Proceeding International Conference Of Innovation Science, Technology, Education, Children And Health
Vol. 4 No. 2, 2024
e-ISSN : 2776-9062, page 01-25
Available online at: https://icistech.org/index.php/icistech

Challenges in Implementing Digital Medical Records in Indonesian Hospitals: Perspectives on Technology, Regulation, and Data Security

Fita Rusdian Ikawati[1*], M. Syauqi Haris[2]
[1, 2] Institute Technology of Science and Health Dr Soepraoen Hospital Malang, Indonesia
fitarusdian@gmail.com [1*]

Address: 2JCM+F4W, ITSK dr. Soepraoen, Kiduldalem, District. Klojen, Malang City, East Java
Author correspondence: fitarusdian@gmail.com

Abstract: *The implementation of digital medical records in Indonesian hospitals faces various challenges, especially in terms of technological readiness, inadequate regulations, and data security threats that need to be addressed to ensure efficient and safe healthcare services. This study aims to identify the challenges in Digital Medical Record Implementation from the perspective of technology, regulation, and data security. This study used a systematic literature review research approach guided by the Preferred Reposrting Items for Systematic Review and Meta-Analysis (PRISMA). The results showed that the implementation of digital medical records in Indonesian hospitals faces considerable challenges from three main perspectives, namely technology, regulation, and data security. The technology perspective includes several challenges such as 1) System Interoperability, 2) Privacy, 3) IT Infrastructure Limitations, 4) Implementation Costs and 5) Maintenance and Technology Adoption by Medical Staff. The regulatory perspective includes challenges such as 1) Regulatory Compliance, 2) Patient Data Protection, 3) Validity of Medical Records, 4) Long-term Data Retention and 5) System Interoperability. The data security perspective includes challenges such as 1) Infrastructure Security, 2) Data Encryption, 3) Access Control, 4) Incident Response and 5) Regular Security Audits. Thus, collaborative efforts between the government, hospitals and technology providers are needed to address these challenges and drive safe and effective digital transformation in Indonesia's healthcare sector.*

Keywords: *Digital Medical Records, Indonesian Hospitals, Technology, Regulation, Data Security*

1. INTRODUCTION

The implementation of digital medical records (DMRs) in Indonesian hospitals is of paramount importance, as it addresses numerous challenges associated with traditional paper-based systems while enhancing the overall quality of healthcare delivery. The transition to electronic medical records is not merely a technological upgrade; it represents a fundamental shift in how patient information is managed, accessed, and utilized within healthcare settings (Li et al., 2021). One of the primary benefits of adopting DMRs is the significant reduction in patient waiting times and the improvement in the continuity of care. A study conducted in Nigerian hospitals found that the adoption of DMRs led to a decrease in patient waiting times due to the availability of accurate and timely patient information, which is crucial for effective clinical decision-making (Onuogu, 2023). This is relevant in Indonesia, where healthcare facilities often face challenges related to patient flow and service delivery efficiency. The ability to quickly access patient records can streamline processes, reduce redundancies, and ultimately enhance patient satisfaction.

Received Agustus 15, 2024; Revised Agustus 30, 2024; Accepted September 15, 2024; Published September 17, 2024

Moreover, the digitalization of medical records facilitates better data management and enhances the quality of healthcare services. A comprehensive medical records system not only serves as a legal document but also plays a critical role in clinical decision-making and patient safety (Nasution, 2023). Incomplete or poorly managed medical records can lead to medical errors, which are a significant concern in healthcare settings. By implementing DMRs, hospitals can ensure that all relevant patient information is accurately recorded and easily accessible, thereby minimizing the risk of errors and improving patient outcomes (Rahmatiqa et al., 2020). In addition to improving operational efficiency and patient safety, the implementation of DMR can also support regulatory compliance and accreditation processes. Accurate and complete medical records are essential to meet the standards set by health authorities and ensure that hospitals maintain their accreditation status (Rahmatiqa et al., 2020). This is important for the overall credibility and quality assurance of healthcare institutions in Indonesia.

However, the implementation of digital medical records (RMD) in Indonesian hospitals faces significant challenges, most of which relate to technology infrastructure, cost, data security, regulation and human resources. One of the main challenges is the inadequate technology infrastructure, especially in remote areas. A report by the Ministry of Health (2021) shows that around 30% of hospitals in Indonesia do not have stable internet network access, which greatly hinders the adoption of RMD systems (Asyfia et al., 2023). This is in line with findings showing that the adoption of electronic medical record (EHR) systems is strongly influenced by the availability of adequate technology infrastructure (Steinhauser & Raptis, 2023; Yi, 2018). The adoption rate of RMD in Indonesia is also still low. Data from the Indonesian Hospital Association (PERSI) in 2022 showed that only around 40% of the 2,800 hospitals had implemented the system (Santoso et al., 2022). High implementation costs are an additional obstacle, especially for small and private hospitals, where the initial investment can reach IDR 1-2 billion (Basani, 2023). Research shows that high initial costs are often a major barrier to EHR implementation in various countries, including Indonesia (Widiyanto, 2023).In addition to improving operational efficiency and patient safety, DMR implementation can also support regulatory compliance and accreditation processes. Accurate and complete medical records are essential to meet the standards set by health authorities and ensure that hospitals maintain their accreditation status (Rahmatiqa et al., 2020). This is important for the credibility and overall quality assurance of healthcare institutions in Indonesia.

In addition, concerns over patient data security further complicate the situation. Data from the Ministry of Communication and Informatics (2021) notes that the healthcare sector in

Indonesia is one of the targets of cyberattacks, with approximately 8 million attacks detected (Keshta & Odeh, 2021). Data security and privacy are important issues that must be addressed to increase trust in the use of RMD (Keshta & Odeh, 2021; Wardhana et al., 2022). Government regulations related to RMD are also inconsistent across regions, causing confusion for many hospitals, especially private ones (Asyfia et al., 2023; Basani, 2023). The lack of human resources skilled in health technology is slowing down the implementation of RMD. The Ministry of Health noted that 35% of hospitals had difficulty in recruiting IT experts with knowledge of RMD (Santoso et al., 2022). Research shows that the success of EHR implementation is highly dependent on the availability of a skilled and trained workforce (Yi, 2018; Widiyanto, 2023). Although this challenge is considerable, with improved infrastructure and support from the government, it is hoped that RMD implementation in Indonesia can run more smoothly in the future (Steinhauser & Raptis, 2023; Santoso et al., 2022).

The failure to resolve the challenges associated with implementing electronic medical records (EMR) in Indonesian hospitals could lead to significant repercussions across various dimensions of healthcare delivery. One of the most pressing concerns is the potential for compromised patient safety and care quality. The transition from paper-based to electronic medical records is not merely a technological upgrade; it necessitates a fundamental change in workflows and practices among healthcare professionals. Research indicates that the persistence of outdated routines surrounding paper records can hinder the effective use of EMR systems, leading to inefficiencies and errors in patient care (Scott et al., 2016). Moreover, inadequate training and preparedness of healthcare staff to utilize these systems can exacerbate these issues, potentially resulting in miscommunication or delayed treatment (Basani, 2023).

In addition to patient safety concerns, the lack of a robust digital medical record system can also lead to legal and ethical complications. The absence of comprehensive electronic records may expose healthcare providers to administrative and legal sanctions, as incomplete or poorly managed medical records can result in violations of health regulations (Mardi, 2022). Furthermore, the ethical implications of data security and patient confidentiality become increasingly critical in the absence of established protocols for EMR usage. The risk of data breaches and unauthorized access to sensitive medical information could undermine patient trust and lead to significant legal liabilities for healthcare institutions (Assagaff, 2023; Budiyanti et al., 2019). Furthermore, without a commitment to resolving EMR implementation challenges, Indonesian hospitals may miss out on the benefits of better data analysis, population health management, and personalized medicine, which are increasingly becoming standard in global healthcare practices (Tapuria et al., 2021).

