Research Article

Improving Healthcare Patient Data Security: An Integrated Framework Model For Electronic Health Records From A Legal Perspective

Ahdiana Yuni Lestari[1*], Misran[2], Trisno Raharjo[3], Muhammad Annas[4] , Dinda Riskanita[5] , Adya Paramita Prabandari[6]

[1]Faculty of Law, Universitas Muhammadiyah Yogyakarta, Indonesia
[2]Faculty of Social and Political Sciences, Universitas Gadjah Mada, Indonesia
[3]Postgraduate, Universitas Muhammadiyah Yogyakarta, Indonesia
[4]Department of Law, Universidad Carlos III de Madrid, Spain
[5]Faculty of Business and Human Sciences, Universitas Siber Muhammadiyah, Indonesia
[6]Faculty of Law, Universitas Diponegoro, Indonesia
[*]ahdianayunilestari@umy.ac.id

ABSTRACT

This study aims to critically examine the legal responsibilities of healthcare facilities in Indonesia regarding the protection of patient data within Electronic Medical Records (EMR). The research employs a mixed-method approach, combining normative legal analysis with empirical data collection from healthcare facilities to assess the implementation of data protection regulations. The findings reveal significant gaps in the enforcement of Minister of Health Regulation Number 24 of 2022 and Law Number 27 of 2022 concerning Personal Data Protection, particularly in smaller clinics and independent practices. These facilities often lack the technical infrastructure and resources required to meet regulatory standards, resulting in inconsistencies in data protection and a higher incidence of data breaches. The study introduces the Integrated Security and Usability Framework for Electronic Medical Records (ISU-EMR), which combines the principles of the Confidentiality, Integrity, and Availability (CIA) Triad with Human-Computer Interaction (HCI) Theory. This framework addresses both the technical and human factors contributing to data breaches, offering a balanced solution for enhancing data protection while maintaining usability in EMR systems. The implications of this research extend to both theory and practice, providing a new model for data protection in healthcare that can be adapted to various settings.

Keywords: Electronic Medical Records; Data Protection; Healthcare Facilities; CIA Triad; Human-Computer Interaction; Indonesia.

A. INTRODUCTION

The accelerated digitization of healthcare services in Indonesia has led to notable advancements as well as challenges, particularly in the area of patient data protection (Abhishek, Tripathy, & Mishra, 2022; Firmansyah, Mantoro, & Persadha, 2022). The integration of Electronic Medical Records (EMR) was intended to enhance patient care by facilitating access to medical histories, optimizing healthcare delivery efficiency, and reducing the potential for errors associated with paper-based records (Vimalachandran, Wang, & Zhang, 2015). However, the transition to EMR has also exposed significant weaknesses in data security, as demonstrated by numerous high-profile data breaches in recent years

(Adamu, Hamzah, & Rosli, 2020). These incidents underscore the urgent need for a thorough examination of the current frameworks and practices governing patient data protection in Indonesia.

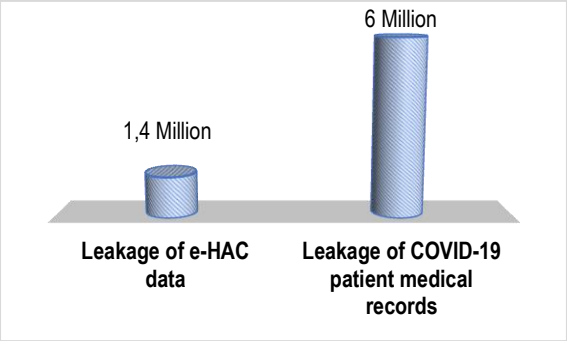

Figure 1. Types and Number of Health Data Leaks in Indonesia (a compilation from various sources by the author)

In 2021, one of the most alarming data breaches occurred when the Electronic Health Alert Card (e-HAC) system was compromised (Kristanto, 2023), leading to the leakage of 1.4 million records (Solehudin & Ruhaeni, 2022). This incident demonstrated the vulnerability of even ostensibly secure systems to unauthorized access. The situation worsened in 2022 when 6 million records of COVID-19-infected patients were illicitly obtained from the Ministry of Health's system and subsequently sold on the online marketplace Raid Forums (Noor & Darmaningrat, 2023). The breach involved the dissemination of highly sensitive information, including medical images, laboratory results, and other personal data, which has profound implications for patient privacy and trust in the healthcare system.

