys used to encrypt the data are intercepted, this shows that more solutions are needed to protect both data at rest and data in motion.[44]

By ensuring interoperability and data sharing, under this factor, there is the following:

The practice of sharing various medical records across different entities and area known as Interoperability brings with it various data security issues. Although interoperability enhances the quality of treatment and gives the healthcare concerned professional a broader perspective of the patient's medical history and current status, it raises the likelihood of losing such information to quacks or wrong hands. Electronic Health Record (HER) systems are commonly used to share data and can have interfaces that are incompatible with other systems or provide insufficient security to protect the privacy and confidentiality of shared data. Standards for electronic data exchange must be set in healthcare organizations, and the issue of integration should not have negative effects on protection of patient information.[45]

- **Data Backup and Disaster Recovery**

One of the biggest risks with using an electronic medical record system and patient data is that it can easily be lost or corrupted in case of a system failure, a cyber attack or a natural disaster. When clinical data are lost, through improper backup and disaster recovery procedures, patient care and their overall safety is greatly affected. Proposals to keep medical records have to call for frequent data backup and subsequent secure storage on local networks or in cloud environments. Also, disaster recovery solutions need to be developed to protect the accessibility of patient data in case of emergency and availability of data for patient care should be restored as soon as possible. Lack of good backup and recovery measures exposes healthcare providers to major operational and even reputational risks.[46]

- **Third-Party Vendor Risks**

Many healthcare organizations outsource business services, information management or any other IT support from third party vendors. Despite the fact that such vendors provide the utility and, in many cases, the knowledge to look after the data safely, they also contribute to raising the level of risk. If a vendor does not implement proper security measures or in case his company was hacked, the medical records of the healthcare organization is also at risk. All the third parties involved in handling the patients' information must meet security requirements and regulations before being contracted. This means that health care organizations should develop well defined agreement with their vendors outlining their data security concerns as well as regular review and assessment schedules. [47] Risk and vulnerability are complex issues in health care organizations and protecting patient data is an umbrella term that encompasses many different issues. From the outside cyber threats to inside threats, compliance to third party risks, the privacy of medical records requires much more than reactive measures.[48] To eliminate these risks, healthcare organizations require sound cybersecurity measures, continuing protection of data exchange processes, fulfilling regulations, and staff education. Since the use of technology progression will go on, it will be fine for healthcare service providers to come up with a new strategy in handling computer security threats and update their data security measures in order to protect patient records

Conclusion

The protection of MEDICAL RECORDS is an uphill task and continuous process in healthcare organizations due to the numerous threats from cyber criminals, insiders, regulations and high flow of patients data. This means that despite the numerous advantages that could come with implementing of the digital systems for storage of patient records and data, there are new risk factors which need to be countered through the implementation of security measures, data encryption and compliance to the existing regulations as well as secure transfer of data. On the other hand, paper based system which is not easily hacked is still subject to physical damage, theft and human error. While healthcare organizations remain in this position, they need to develop broad strategies that incorporate technologies that address those problems while also protecting data. Through staff awareness, technological implementation and adherence to high risk management standards on data security in healthcare organizations, patient' information is protected thus the credibility of medical records improved hence patient care in the healthcare system.

References

1. Teno, J. M., Price, R. A., & Makaroun, L. K. (2017). Challenges of measuring quality of community-based programs for seriously ill individuals and their families. *Health Affairs, 36*(7), 1227–1233. https://doi.org/10.1377/hlthaff.2017.0161
2. Thwin, T. T., & Vasupongayya, S. (2018). Blockchain-based secret-data sharing model for personal health record system. In *2018 5th International*

Conference on Advanced Informatics: Concepts, Theory and Applications (ICAICTA) (pp. 196–201). IEEE.