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

This research proposes a comprehensive approach that integrates technology, regulation and data security in the implementation of digital medical records in Indonesian hospitals. This approach is important given the challenges faced, such as uneven technological infrastructure and evolving regulations (Asyfia et al., 2023; Sanjaya, 2023). Previous research has often separated studies on these aspects, ignoring the interaction between the three (Elkefi & Asan, 2022). In addition, data security awareness among healthcare workers is still low, which may increase the risk of privacy breaches (Uwizeyemungu et al., 2019). In addition, this research also provides a special focus on the Indonesian context, which has unique challenges such as uneven technology infrastructure, evolving regulations, and relatively low levels of data security awareness in many hospitals. Thus, this research is expected to provide new contributions to the development of a more efficient, secure, and regulatory compliant digital medical record implementation strategy in Indonesia.

The implementation of digital medical records (RMD) in Indonesian hospitals is becoming increasingly important along with the rapid development of information technology and the need for more efficient health services. Digital medical records (RMD) have great potential to improve hospital operational efficiency, speed up diagnosis, and facilitate patient data access and exchange. However, there are still significant challenges in implementing RMD in Indonesia, mainly related to technological readiness, limited comprehensive regulations, and evolving threats to data security. In the midst of accelerated digitization driven by the need for fast and accurate healthcare services, the lack of understanding and strategies in addressing technical, legal, and security aspects may hinder the full adoption of RMD. This research becomes urgent to provide appropriate recommendations, as well as to ensure that the implementation of RMD can be done safely, efficiently, and in accordance with applicable legal standards, so that hospitals can provide better and reliable health services to the community. Thus, this study aims to identify the challenges in Digital Medical Record Implementation from the perspective of technology, regulation, and data security.

2. RESEARCH METHODOLOGY

Overview of the Systematic Literature Review Process

The methodology used in this study is Systematic Literature Review (SLR), which aims to identify, assess, and interpret all relevant research findings related to challenges in the implementation of Digital Medical Records in Indonesian Hospitals from the perspective of technology, regulation, and data security. The SLR process follows the PRISMA (Preferred

Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, which consists of the following stages:

a. Identification: At this stage, a literature search was conducted to collect articles, journals and other documents relevant to the research topic. The search was conducted through electronic databases such as Google Scholar, Scopus, and Web of Science using predetermined keywords.
b. Filtering: After the identification stage, the search results were screened to eliminate duplicates and irrelevant articles. Articles that did not meet the inclusion criteria or were outside the scope of the study were eliminated at this stage.
c. Eligibility: Articles that passed the screening stage were then evaluated for eligibility based on the predetermined inclusion and exclusion criteria. Articles that did not provide sufficient data or were not relevant to the research focus were also eliminated at this stage.
d. Inclusion: Articles that met all the criteria were included for further analysis. This stage resulted in a final list of literature that would be analyzed in depth in the study.

Data Extraction

After the literature selection process is completed, the next stage is data extraction from the selected articles. This process includes identifying and recording key information from each article relevant to the research objectives.

a. Search String

The literature search is conducted using various keywords relevant to the research topic. The keywords used are tailored to the databases accessed and include terms such as "technology adoption", " regulatory frameworks", and "data security".

b. Inclusion and Exclusion Criteria

Inclusion Criteria:

1) Articles published in reputable scientific journals.
2) Articles that discuss challenges in implementing Digital Medical Records in Indonesian hospitals
3) Articles published within the last 10 years to ensure data relevance.
4) Articles are available in English or Indonesian.

Exclusion Criteria:

1) Articles that do not provide empirical data or concrete research findings.
2) Articles that are not fully accessible (only available as abstracts).

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

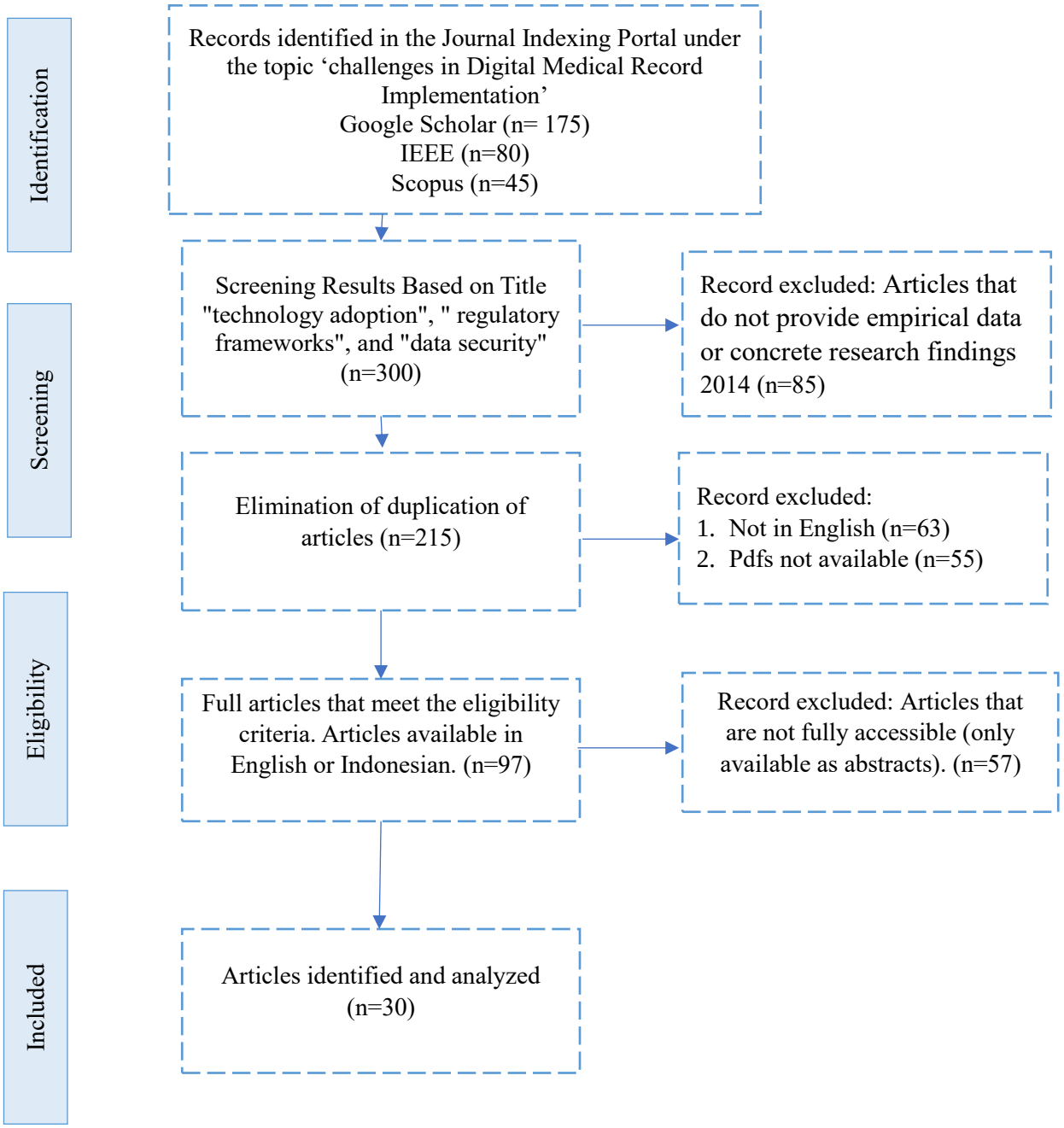

Figure 1. Systematic Review Diagram based on PRISMA

3. RESULT

Distribution Paper Based on Developing Countries

Table 1. Distribution Paper Based on Developing Countries

Countries	No. of Paper	Pesentage
Jerman	3	10%
New York	1	3,33%
Inggris	1	3,33%
China	1	3,33%
Indonesia	2	6,66%
India	6	20%
Iran	1	3,33%
Israel	1	3,33%
Malaysia	1	3,33%
Polandia	1	3,33%
Austaralia	2	6,66%
Prancis	1	3,33%
Arab	1	3,33%
Rusia	2	6,66%
Switzerland	1	3,33%
China	1	3,33%
Thailand	1	3,33%