These incidents have exposed considerable shortcomings in the current data protection tools within Indonesia's healthcare system. Although a regulatory framework exists—such as Minister of Health Regulation (PERMENKES) No. 24 of 2022 on Medical Records and Law No. 27 of 2022 on Personal Data Protection, as well as Law No. 17 of 2023 on Health, Government Regulation No. 28 of 2024 on the Implementation of Law No. 17 of 2023, and PERMENKES No. 24 of 2024 on Medical Records—these measures appear inadequate for preventing large-scale breaches. The responsibility for protecting patient data falls primarily on healthcare institutions, which are legally obliged to prevent the loss, damage, or unauthorized access to medical records. However, the recurring data breaches suggest that these institutions may lack the necessary resources, training, or infrastructure to effectively safeguard patient information.

Despite extensive research on EMR and data security in Indonesia, significant gaps remain in understanding the root causes of data breaches and the effectiveness of current protective measures (Januarita, Alamsyah, & Perdana, 2024). Previous studies have primarily focused on the technical aspects of EMR implementation, such as system architecture and data storage solutions, without sufficiently addressing the human factors contributing to security lapses (Larson & Alexander, 2021). Moreover, while there is a growing body of

literature on the legal implications of data breaches, there is a paucity of studies critically analyzing the intersection of technological vulnerabilities and regulatory shortcomings in the Indonesian context (Sudarwanto & Kharisma, 2022).

This study aims to address these shortcomings by providing a comprehensive analysis of patient data protection in the context of EMR implementation in Indonesia. Unlike previous research, which often treats data breaches as isolated incidents, this study will examine the systemic issues that contribute to these breaches, including both technological vulnerabilities and the adequacy of legal protections. The objective is to offer a more holistic understanding of the challenges healthcare providers face in protecting patient data.

In addition to examining the technological and legal aspects of EMR-related data breaches, this research will explore the human factors that play a critical role in data security. It is well documented that human error significantly contributes to data breaches. However, this aspect has been underexplored in the context of Indonesian healthcare. By investigating the role of training, awareness, and institutional culture in preventing data breaches, this study aims to offer practical recommendations for mitigating these risks.

Moreover, this study will critically examine the existing legal frameworks governing the protection of patient data in Indonesia. Although regulations such as the Personal Data Protection Law No. 27 of 2022 provide a legal foundation for data security, their implementation and enforcement remain inconsistent. This research will evaluate the efficacy of these regulations in practice and identify any regulatory gaps that contribute to the persistence of data breaches.

The value of this research lies in its potential to inform policy and practice regarding the protection of patient data in Indonesia. By providing a comprehensive examination of the technological and human factors that contribute to data breaches, this study will offer valuable insights for healthcare providers, policymakers, and regulators. It is anticipated that the findings will help in formulating more robust and effective data protection strategies, ensuring that the benefits of EMR are not realized at the expense of patient privacy and trust.

While the adoption of EMR represents significant progress in Indonesia's healthcare system, it also introduces new challenges related to data security that require urgent attention. This research aims to bridge the gap between technological innovation and data protection, offering comprehensive recommendations to strengthen the security of patient information in the digital age. Through a thorough examination of current practices, legal frameworks, and human factors, this study seeks to contribute to the development of a more secure and reliable healthcare system in Indonesia.

Information security is a critical component in the management of EMR. Its theoretical foundations are essential for understanding the complexities of data protection in healthcare (Kapila & Pillai, 2023; Mahfuth, Dillon, & Drus, 2016; Sharma, Bir, & Prakash, 2024; Sher et al., 2017; Yeng et al., 2021). The Confidentiality, Integrity, and Availability (CIA) Triad is a widely accepted framework in information security (Al-Far, Qusef, & Almajali, 2018; Azadi, Zare, & Zare, 2018; Cybenko & Hughes, 2014; Howard et al., 2023; Wang et al., 2023). It ensures that data is protected against unauthorized access (confidentiality), remains accurate and unaltered (integrity), and is accessible when needed by authorized personnel (availability). In the healthcare sector, these principles are particularly important due to the sensitive nature of patient data (Chakraborty & Rathi, 2021). The CIA Triad provides a foundation for assessing the security protocols implemented within EMR systems, guiding the development of strategies to mitigate the risks associated with data breaches (Kang, Fahd, & Venkatraman, 2018).

In addition to the technical aspects, the human element plays a significant role in information security, particularly within the healthcare environment, where the interaction between healthcare professionals and technology is frequent and complex. Human-Computer Interaction (HCI) Theory examines how users interact with EMR systems, highlighting the importance of user-friendly designs that reduce the likelihood of errors and enhance security (Helou et al., 2019; Price et al., 2015). This theory posits that poorly designed interfaces can lead to user errors, which are a major cause of data breaches (Ardito et al., 2019; Naqvi & Seffah, 2019; Winckler et al., 2017). Applying HCI principles enables healthcare institutions to better understand the relationship between user behavior and data security (Fischer-Hübner, Pettersson, & Angulo, 2015; Humaidi, Balakrishnan, & Shahrom, 2014; Shahri & Mohanna, 2016). This, in turn, facilitates the development of more effective training programs and system designs that can reduce the likelihood of human error contributing to data breaches.