3. Urkude, S. V., Sharma, H., Kumar, S. U., & Urkude, V. R. (2021). Anatomy of blockchain: Implementation in healthcare. In *Blockchain Technology: Applications and Challenges* (pp. 51–76). Springer.
4. Venkateswaran, N., & Prabaharan, S. P. (2022). An efficient neuro deep learning intrusion detection system for mobile ad hoc networks. *EAI Endorsed Transactions on Scalable Information Systems, 9*(6), e27.
5. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy, and blockchain: A review. *SN Computer Science, 3*(2), 1–12.
6. Yin, J., Tang, M., Cao, J., You, M., Wang, H., & Alazab, M. (2022). Knowledge-driven cybersecurity intelligence: Software vulnerability coexploitation behavior discovery. *IEEE Transactions on Industrial Informatics, 19*(4), 5593–5601.
7. Zhang, L., Xu, J., Vijayakumar, P., Sharma, P. K., & Ghosh, U. (2022). Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare systems. *IEEE Transactions on Network Science and Engineering.*
8. Zhang, X., & Poslad, S. (2018). Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In *2018 IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE.
9. Kumar Panda, S., Jena, A. K., Swain, S. K., & Satapathy, S. C. (2021). *Blockchain technology applications and challenges*. Springer.
10. Patil, D. R., & Pattewar, T. M. (2022). Majority voting and feature selection-based network intrusion detection system. *EAI Endorsed Transactions on Scalable Information Systems, 9*(&), ееб-еб.
11. Peloquin, D., DiMain, M., Bierer, B., & Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics, 28*(6), 697–705.
12. Pountoukidou, A., Potamiti-Komi, M., Sarri, V., Papapanou, M., Routsi, E., Tsiatsiani, A. M., Vlahos, N., & Siristatidis, C. (2021). Management and prevention of COVID-19 in pregnancy and pandemic obstetric care: A review of current practices. *Healthcare, 9*(467).
13. Rezaribagha, F., Mu, Y., Susilo, W., & Win, K. T. (2017). Multi-authority security framework for scalable EHR systems. *International Journal of Medical Engineering and Informatics, 8*(4), 390–408.
14. Shahmoradi, L., Darrudi, A., Arji, G., & Farzaneh Nejad, A. (2017). Electronic health record implementation: A SWOT analysis. *Acta Medica Iranica, 55*(6), 642–649.
15. Shi, X., & Wu, X. (2017). An overview of human genetic privacy. *Annals of the New York Academy of Sciences, 1387*(1), 61–72.
16. Shore, A., Reddy, A., & Klein, C. (2022). A student-centered privacy model for responsible technology use. In *Higher education implications for teaching and learning during COVID-19* (pp. 81).
17. Solove, D. J., & Hartzog, W. (2022). Unifying privacy and data security.
18. Souza, J., Pimenta, D., Caballero, I., & Freitas, A. (2020). Measuring data credibility and medical coding: A case study using a nationwide Portuguese inpatient database. *Software Quality Journal, 28*(3), 1043–1061.

19. Sravani, M. M., & Durai, S. A. (2021). Attacks on cryptosystems implemented via VLSI: A review. *Journal of Information Security and Applications, 60*, 102861.
20. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications, 50*, 102407.
21. Kahetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41(10), 1027–1038.
22. Lahti, A. C., Wang, D., Pei, H., Baker, S., & Narayan, V. A. (2021). Clinical utility of wearable sensors and patient-reported surveys in patients with schizophrenia: Noninterventional, observational study. *JMIR Mental Health, 8*(8), e26234.
23. Lettieri, G. K., Tai, A. H., Hütter, A. R., Raszl, A. L. T., Moura, M., & Cintra, R. B. (2022). Medical confidentiality in the digital era: An analysis of physician-patient relations. Revista Bioetica, 29*, 814–824.
24. Li, T., Wang, H., He, D., & Yu, J. (2022). Blockchain-based privacy-preserving and rewarding private data sharing for IoT. IEEE Internet of Things Journal.
25. Ma, Y., Zhou, G., & Wang, S. (2019). WiFi sensing with channel state information: A survey. ACM Computing Surveys (CSUR), 52(3), 1–36.
26. Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, 251–279.
27. Mayer, A. H., Costa, C. A., & Righi, R. R. (2020). Electronic health records in a Blockchain: A systematic review. Health Informatics Journal, 26(2), 1273–1288.
28. McIntosh, T., Kayes, A. S. M., Chen, Y.-P. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. ACM Computing Surveys (CSUR), 54(9), 1–36.
29. Mesquita, R. C., & de Edwarda, I. (2020). Systematic literature review of My Health Record system. Asia Pacific Journal of Health Management, 15, 14–25.
30. MHMD. (2017). Initial list of main requirements, Deliverable 1.1. Retrieved from http://www.myhealthmydata.eu/wp-content/themes/Parallax-One/deliverables/D1.1_InitialList-of-Main-Requirements.pdf
31. MHMD. (2018). Shaping our future, Newsletter 01. Retrieved from http://www.myhealthmydata.eu/wp-content/uploads/2017/10/MHMD_newsletter_01DEF_WEB_pagdoppie_110718.pdf
32. Mohammadi, M., Larijani, B., Razavi, S. H. E., Fotouhi, A., Ghaderi, A., Madani, S. J., & Shafiei, M. N. (2018). Do patients know that physicians should be confidential? Study on patients' awareness of privacy and confidentiality. Journal of Medical Ethics and History of Medicine, 11.
33. Olla, P., Tan, J., Elliott, L., & Abuneeiz, M. (2022). Security and privacy issues. Digital Health Care: Perspectives, Applications, and Cases*, 105.
34. Enaizan, O., Zaidan, A. A., Alwi, N. H. M., Zaidan, B. B., & Alsalem, M. A. (2020). Electronic medical record systems: Decision support examination framework for individual, security, and privacy concerns using multi-perspective analysis. Health and Technology, 10(4), 795–822. https://doi.org/10.1007/s12553-019-00406-x