Based on the distribution of countries, the research reviewed in this study was published in several countries, including Jerman, New York, Inggris, China, Indonesia, India, Iran, Israel, Malaysia, Polandia, Austaralia, Prancis, Arab, Rusia, Switzerland, China and Thailand. Based on the findings from these countries, the country with the highest journal article publication is India with 6 journals each and a percentage of 20%.

Distribution Paper Based on Year

Table 2. Distribution Paper Based on Year

Year	No. of Paper	Pesentage
2019	2	6,66%
2020	1	3,33%
2021	2	6,66%
2022	7	23,3%
2023	9	30%
2024	9	30%

Based on the years of research in the range 2019-2024, 30 years of journal and proceedings publications were obtained with a total percentage of 100%. In 2019, 2021 there was 2 journal with a percentage of 6,66%. In 2022 there were 7 journals with a percentage of 23,33%. In 2023, 2024 there were 9 journals with a percentage of 30%. Based on this data, it can be concluded that from 2016 to 2024 there were fluctuations in publishing.

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

Target Paper

Table 3. Target Paper

Type of Paper	No. of Paper	Percentage
Proceedings	5	16,6%
Journal	25	83,3%

Based on the type of journal, this research is divided into two, namely proceedings and scientific journals. Based on the findings of these two types of research, there are 5 proceedings journals with a total percentage of 16.6% and 25 published research journals with a total percentage of 83.3%.

Challenges in Implementing Digital Medical Records (DMR) from a Technological Perspective

Tabel 4. Challenges in Implementing Digital Medical Records (DMR) from a Technological Perspective

Technology Aspect	Description	Examples and Implications	Research Findings	Author
System Interoperability	Difficulty in connecting different health systems, limiting data exchange across hospitals.	1. Different systems in various hospitals cannot connect, limiting the exchange of patient data. 2. Limited access to data across institutions.	Poor interoperability slows medical decision-making as hospitals can't access patient data from other facilities.	Danny et al (2024); Oshani (2023)
Privacy	Maintaining data confidentiality and protecting against cyber threats.	1. Health data breaches can lead to privacy violations. 2. Risk of identity theft and misuse of sensitive medical information.	Hospitals struggle with securing patient data from breaches, risking public trust in digital systems.	Christopher et al (2023); Hassan et al (2024)
IT Infrastructure Limitations	Insufficient internet access and inadequate hardware in some hospitals.	1. Hospitals in remote areas face poor network conditions, limiting access to DMR 2. Computers or servers often experience breakdowns or overheating.	Rural hospitals often lack proper infrastructure, which hinders effective DMR implementation.	S. Badsha et al (2019); Rachel, V. et al (2023)
Implementation and Maintenance Costs	High initial costs and ongoing maintenance	1. The cost of software acquisition and staff training is high.	Small and medium hospitals face financial difficulties in	Anubhav et al (2024); Masarat, Ayat (2024)

Technology Aspect	Description	Examples and Implications	Research Findings	Author
	for DMR technology.	2. Small hospitals often lack the budget for regular system updates.	adopting and maintaining DMR systems.	
Technology Adoption by Medical Staff	Resistance from staff used to manual methods; training required.	1. Doctors and nurses are reluctant to use new systems due to perceived complexity. 2. Intensive training is needed, but medical staff often lack time for training.	Medical staff face challenges transitioning to digital systems, slowing adoption due to limited training opportunities.	Venkatesh et al (2024); Muhammad et al (2023)

The implementation of Digital Medical Records in Indonesian hospitals faces several significant technological challenges. One major issue is system interoperability, where the Digital Medical Records system must integrate with various existing systems, such as laboratory and radiology systems. Incompatibility between these systems often hampers the efficient flow of information and creates difficulties in effective data sharing.

Privacy concerns are also a primary focus, given that medical data is highly sensitive. Many hospitals struggle to implement systems that are secure enough to protect patient data from unauthorized access. Additionally, IT infrastructure limitations pose a significant barrier, as existing hardware and software may be inadequate to support advanced Digital Medical Records systems.

Moreover, implementation and maintenance costs for Digital Medical Records systems can be very high, adding a substantial burden to many hospitals. Technology adoption by medical staff is another challenge, especially for those who are not familiar with digital technology or who receive insufficient training. Addressing these challenges requires effective strategies and support from various stakeholders to ensure the successful implementation of Digital Medical Records.

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

Challenges in Implementing Digital Medical Records (DMR) from a Regulation Perspective

Tabel 5. Challenges in Implementing Digital Medical Records (DMR) from a Regulation Perspective

Regulation Aspect	Description	Examples and Implications	Research Findings	Author
Regulatory Compliance	Hospitals must comply with government regulations on data storage and access.	Lack of understanding can lead to legal violations and penalties.	Many hospitals do not fully understand regulations related to data security.	Krzysztof, Świtała. (2023); Patience, Onuogu (2023)
Patient Data Protection	Data privacy regulations in the digital context are still vague.	Weak security systems increase the risk of data breaches, leading to loss of public trust.	Some hospitals lack adequate systems to protect patient data.	Susan, et al (2024); Iris et al (2022)
Medical Record Validity	Rules on digital signatures and authentication are unclear.	Uncertainty around digital signatures delays the adoption of digital technology.	Many healthcare workers are unclear on how to properly implement legal digital signatures.	François et al (2022); Utkarsh et al (2021)
Long-Term Data Storage	Regulations on long-term data storage are not clearly defined.	Unclear rules may result in the loss of important data over time.	Many hospitals still keep physical records as backups due to digital regulation uncertainty.	Elif, et al (2024); Nehama et al (2022)
System Interoperability	No national standard for integrating different medical record systems.	Different systems make it difficult to exchange data between hospitals and other institutions.	Many hospitals struggle to integrate their digital systems with others.	Wisnu et al (2024); T., Sujithra (2022)

The implementation of Digital Medical Records (DMR) in Indonesian hospitals faces several significant challenges. One major issue is Regulatory Compliance, where hospitals must adhere to complex and evolving regulations and ensure that DMR systems align with health and privacy laws. Additionally, Patient Data Protection is a crucial concern, as safeguarding patient data from breaches or unauthorized access is essential. This requires robust security mechanisms to protect sensitive patient information.

On the other hand, ensuring Medical Record Validity is vital to maintain the accuracy and medical legitimacy of recorded data, as errors in medical records can have serious implications for patient care. Long-Term Data Storage is also a critical challenge, necessitating adequate planning and infrastructure to securely store data and ensure consistent access over time. Lastly, System Interoperability requires that DMR systems integrate effectively with other health systems to facilitate efficient information exchange across the healthcare network. Addressing these challenges is key to the successful implementation of DMR in Indonesian hospitals.