The protection of patient data within electronic medical records is not merely a technical challenge; it is also a legal obligation governed by multiple regulatory frameworks (Bhardwaj & Kumar, 2021; Patel, Patel, & Parikh, 2020; Vaishnavi, Sam Nithish, & Parvathi, 2024; Xiang, Cao, & Fan, 2022). Compliance theory is crucial for understanding how healthcare institutions adhere to the legal and regulatory frameworks that mandate the protection of patient data (Almuwail et al., 2023; Essefi et al., 2021; Marotta & Madnick, 2022; Obeng & Paul, 2019). This theory suggests that compliance is driven by the need to align with legal requirements, institutional policies, and societal expectations (Kuiper et al., 2023; Peat, Fikfak, & Van Der Zee, 2022). In Indonesia, regulations such as PERMENKES No. 24 of 2022 and the Personal

Data Protection Law No. 27 of 2022 outline the specific responsibilities of healthcare providers concerning the safeguarding of patient data. However, the effectiveness of these regulations depends on their comprehension, implementation, and enforcement within healthcare institutions.

In addition to the aforementioned regulatory frameworks, the Theory of Planned Behavior provides insights into the psychological factors that influence healthcare professionals' compliance with data protection regulations (Foth, 2016; Zoghlami, Ayeb, & Rached, 2021). This theory posits that a healthcare provider's behavior is influenced by three key factors: their attitudes toward the regulations, perceived social pressures (subjective norms), and perceived control over compliance-related actions (Bastani, Javanbakht, & Ravangard, 2019; Widianto et al., 2021; Zielińska-Tomczak et al., 2021). For instance, if healthcare providers believe that following data protection protocols is crucial and that their colleagues also adhere to these standards, they are more likely to comply (Georgiou & Lambrinoudakis, 2021). Understanding these psychological factors is essential for developing targeted interventions that promote compliance, such as modifying institutional policies to make adherence more achievable and straightforward (Lawelai, Iswanto, & Raharja, 2023). This approach helps bridge the gap between legal mandates and actual practice, ensuring that regulatory frameworks effectively protect patient data in real-world settings.

This research differs from previous studies, such as those that focus on the situation and problems surrounding health data breaches in government-owned applications in Indonesia (Gunawan et al., 2022), or those that examine the judicial review of the increase in BPJS premiums based on the principle of justice in healthcare and social security policies (Syahputra & Munandar, 2021). Other research analyzes personal data protection regulations in the health sector from a comparative legal perspective between Indonesia, Singapore, and the European Union (Kharisma & Diakanza, 2024). Additionally, some studies explore the interplay between information and communication technologies (ICTs) and the right to informational privacy in healthcare, examining the legal and ethical aspects of maintaining confidentiality and the security of personal health information (Jose, 2023). Another line of research focuses on designing and testing systems that allow the sharing of patient data while addressing privacy concerns, such as a digital information system that restricts access to patient data unless approved by the patient's mobile device (Zalloum, Mutaz, Alamleh, & Hosam, 2020).

B. RESEARCH METHODS

1. Types of Research

This research employs a combination of normative and empirical legal research (Hamzani et al., 2024; van Boom, Desmet, & Mascini, 2018) to explore the protection of patient data in the context of EMR implementation in Indonesia.

Normative legal research involves the analysis of legal norms, principles, and standards derived from various sources, including legislation, regulatory frameworks, judicial decisions, contractual agreements, and legal doctrines (Mukhachev, Gondarenko, & Gryaznov, 2022). This examination focuses on how these legal frameworks regulate the protection of patient data and the responsibilities of healthcare institutions. On the other hand, empirical legal research involves the collection and analysis of primary data obtained directly from the field, offering insights into the practical application of legal norms within healthcare settings. This dual approach provides a comprehensive understanding of both the theoretical foundations and practical implications of patient data protection in the context of digital healthcare.