35. 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
36. Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges, and existing techniques for data security and privacy. Computers in Biology and Medicine, 129, 104130. https://doi.org/10.1016/j.compbiomed.2020.104130
37. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500. https://doi.org/10.1016/j.comnet.2021.108500
38. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Kim-Kwang. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97, 101966. https://doi.org/10.1016/j.cose.2020.101966
39. Shamshad, S., Mahmood, K., Kumari, S., & Chen, C.-M. (2020). A secure blockchain-based e-health records storage and sharing scheme. Journal of Information Security and Applications, 55, 102590. https://doi.org/10.1016/j.jisa.2020.102590
40. Mani, V., Manickam, P., Saleh Alghamdi, Y. A., & Ibrahim, O. (2021). Hyperledger healthchain: Patient-centric IPFS-based storage of health records. Electronics, 10*(23), 3003. https://doi.org/10.3390/electronics10233003
41. Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges, and functionalities. IEEE Access, 9, 12730–12749. https://doi.org/10.1109/ACCESS.2021.3052024
42. Albahri, O. S., et al. (2018). 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, 42(5), 80. https://doi.org/10.1007/s10916-018-0959-5
43. Al-Qaysi, Z. T., et al. (2018). A review of disability EEG-based wheelchair control system: Coherent taxonomy, open challenges, and recommendations. Computer Methods and Programs in Biomedicine, 164,221–237. https://doi.org/10.1016/j.cmpb.2018.07.011
44. Yas, Q. M., et al. (2018). A systematic review on smartphone skin cancer apps: Coherent taxonomy, motivations, open challenges and recommendations, and new research direction. Journal of Circuits, Systems, and Computers, 27(05), 1830003. https://doi.org/10.1142/S0218126618300037
45. Alsalem, M. A., et al. (2018). Systematic review of an automated multiclass detection and classification system for acute leukemia in terms of evaluation and benchmarking, open challenges, issues, and methodological aspects. Journal of Medical Systems, 42(11), 204. https://doi.org/10.1007/s10916-018-1055-6
46. Alsalem, M. A., et al. (2018). A review of the automated detection and classification of acute leukemia: Coherent taxonomy, datasets, validation and performance measurements, motivation, open challenges, and recommendations. Computer Methods and Programs in Biomedicine, 158, 93–112. https://doi.org/10.1016/j.cmpb.2018.02.015

47. Hamada, M., et al. (2018). A systematic review for human EEG brain signals-based emotion classification, feature extraction, brain condition, group comparison. Journal of Medical Systems, 42(9), 162. https://doi.org/10.1007/s10916-018-1014-2

48. Ali, A. H., et al. (2018). High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. Multimedia Tools and Applications, 77(23), 31487–31516. https://doi.org/10.1007/s11042-018-6083-9

تحديات أمان البيانات في السجلات الطبية: تحليل مقارن بين الأنظمة الرقمية والورقية

الملخص

الخلفية: أصبح موضوع أمان البيانات أكثر أهمية مع الانتقال في قطاع الرعاية الصحية من الأنظمة الورقية إلى الأنظمة الإلكترونية. كلا النظامين معرض لمخاطر مختلفة، مثل الهجمات الإلكترونية والخسائر المادية، مما يجعل مسألة أمان البيانات مشكلة ملحة.

الهدف: يهدف هذا العمل إلى تحديد القضايا الرئيسية المتعلقة بحماية سجلات المرضى واستكشاف الفروقات في المخاطر المرتبطة بإدارة السجلات الرقمية والورقية في المؤسسات الصحية.

المنهجية: تم إجراء مراجعة للأدبيات لمقارنة المخاطر المرتبطة باستخدام الأنظمة الطبية الرقمية والورقية، مع التركيز على انتهاكات البيانات، والتنظيمات، والتدابير الأمنية في دراسات الحالة.

النتائج: تشمل العيوب الرئيسية للأنظمة الرقمية الهجمات الإلكترونية على السجلات وتعريض البيانات للاختراق. من ناحية أخرى، تواجه السجلات الورقية مخاطر مرتفعة مثل السرقة، أو التلف، أو الضياع. كلا النظامين يواجهان تحديات في الامتثال للمعايير وفي مشاركة البيانات بشكل آمن.

الخاتمة: يتطلب ضمان أمان بيانات المنشآت الطبية معالجة الجوانب المتعلقة بكل من الأنظمة الورقية والرقمية من خلال التشفير، والامتثال للقوانين، أو تثقيف الموظفين. يُنظر إلى التكيف المستمر كعامل رئيسي في الحماية الناجحة لبيانات المرضى.

الكلمات المفتاحية: السجلات الصحية الإلكترونية، التوثيق، الأنظمة الإلكترونية، الأنظمة الورقية، تسريب المعلومات الصحية، الأمان.