Challenges in Implementing Digital Medical Records (DMR) from a Data Security Perspective

Tabel 6. Challenges in Implementing Digital Medical Records (DMR) from a Data Security Perspective

Regulation Aspect	Description	Examples and Implications	Research Findings	Author
Infrastructure Security	Protecting IT infrastructure from cyberattacks.	Servers vulnerable to ransomware: Loss of sensitive medical data.	Many hospitals lack optimal protection systems.	Yasir et al (2023); AA, Mokhov (2022)
Data Encryption	Data must be encrypted during storage and transfer.	Unencrypted data: Risk of data theft by hackers.	Only some hospitals apply strong data encryption.	Salem et al (2020); Yaping et al (2022)
Access Control	Restricting access to medical records for authorized staff.	Unrestricted access: Privacy violations.	Access control is often inadequate.	Nahla, F. et al (2022); Naresh et al (2023)
Incident Response	Quick response to data breaches or cyberattacks.	No response plan: Slow incident handling, patient data risk.	Many hospitals lack comprehensive incident protocols.	G., Sucharitha. Et al (2023); P.Y.S., Lakshman et al (2021)
Regular Security Audits	Routine audits to identify security weaknesses.	No regular audits: System vulnerabilities remain undetected.	Security audits are infrequent, especially in rural areas.	Rashmi et al (2024); Wasinee et al (2019)

The implementation of Digital Medical Records (DMR) in Indonesian hospitals faces several challenges, particularly concerning data security. One major challenge is Infrastructure Security. A robust and secure infrastructure is essential to protect DMR systems from cyber threats. Many hospitals lack the necessary infrastructure to handle the risks associated with

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

storing and managing digital medical data, such as servers and networks vulnerable to hacking or technical failures. This requires substantial investment in technology and human resources to ensure that DMR systems operate securely and reliably.

Additionally, Data Encryption, Access Control, Incident Response, and Regular Security Audits are critical components. Data Encryption is vital for safeguarding sensitive medical information from unauthorized access during storage and transmission. Access Control ensures that only authorized personnel can access specific data, reducing the risk of information leaks. Incident Response refers to the hospital's preparedness to swiftly and effectively address security breaches. Lastly, Regular Security Audits are necessary to identify potential vulnerabilities and ensure compliance with security standards. Overall, addressing these challenges requires strategic planning and attention to maintain the integrity and confidentiality of medical data in DMR implementation.

3. DISCUSSIONS

Challenges in Implementing DMR from a Technological Perspective

The implementation of digital medical records (DMRs) presents a myriad of challenges from a technological perspective, which can significantly impact the efficiency and effectiveness of healthcare delivery systems. These challenges are multifaceted, encompassing issues related to interoperability, user acceptance, data security, and the integration of advanced technologies such as artificial intelligence and blockchain. One of the primary technological challenges in implementing DMRs is interoperability. Interoperability refers to the ability of different information systems and software applications to communicate, exchange data, and use the information that has been exchanged. The lack of standardized interfaces among various electronic health record (EHR) systems can lead to fragmented healthcare delivery, where patient information is siloed within different systems, making it difficult for healthcare providers to access comprehensive patient histories (Sanjaya, 2023; Janett & Yeracaris, 2020). This fragmentation not only complicates care coordination but also increases the risk of medical errors due to incomplete information being available to clinicians (Meshkat et al., 2022; Gee & Newman, 2013).

Moreover, the integration of DMRs into existing healthcare workflows poses significant challenges. Many healthcare professionals are accustomed to traditional paper-based records, and transitioning to a digital system requires substantial changes in daily routines and workflows. This transition can lead to increased documentation burdens, which may detract from face-to-face patient interactions and contribute to clinician burnout (Meshkat

et al., 2022; Gee & Newman, 2013; Quiroz et al., 2019). The need for extensive training and adaptation to new technologies can further exacerbate resistance among healthcare staff, hindering the successful adoption of DMRs (Quiroz et al., 2019).Data security and privacy concerns are also paramount in the implementation of DMRs. The digitization of sensitive patient information raises the stakes for data breaches and unauthorized access, necessitating robust cybersecurity measures to protect patient data (Negro-Calduch et al., 2021; Carter et al., 2019). Healthcare organizations must navigate complex regulatory environments, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandates stringent protections for patient information. Failure to comply with these regulations can result in severe penalties and loss of patient trust (Negro-Calduch et al., 2021).

In addition to these challenges, the integration of advanced technologies such as artificial intelligence (AI) and blockchain into DMR systems presents both opportunities and obstacles. AI has the potential to enhance clinical documentation processes and improve patient care through predictive analytics and decision support tools (Lin et al., 2018). However, the successful implementation of AI requires careful consideration of the ethical implications, potential biases in algorithms, and the need for transparency in AI-driven decision-making processes (Lin et al., 2018). Similarly, while blockchain technology offers promising solutions for secure and efficient health records management, its implementation is hindered by scalability issues, the need for widespread adoption, and the complexity of integrating blockchain with existing systems (Santoso et al., 2020).

The financial implications of implementing DMRs also cannot be overlooked. The costs associated with purchasing, maintaining, and upgrading electronic health record systems can be substantial, often running into millions of dollars for large healthcare organizations (Gee & Newman, 2013). Furthermore, the initial investment may not yield immediate returns, as the transition period often involves decreased productivity and increased operational costs due to the learning curve associated with new technologies (Gee & Newman, 2013). In summary, the challenges in implementing digital medical records from a technological perspective are complex and interrelated. Issues of interoperability, user acceptance, data security, and the integration of advanced technologies all contribute to the difficulties faced by healthcare organizations in adopting DMRs. Addressing these challenges requires a multifaceted approach that includes stakeholder engagement, investment in training and support, and the development of standardized protocols to facilitate seamless information exchange across different systems.

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

Challenges in Implementing DMR from a Regulation Perspective

The implementation of digital medical records (DMRs) presents a myriad of challenges, particularly from a regulatory perspective. As healthcare systems increasingly transition from paper-based records to electronic formats, the complexities surrounding compliance with existing regulations, data privacy, and interoperability become paramount. One of the foremost challenges in implementing DMRs is ensuring compliance with regulatory frameworks that govern data privacy and security. The Health Information Technology for Economic and Clinical Health (HITECH) Act, for instance, has set forth stringent requirements for the protection of electronic health information, mandating that healthcare providers adopt secure electronic medical record (EMR) systems (Carter et al., 2019). However, many healthcare organizations struggle to meet these standards due to a lack of resources and expertise in cybersecurity, which can lead to vulnerabilities in patient data protection (Escano & Raheja, 2017). The integration of disparate systems further complicates compliance, as different entities may have varying standards and protocols, making it difficult to maintain a cohesive regulatory approach (Escano & Raheja, 2017; Janett & Yeracaris, 2020).

Moreover, the issue of interoperability remains a significant barrier to the effective implementation of DMRs. Interoperability refers to the ability of different health information systems to communicate and exchange data seamlessly. A lack of standardized interfaces among various EMR systems can impair the effective collaboration and information exchange necessary for comprehensive patient care (Janett & Yeracaris, 2020). This fragmentation not only hinders the quality of care but also poses regulatory challenges, as healthcare providers may inadvertently violate data sharing regulations due to incompatible systems (Janett & Yeracaris, 2020; Isakari et al., 2023). The need for standardized protocols is further emphasized by the increasing demand for integrated health records that can facilitate coordinated care across multiple providers (Houben et al., 2015).