2. Data Sources

The data sources for this study include both secondary and primary data. Secondary data are derived from a comprehensive literature review (Cole, Friedlander, & Trinh, 2018; Santos, Santos, & De Mendonça, 2015), including primary legal materials such as legislation and regulations directly related to the protection of patient data. The study examines key regulations, including Law Number 27 of 2022 concerning Personal Data Protection, Law Number 29 of 2004 concerning Medical Practice, and Minister of Health Regulation Number 24 of 2022 regarding Medical Records. Additionally, secondary legal materials, such as books, journal articles, and research reports on the management of EMR, are analyzed. Tertiary materials, such as legal dictionaries and non-legal resources (e.g., books and research on medical records management from non-legal perspectives), provide supplementary context. Primary data are collected through direct interviews with key informants involved in EMR management, including healthcare professionals and administrators from Firdaus 24 Hours Clinic in Yogyakarta.

3. Data Collection Techniques

This study employs a two-pronged approach to data collection, combining a literature review with fieldwork (Costa et al., 2023). Secondary data are obtained through an extensive literature review, systematically collecting and analyzing relevant laws, regulations, legal documents, books, and research papers (Cairo, Olivares, & Peralta, 2024; Solihin et al., 2021; Williams, 2020). The primary objective is to identify and extract legal norms and rules related to the protection of patient data within EMR systems. Secondary legal materials, including academic publications and previous research, are also examined to extract relevant theories and findings that inform the research. Concurrently, primary data are gathered through structured interviews with healthcare professionals who have direct experience implementing EMR. These interviews provide practical insights into the challenges and realities of managing patient data within digital systems,

offering valuable context to the theoretical analysis of legal frameworks.

4. Data Analysis

The data analysis uses a descriptive-analytical approach, methodically organizing and presenting data obtained from both secondary and primary sources (Avila-Barrientos, 2020). The analysis begins with a comprehensive examination of the legal frameworks governing medical records in Indonesia, with a focus on how these regulations are applied in the context of EMR. The study then compares the practical implementation of EMR at Firdaus 24 Hours Clinic with the standards set forth in Minister of Health Regulation Number 24 of 2022. This comparison assesses whether the clinic's practices align with or exceed legal requirements. The analysis aims to identify discrepancies between regulatory intent and practical application, providing a basis for recommendations to enhance the protection of patient data in Indonesia's healthcare system.

C. RESULTS AND DISCUSSION

1. Legal Responsibility of Healthcare Facilities in Protecting Patient Medical Records

The safeguarding of patient data, particularly within electronic medical records (EMR), is a pivotal aspect of healthcare service delivery that has garnered heightened attention in recent years (Keshta & Odeh, 2021). The rapid digitization of healthcare services in Indonesia has introduced several significant challenges regarding the confidentiality, integrity, and availability of patient data (Fuad et al., 2019). According to the stipulations set forth in Law Number 36 of 2009 concerning Health, healthcare facilities in Indonesia are legally bound to provide safe, comprehensive, and non-discriminatory services. This legislation explicitly delineates the government's obligation to ensure the availability and accessibility of healthcare services, which inherently encompasses the protection of patient data (Njotini, 2018). However, the legal responsibility of healthcare facilities extends beyond the mere provision of services to include the safeguarding of sensitive patient information. The Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records categorizes electronic medical records as a critical subsystem within the broader healthcare information system. This regulation mandates the implementation of EMR across all healthcare facilities, including hospitals, clinics, and independent practices. Therefore, these facilities must develop and adhere to rigorous operational procedures aimed at safeguarding patient data, underscoring the paramount importance of maintaining data security at all levels of healthcare delivery (Mbonihankuye et al., 2019). Nevertheless, the prevalence of data breaches in the healthcare sector indicates substantial deficiencies in implementing and enforcing these regulations. Such breaches not only compromise patients' privacy but also erode public trust in the healthcare system.

The responsibility for ensuring the security of electronic medical records (EMR) falls primarily on healthcare facilities, which are obligated to guarantee the integrity of their electronic systems, enforce rigorous operational procedures, and address any breaches promptly and effectively (Hwang & Lin, 2020). The regulations stipulate that healthcare facilities must implement comprehensive data protection measures, including developing secure electronic systems, conducting regular audits, and providing training for healthcare workers. However, the efficacy of these measures is often constrained by insufficient resources, a lack of awareness, and the complexity of managing vast quantities of sensitive data. This section critically examines the extent to which healthcare facilities are meeting their legal responsibilities and identifies the key challenges they face in doing so.

One of the most significant challenges identified is the inadequate technical infrastructure and expertise within healthcare facilities, particularly in smaller clinics and independent practices (Kesale & Swai, 2023). Many of these facilities encounter difficulties in implementing the sophisticated security measures necessary to ensure the effective protection of EMR. The absence of a unified, standardized approach to data protection across diverse healthcare facilities further complicates the issue, resulting in inconsistencies in the management and protection of patient data. Furthermore, the accelerated rate of technological advancement necessitates that healthcare facilities regularly update their systems and procedures to remain aligned with evolving security threats. This requires sustained investment in technology and training, which can prove burdensome for smaller facilities.