In addition to compliance and interoperability, the challenge of ensuring patient privacy and data security cannot be overstated. The digitization of medical records raises significant concerns regarding the confidentiality of sensitive health information. Patients often express anxiety about the potential for data breaches and unauthorized access to their medical records (Tapuria et al., 2021). Regulatory bodies have responded by instituting strict guidelines for data handling and patient consent, yet the rapid pace of technological advancement often outstrips the ability of regulations to adapt (Chen et al., 2012). As healthcare organizations implement DMRs, they must navigate a complex landscape of legal requirements while also addressing the ethical implications of patient data usage (Isakari et al., 2023; Taki, 2023). Furthermore,

the implementation of DMRs can exacerbate existing disparities in healthcare access and quality. In many regions, particularly in low- and middle-income countries, there are significant gaps in digital infrastructure and workforce training (Mumtaz, 2023; Owoyemi et al., 2022). These disparities can hinder the effective rollout of DMR systems, as healthcare providers may lack the necessary skills to utilize digital tools effectively (Mumtaz, 2023). Regulatory frameworks must therefore account for these inequalities, ensuring that all healthcare providers have the resources and training needed to comply with digital record-keeping standards (Mumtaz, 2023; Owoyemi et al., 2022).

The transition to DMRs also necessitates a cultural shift within healthcare organizations, which can be met with resistance from staff accustomed to traditional record-keeping methods. Training and education are critical components of this transition, as healthcare workers must be equipped with the knowledge and skills to navigate new technologies (Ismawati et al., 2021). However, regulatory bodies often do not provide sufficient guidance or support for training initiatives, leaving organizations to develop their own strategies for workforce development (Ismawati et al., 2021). This lack of standardized training can lead to inconsistencies in record-keeping practices, further complicating compliance efforts.

Moreover, the ethical implications of patient access to their own health records must be considered. While empowering patients to access their medical information can enhance engagement and self-management, it also raises questions about the potential for misinterpretation of data and the psychological impact of accessing sensitive health information (Hägglund et al., 2022). Regulatory frameworks must strike a balance between promoting patient empowerment and safeguarding against the risks associated with increased access to personal health data (Hägglund et al., 2022). Finally, the global nature of healthcare necessitates a consideration of international regulatory standards in the implementation of DMRs. As healthcare providers increasingly operate across borders, the need for harmonized regulations becomes critical to ensure compliance and protect patient data (Taki, 2023). However, differing legal frameworks and cultural attitudes towards data privacy can complicate efforts to establish a unified approach to digital record-keeping (Taki, 2023). Regulatory bodies must engage in international dialogue to develop standards that can be universally applied while respecting local laws and customs (Taki, 2023).

In conclusion, the challenges associated with implementing digital medical records from a regulatory perspective are multifaceted and complex. Compliance with existing regulations, ensuring interoperability, safeguarding patient privacy, addressing disparities in

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

access, and navigating the financial and ethical implications of digital record-keeping all present significant hurdles. As healthcare organizations continue to adopt DMR systems, it is imperative that regulatory bodies provide clear guidance and support to facilitate a successful transition that prioritizes patient safety and quality of care.

Challenges in Implementing DMR from a Data Security Perspective

The implementation of digital medical records (DMRs) in healthcare settings has been met with numerous challenges, particularly from a data security perspective. As healthcare organizations increasingly adopt electronic health records (EHRs), the protection of sensitive patient information has become paramount. The transition from paper-based records to digital formats introduces vulnerabilities that can be exploited by cybercriminals, leading to data breaches and compromised patient confidentiality. This discussion synthesizes various scholarly sources to explore the multifaceted challenges associated with the security of digital medical records.

One of the most significant challenges in implementing DMRs is the inherent risk of cyberattacks. The healthcare sector has become a prime target for cybercriminals due to the sensitive nature of the data it handles. Research indicates that healthcare organizations are frequently subjected to ransomware attacks, which can lock access to critical patient data until a ransom is paid (Alanazi, 2023; Lekshmi, 2022; Wright, 2023). The WannaCry ransomware attack in 2017 serves as a stark reminder of the vulnerabilities present in healthcare systems, affecting numerous organizations globally and highlighting the urgent need for robust cybersecurity measures (Aljuraid & Justinia, 2022). The financial implications of such attacks are substantial, not only due to ransom payments but also because of the potential costs associated with data recovery, legal liabilities, and damage to reputation (Nifakos et al., 2021; Sanmorino, 2023). Moreover, the complexity of healthcare IT environments exacerbates security challenges. The integration of various technologies, including cloud computing, mobile devices, and interconnected medical devices, creates a heterogeneous landscape that is difficult to secure (Sanmorino, 2023; Arain et al., 2019). Each device and application may have different security protocols, leading to potential gaps in protection. The legal and ethical implications of data security in healthcare cannot be overlooked. The use of DMRs raises questions regarding data ownership, consent, and the ethical responsibilities of healthcare providers to protect patient information (Budiyanti et al., 2019). As healthcare becomes increasingly personalized, the need for stringent data protection measures grows, particularly concerning genomic data and other sensitive health information. The lack of specific

regulations governing data security in some regions further complicates the landscape, leaving healthcare organizations vulnerable to legal repercussions in the event of a data breach (Budiyanti et al., 2019).

Furthermore, the evolving nature of cyber threats necessitates continuous adaptation of security strategies. Cybercriminals are constantly developing new techniques to exploit vulnerabilities, making it imperative for healthcare organizations to stay ahead of potential threats (Alanazi, 2023; Baptist, 2023). This dynamic environment requires regular assessments of security protocols, investment in advanced technologies, and collaboration with cybersecurity experts to identify and address emerging risks (Jerry-Egemba, 2023). Hospital must also consider the integration of advanced technologies such as artificial intelligence and machine learning to enhance threat detection and response capabilities (Sanmorino, 2023; Coventry & Branley, 2018). In addition, interoperability presents another challenge in securing digital medical records. The ability to share data across different systems and platforms is essential for providing comprehensive patient care, yet it also increases the risk of data breaches (Rigas, 2023; Natsiavas et al., 2018). Ensuring that data remains secure during transmission and that all systems adhere to consistent security standards is crucial for maintaining patient confidentiality. The development of standardized protocols for data exchange can help mitigate these risks, but achieving interoperability while ensuring security remains a complex challenge (Natsiavas et al., 2018).

In conclusion, the implementation of digital medical records in healthcare settings is fraught with challenges from a data security perspective. Cyberattacks, complex IT environments, human factors, legal and ethical considerations, evolving threats, economic implications, and interoperability issues all contribute to the difficulties faced by healthcare organizations. Addressing these challenges requires a multifaceted approach that includes robust cybersecurity measures, clear regulatory guidelines, and ongoing investment in technology and infrastructure. As the healthcare sector continues to evolve, prioritizing the security of digital medical records will be essential for protecting patient information and maintaining trust in healthcare systems.

4. CONCLUSIONS

Based on the literature review that has been conducted, it is known that the research findings show that the implementation of digital medical records in Indonesian hospitals faces various significant challenges from three main perspectives, namely technology, regulation, and data security. The technology perspective includes several challenges such as 1) System

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

Interoperability, Privacy, IT Infrastructure Limitations, Implementation and Maintenance Costs and Technology Adoption by Medical Staff. The regulatory perspective includes several challenges such as 1) Regulatory Compliance, Patient Data Protection, Medical Record Validity, Long-Term Data Storage and System Interoperability. The data security perspective includes challenges such as 1) Infrastructure Security, Data Encryption, Access Control, Incident Response and Regular Security Audits. Therefore, a comprehensive and structured collaborative effort is needed between various stakeholders, including the government, hospitals, technology providers, and other related institutions, to overcome the various challenges faced in the implementation of digital medical records. These efforts should include strengthening regulations, improving technology infrastructure, and training for medical personnel. In addition, a focus on data security with protection systems that comply with international standards is essential to prevent information leakage. With these measures, digital transformation in Indonesia's healthcare sector can be effective and safe, improving the overall quality of healthcare services.

REFRENCES

AA, Mokhov. (2022). 23. Digital health: challenges facing medical ethics. doi: 10.24075/medet.2021.025

Alanazi, A. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. Cureus. https://doi.org/10.7759/cureus.47026

Aljuraid, R. and Justinia, T. (2022). Classification of challenges and threats in healthcare cybersecurity: a systematic review.. https://doi.org/10.3233/shti220739

Anubhav, Gupta., Ankur, Sharma., Deepak, Kumar, Jha. (2024). 1. Overcoming Obstacles STEP By STEP: A Comprehensive Review of Challenges and Strategies in Implementing Hospital Management Information Systems in India. doi: 10.21203/rs.3.rs-4631703/v1

Arain, M., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on it security and privacy in a large healthcare organization. Journal of Multidisciplinary Healthcare, Volume 12, 73-81. https://doi.org/10.2147/jmdh.s183275

Assagaff, S. (2023). Implementation of teledentistry during the covid-19 pandemic at bandung community health centers. Majalah Kedokteran Gigi Indonesia, 8(3), 215. https://doi.org/10.22146/majkedgiind.75954

Asyfia, A., Mahendika, D., & Setyowati, M. (2023). Medical record digitization policy: overview of the health minister regulation number 24 of 2022. Consilium Sanitatis Journal of Health Science and Policy, 1(2), 54-61. https://doi.org/10.56855/jhsp.v1i2.227

Asyfia, A., Mahendika, D., & Setyowati, M. (2023). Medical record digitization policy: overview of the health minister regulation number 24 of 2022. Consilium Sanitatis

Journal of Health Science and Policy, 1(2), 54-61. https://doi.org/10.56855/jhsp.v1i2.227

Awaludin, A., Sulistyadi, W., & Chandra, A. (2023). Analysis of attacks and cybersecurity in the health sector during a pandemic covid-19: scoping review. Journal of Social Science, 4(1), 62-70. https://doi.org/10.46799/jss.v4i1.512

Baptist, A. (2023). Unravelling the web of issues and challenges in healthcare cybersecurity for a secure tomorrow. Business and Economic Research, 13(4), 59. https://doi.org/10.5296/ber.v13i4.21341

Basani, C. (2023). Legal protection of patient's electronic medical record: indonesian legal perspective. Dialogia Iuridica, 15(1), 094-112. https://doi.org/10.28932/di.v15i1.7492

Basani, C. (2023). Legal protection of patient's electronic medical record: indonesian legal perspective. Dialogia Iuridica, 15(1), 094-112. https://doi.org/10.28932/di.v15i1.7492

Budiyanti, R., Herlambang, P., & Nandini, N. (2019). Tantangan etika dan hukum penggunaan rekam medis elektronik dalam era personalized medicine. Jurnal Kesehatan Vokasional, 4(1), 49. https://doi.org/10.22146/jkesvo.41994

Budiyanti, R., Herlambang, P., & Nandini, N. (2019). Tantangan etika dan hukum penggunaan rekam medis elektronik dalam era personalized medicine. Jurnal Kesehatan Vokasional, 4(1), 49. https://doi.org/10.22146/jkesvo.41994

Carter, G., White, D., Nalla, A., Shahriar, H., & Sneha, S. (2019). Toward application of blockchain for improved health records management and patient care. Blockchain in Healthcare Today, 2. https://doi.org/10.30953/bhty.v2.37

Chen, Y., Cheng, B., Chen, H., Lin, C., Liao, G., Hou, B., … & Hsu, S. (2012). A privacy-preserved analytical method for ehealth database with minimized information loss. Journal of Biomedicine and Biotechnology, 2012, 1-9. https://doi.org/10.1155/2012/521267

Christopher, Bourn., Joseph, Heirendt., Kamsiyochukwu, Ben-Chiobi., Alexander, Haastrup., Ahmed, Sherif., Mohamed, Elsersy. (2023). 1. Privacy-Preserving Data Sharing Scheme for E-Health Systems. doi: 10.1109/itt59889.2023.10184235

Coventry, L. and Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, 113, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

Danny, Ammon., Maximilian, Kurscheidt., Karoline, Buckow., Toralf, Kirsten., Matthias, Löbe., Frank, A., Meineke., F., Prasser., Julian, Saß., Ulrich, Sax., Sebastian, Stäubert., Sylvia, Thun., Reto, Wettstein., Joshua, P, Wiedekopf., Judith, A, H, Wodke., Martin, Boeker., Thomas, Ganslandt. (2024). 1. [Interoperability Working Group: core dataset and information systems for data integration and data exchange in the Medical Informatics Initiative].. doi: 10.1007/s00103-024-03888-4

Elif, Tekin., Nagihan, Kartal. (2024). 17. Security of Digital Transformation in the Healthcare Sector. Advances in electronic government, digital divide, and regional development book series, doi: 10.4018/979-8-3693-3567-3.ch010

Elkefi, S. and Asan, O. (2022). Digital twins for managing health care systems: rapid literature review. Journal of Medical Internet Research, 24(8), e37641. https://doi.org/10.2196/37641

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

Emanuel, A. (2019). Challenges and proposed model in implementing integrated medical record systems in indonesia. International Journal of Advanced Science and Technology, 130, 1-10. https://doi.org/10.33832/ijast.2019.130.01

Escano, M. and Raheja, D. (2017). System safety in healthcare. Journal of System Safety, 53(2), 8-10. https://doi.org/10.56094/jss.v53i2.88

François, Bocquet., Mario, Campone., Marc, Cuggia. (2022). 14. The Challenges of Implementing Comprehensive Clinical Data Warehouses in Hospitals. International Journal of Environmental Research and Public Health, doi: 10.3390/ijerph19127379

G., Sucharitha., G., Sai, Aditya., J., Varsha., G., Sai, Nikhil. (2023). 29. Electronic Medical Records Using Blockchain Technology. EAI Endorsed Transactions on Pervasive Health and Technology, doi: 10.4108/eetpht.9.4284

Gee, R. and Newman, J. (2013). Health information technology. Obstetrics and Gynecology, 121(6), 1161-1164. https://doi.org/10.1097/aog.0b013e318293741e

Gordon, W., Wright, A., Aiyagari, R., Corbo, L., Glynn, R., Kadakia, J., … & Landman, A. (2019). Assessment of employee susceptibility to phishing attacks at us health care institutions. Jama Network Open, 2(3), e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Hägglund, M., McMillan, B., Whittaker, R., & Blease, C. (2022). Patient empowerment through online access to health records. BMJ, e071531. https://doi.org/10.1136/bmj-2022-071531

Hassan, Jamal., Nasir, Ahmed, Algeelani., Najeeb, Abbas, Al-Sammarraie. (2024). 2. Safeguarding data privacy: strategies to counteract internal and external hacking threats. Computer Science and Information Technologies, doi: 10.11591/csit.v5i1.p46-54

Houben, S., Frost, M., & Bardram, J. (2015). Collaborative affordances of hybrid patient record technologies in medical work.. https://doi.org/10.1145/2675133.2675164

Iris, Cathrina, Abacan, Pilares., Sami, Azam., Serkan, Akbulut., Mirjam, Jonkman., Bharanidharan, Shanmugam. (2022). 13. Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. Sensors, doi: 10.3390/s22114032

Isakari, M., Sanchez, A., Conic, R., Peretti, J., Saito, K., Sitapati, A., … & Longhurst, C. (2023). Benefits and challenges of transitioning occupational health to an enterprise electronic health record. Journal of Occupational and Environmental Medicine, 65(7), 615-620. https://doi.org/10.1097/jom.0000000000002864

Ismawati, N., Supriyanto, S., Haksama, S., & Hadi, C. (2021). The influence of knowledge and perceptions of doctors on the quality of medical records. Journal of Public Health Research, 10(2), jphr.2021.2228. https://doi.org/10.4081/jphr.2021.2228

Janett, R. and Yeracaris, P. (2020). Electronic medical records in the american health system: challenges and lessons learned. Ciência & Saúde Coletiva, 25(4), 1293-1304. https://doi.org/10.1590/1413-81232020254.28922019

Janett, R. and Yeracaris, P. (2020). Electronic medical records in the american health system: challenges and lessons learned. Ciência & Saúde Coletiva, 25(4), 1293-1304. https://doi.org/10.1590/1413-81232020254.28922019

Jerry-Egemba, N. (2023). Safe and sound: strengthening cybersecurity in healthcare through robust staff educational programs. Healthcare Management Forum, 37(1), 21-25. https://doi.org/10.1177/08404704231194577

Keshta, I. and 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

Ko, H., Mesicek, L., Choi, J., & Hwang, S. (2018). A study on secure medical-contents strategies with drm based on cloud computing. Journal of Healthcare Engineering, 2018, 1-7. https://doi.org/10.1155/2018/6410180

Krzysztof, Świtała. (2023). 7. Medical Data in the Digital Era - Legal Challenges Related to Providing Information Security, Applying GDPR and Respecting the Professional Secrecy. doi: 10.23919/MIPRO57284.2023.10159891

Larkin, K. and Kelliher, A. (2011). Designing flexible emr systems for recording and summarizing doctor-patient interactions.. https://doi.org/10.1145/1979742.1979816

Lekshmi, A. (2022). Growing concern on healthcare cyberattacks & need for cybersecurity.. https://doi.org/10.31234/osf.io/7m4qf

Li, H., Chen, Y., Chen, T., Chiou, S., & Hwang, S. (2021). The role of patient records in research: a bibliometric analysis of publications from an academic medical center in taiwan. Journal of the Chinese Medical Association, 84(7), 718-721. https://doi.org/10.1097/jcma.0000000000000554

Lin, S., Shanafelt, T., & Asch, S. (2018). Reimagining clinical documentation with artificial intelligence. Mayo Clinic Proceedings, 93(5), 563-565. https://doi.org/10.1016/j.mayocp.2018.02.016

Mardi, Y. (2022). Electronic medical record as literature study. Proceeding International Conference on Medical Record, 2(1), 45-51. https://doi.org/10.47387/icmr.v2i1.154

Masarat, Ayat. (2024). 2. E-Health Implementation Challenges and HIS Evaluation in Accordance with EMRAM in Iran. Health technology assessment in action, doi: 10.18502/htaa.v8i2.15628

Mayer, A., Costa, C., & Righi, R. (2019). Electronic health records in a blockchain: a systematic review. Health Informatics Journal, 26(2), 1273-1288. https://doi.org/10.1177/1460458219866350

Meshkat, Y., Kodiyattu, Z., Engstrom, T., Chan, W., Mifsud, J., Pole, J., … & Sullivan, C. (2022). Understanding the digital disruption of health care: an ethnographic study of real-time multidisciplinary clinical behavior in a new digital hospital. Applied Clinical Informatics, 13(05), 1079-1091. https://doi.org/10.1055/s-0042-1758482

Muhammad, Izdihar, Sahalan., Fathi, Yusof., Hafiza, Abas. (2023). 6. The challenges of using blockchain technology for medical data in public hospitals in Malaysia. Open international journal of informatics, doi: 10.11113/oiji2018.6n1.277

Mumtaz, H. (2023). Current challenges and potential solutions to the use of digital health technologies in evidence generation: a narrative review. Frontiers in Digital Health, 5. https://doi.org/10.3389/fdgth.2023.1203945

Nahla, F., AL, Hamad., Jing-Chiou, Liou. (2022). 27. Current Cybersecurity Challenges of Applying Blockchain in Healthcare. doi: 10.1109/csci58124.2022.00305

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

Naresh, Kumar, Miryala., Divit, Gupta. (2023). 28. Data Security Challenges and Industry Trends. nternational journal of advanced research in computer and communication engineering, doi: 10.17148/ijarcce.2022.111160

Nasution, S. (2023). An analysis of effect job demand control-support and protection motivation on compliance in filling inpatient care medical record files at rsu eshmun medan. Cerdika Jurnal Ilmiah Indonesia, 3(6), 636-650. https://doi.org/10.59141/cerdika.v3i6.615

Natsiavas, P., Rasmussen, J., Voss-Knude, M., Votis, K., Coppolino, L., Campegiani, P., … & Komnios, I. (2018). Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Medical Informatics and Decision Making, 18(1). https://doi.org/10.1186/s12911-018-0664-0

Negro-Calduch, E., Azzopardi-Muscat, N., Krishnamurthy, R., & Novillo-Ortiz, D. (2021). Technological progress in electronic health record system optimization: systematic review of systematic literature reviews. International Journal of Medical Informatics, 152, 104507. https://doi.org/10.1016/j.ijmedinf.2021.104507

Nehama, Lewis., Yaron, Connelly., Gilead, Henkin., Max, Leibovich., Adi, Akavia. (2022). 18. Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records. Healthcare Informatics Research, doi: 10.4258/hir.2022.28.2.132

Nifakos, S., Chandramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., … & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

Onuogu, P. (2023). Benefits and challenges of adopting electronic medical records in nigerian federal capital territory hospitals-lessons learned. International Journal of Science and Research Archive, 10(1), 187-193. https://doi.org/10.30574/ijsra.2023.10.1.0734

Oshani, Seneviratne. (2023). 3. Enabling Data Interoperability for Decentralized, Smart, and Connected Health Applications. doi: 10.1145/3580252.3589433

Owoyemi, A., Osuchukwu, J., Azubuike, C., Ikpe, R., Nwachukwu, B., Akinde, C., … & Olaniran, S. (2022). Digital solutions for community and primary health workers: lessons from implementations in africa. Frontiers in Digital Health, 4. https://doi.org/10.3389/fdgth.2022.876957

P.Y.S., Lakshman., D.Priya, Kumar., N., Ramesh., K., Pranathi. (2021). 30. Medical Records Management Using Cloud Technology. doi: 10.1109/ICESC51422.2021.9532675

Patience, Onuogu. (2023). 10. Benefits and challenges of adopting Electronic Medical Records in Nigerian Federal Capital Territory Hospitals-lessons learned. International Journal of Science and Research Archive, doi: 10.30574/ijsra.2023.10.1.0734

Rachel, V., Rose., Abhay, Kumar., Joseph, S., Kass. (2023). 9. Protecting Privacy: Health Insurance Portability and Accountability Act of 1996, Twenty-First Century Cures Act, and Social Media.. Neurologic Clinics, doi: 10.1016/j.ncl.2023.03.007

Rahmatiqa, C., Abdillah, N., & Yuniko, F. (2020). Factors that cause compliance filling medical records in hospitals. International Journal of Community Medicine and Public Health, 7(10), 4180. https://doi.org/10.18203/2394-6040.ijcmph20204393

Rashmi, Agrawal., Kanchan, Patil. (2024). 31. Blockchain Technology for Medical Records Security Using Fit Viability Approach. doi: 10.1109/incacct61598.2024.10551119

Rigas, E. (2023). A hackathon as a tool to enhance research and practice on electronic health record systems' interoperability for chronic disease management and prevention. Frontiers in Digital Health, 5. https://doi.org/10.3389/fdgth.2023.1275711

S. Badsha, I. Vakilinia and S. Sengupta, "Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0708-0714, doi: 10.1109/CCWC.2019.8666477.

Salem, T., Argaw., Juan, Ramón, Troncoso-Pastoriza., Darren, Lacey., Marie-Valentine, Florin., Franck, Calcavecchia., Denise, Anderson., Wayne, Burleson., Jan-Michael, Vogel., Chana, O'Leary., Bruce, Eshaya-Chauvin., Antoine, Flahault. (2020). 24. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, doi: 10.1186/S12911-020-01161-7

Sanjaya, G. (2023). Analytical data for electronic medical records in primary health care. Bio Web of Conferences, 75, 05003. https://doi.org/10.1051/bioconf/20237505003

Sanjaya, G. (2023). Analytical data for electronic medical records in primary health care. Bio Web of Conferences, 75, 05003. https://doi.org/10.1051/bioconf/20237505003

Sanjaya, G. (2023). Digital capabilities of health workers to use electronic medical records: digital maturity self-assessment in indonesian hospitals. ihelis, 1(2), 52-62. https://doi.org/10.60074/ihelis.v1i2.43

Sanmorino, A. (2023). Emerging trends in cybersecurity for health technologies. Jurnal Ilmiah Informatika Global, 14(3), 76-81. https://doi.org/10.36982/jiig.v14i3.3530

Santoso, D. and Rokhman, N. (2022). Experience of electronic medical records adoption in primary health care in indonesia. Advances in Science and Technology. https://doi.org/10.4028/p-j260sd

Santoso, D., Fuad, A., Herwanto, G., & Maula, A. (2020). Blockchain technology implementation on medical records data management: a review of recent studies. Jurnal Riset Kesehatan, 9(2), 107-112. https://doi.org/10.31983/jrk.v9i2.5742

Scott, P., Curley, P., Williams, P., Linehan, I., & Shaha, S. (2016). Measuring the operational impact of digitized hospital records: a mixed methods study. BMC Medical Informatics and Decision Making, 16(1). https://doi.org/10.1186/s12911-016-0380-6

Semyonov, A. (2023). Digital health information systems in the member states of the commonwealth of independent states: status and prospects. Digital, 3(3), 189-199. https://doi.org/10.3390/digital3030013

Steinhauser, S. and Raptis, G. (2023). Design propositions for nudging in healthcare: adoption of national electronic health record systems. Digital Health, 9, 205520762311812. https://doi.org/10.1177/20552076231181208

Susan, J, Oudbier., B, Chen., Britney, S, J, Chen., Kirsten, A., Ziesemer., Susan, J, Oudbier., Ellen, M.A., Smets. (2024). 12. Implementation barriers and facilitators of remote monitoring, remote consultation and digital care platforms through the eyes of healthcare professionals: a review of reviews. BMJ Open, doi: 10.1136/bmjopen-2023-075833

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023

T., Sujithra. (2022). 20. Swift and Secure Medical Data Transaction. doi: 10.1007/978-981-19-1018-0_19

Taki, M. (2023). An analysis of digital records and their juridical ramifications: bangladesh perspective. Beijing Law Review, 14(04), 1930-1940. https://doi.org/10.4236/blr.2023.144106

Tapuria, A., Porat, T., Kalra, D., D'souza, G., Sun, X., & Ćurčin, V. (2021). Impact of patient access to their electronic health record: systematic review. Informatics for Health and Social Care, 46(2), 194-206. https://doi.org/10.1080/17538157.2021.1879810

Tapuria, A., Porat, T., Kalra, D., D'souza, G., Sun, X., & Ćurčin, V. (2021). Impact of patient access to their electronic health record: systematic review. Informatics for Health and Social Care, 46(2), 194-206. https://doi.org/10.1080/17538157.2021.1879810

Tilaar, T. (2023). Review of electronic medical records in indonesia and its developments based on legal regulations in indonesia and its harmonization with electronic health records (manual for developing countries). Daengku Journal of Humanities and Social Sciences Innovation, 3(3), 422-430. https://doi.org/10.35877/454ri.daengku1662

Utkarsh, Shrivastava., Jiahe, Song., Bernard, T., Han., Doug, Dietzman. (2021). 15. Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation.. International Journal of Medical Informatics, doi: 10.1016/J.IJMEDINF.2021.104401

Uwizeyemungu, S., Poba-Nzaou, P., & Cantinotti, M. (2019). European hospitals' transition toward fully electronic-based systems: do information technology security and privacy practices follow?. Jmir Medical Informatics, 7(1), e11211. https://doi.org/10.2196/11211

Vazirani, A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing blockchains for efficient health care: systematic review. Journal of Medical Internet Research, 21(2), e12439. https://doi.org/10.2196/12439

Venkatesh, Janarthanan., S., Kumaran, M., Ninad, V, Nagrale., O., G., Singh., Karthi, Vignesh, Raj. (2024). 5. Legal and Ethical Issues Associated With Challenges in the Implementation of the Electronic Medical Record System and Its Current Laws in India. Cureus, doi: 10.7759/cureus.56518

Wardhana, E., Suryono, S., Hernawan, A., & Nugroho, L. (2022). Evaluation of format and security of dental electronic medical record systems in general hospital based on legislation. Odonto Dental Journal, 9, 80. https://doi.org/10.30659/odj.9.0.80-89

Wasinee, Noonpakdee., Acharaphun, Phothichai., Thitiporn, Khunkornsiri. (2019). 32. Challenges of Big Data Implementation in a Public Hospital. doi: 10.1109/WOCC.2019.8770562

Widiyanto, W. (2023). Analysis of readiness for implementation of electronic medical records using doq-it method. International Journal of Computer and Information System (Ijcis), 4(4), 158-164. https://doi.org/10.29040/ijcis.v4i4.146

Wisnu, Uriawan., Sumitra, Adriansyah., Siti, Jahro, Maulidiyah., Stefanus, Julianto., Wildan, Sophal, Jamil. (2024). 19. Challenges and Opportunities: Improve Patient Data Security and Privacy in Distributed Systems. doi: 10.20944/preprints202407.0163.v1

Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. HEM, 4(4), 17-27. https://doi.org/10.61093/hem.2023.4-02

Yaping, Yang., Wei, Zhang. (2022). 25. Research on digital medical data security protection technology. doi: 10.1117/12.2636600

Yasir, Hamid., Rameez, Yousuf. (2023). 21. Security in Health Information Management Records through Blockchain Technology. Journal of Information Security and Cybercrimes Research, doi: 10.26735/qbij3667

Yi, M. (2018). Major issues in adoption of electronic health records. Journal of Digital Information Management, 16(4), 180. https://doi.org/10.6025/jdim/2018/16/4/180-191

Received Agustus 15, 2023; Revised Agustus 30, 2023; Accepted September 15, 2023; Published September 17, 2023