Another critical issue is the role of human error in the occurrence of data breaches. Despite the implementation of optimal technical safeguards, the actions of healthcare workers, whether intentional or unintentional, can lead to substantial data breaches (Yeo & Banfield, 2022). The Minister of Health's regulation underscores the necessity of training healthcare professionals in data protection; however, in practice, this is often overlooked or inadequate. A significant number of healthcare workers lack the requisite training in data protection, resulting in errors such as the improper handling of patient information, inadequate utilization of security features, and non-compliance with established protocols. These human factors represent a significant vulnerability in the protection of patient data and require immediate attention.

2. Global and Comparative Perspectives on Patient Data Protection

The protection of patient data is not an isolated issue confined to Indonesia; rather, it is a global concern that has garnered significant attention in the international community. The growing digitization of healthcare services worldwide has prompted the implementation of rigorous data protection regulations in numerous

countries, with the objective of safeguarding patient information and preventing data breaches (Jones, 2022). The European Union's General Data Protection Regulation (GDPR) represents one of the most comprehensive legal frameworks in this regard. The GDPR establishes rigorous standards for data protection, including the necessity for explicit consent from patients for the utilization of their data, the implementation of robust technical and organizational measures to safeguard data (Padrão, Ribeiro, & Lopes, 2024), and the provision of transparent guidelines for reporting and handling data breaches.

In comparison, the Indonesian legal framework for data protection, while evolving, still exhibits significant deficiencies. The Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records and Law Number 27 of 2022 concerning Personal Data Protection represent significant advancements; yet, they lack the comprehensive rigor and robust enforcement mechanisms observed in the GDPR. For example, the GDPR stipulates that any data breach must be reported within 72 hours, with severe penalties for non-compliance. In contrast, the enforcement of data protection regulations in Indonesia is often inconsistent, with numerous healthcare facilities failing to report breaches or implement the requisite safeguards to prevent them.

A comparative analysis with other countries that have successfully implemented robust data protection measures can provide valuable insights for Indonesia. The United States has implemented the Health Insurance Portability and Accountability Act (HIPAA), which includes specific provisions for the security and privacy of health data (Schulman, 2006). HIPAA mandates that healthcare providers implement physical, technical, and administrative safeguards to protect patient information (Cheng & Hung, 2006). Furthermore, HIPAA imposes significant penalties for breaches of these requirements. Adopting comparable standards in Indonesia would be advantageous, particularly regarding the enforcement of compliance and the provision of more explicit directives to healthcare facilities on the safeguarding of patient data.

Furthermore, the incorporation of global best practices into Indonesia's data protection framework could assist in addressing some of the challenges currently faced by healthcare facilities. For example, the GDPR places significant emphasis on data minimization, which requires that only the minimum necessary amount of patient data be collected and processed (Shanmugam et al., 2022). This principle could prove valuable in the context of Indonesian regulations, as it mitigates the risk of data breaches by limiting the amount of sensitive information that could be compromised. Additionally, the GDPR's stipulation that regular data protection impact assessments be conducted could be adopted in Indonesia to assist healthcare facilities in identifying and mitigating potential risks before they result in breaches.

Nevertheless, implementing these global best practices in Indonesia necessitates a meticulous examination of the local context. The diversity of healthcare facilities in Indonesia, which ranges from large, well-resourced hospitals to small, rural clinics, indicates that a one-size-fits-all approach is ineffective (Diana, Hollingworth, & Marks, 2015). Instead, Indonesia must develop a flexible, scalable framework that can be adapted to the specific needs and capabilities of various types of healthcare facilities (Suwantika et al., 2023). This will require collaboration between the government, healthcare providers, and other stakeholders to develop guidelines and support mechanisms that can assist all healthcare facilities, regardless of size or location, in effectively protecting patient data.

3. Proposed Model: Integrated Security and Usability Framework for Electronic Medical Records

The previous theoretical frameworks in the realm of EMR often focused heavily on either security or usability but rarely on the integration of both (Hausawi & Allen, 2015; Horcher & Tejay, 2013; Kumar et al., 2020; Naqvi, Clarke, & Porras, 2020). The CIA Triad is a cornerstone of information security, emphasizing the need for data confidentiality, integrity, and availability (Cybenko & Hughes, 2014; Howard et al., 2023; Sumra, Hasbullah, & AbManan, 2015; Wang et al., 2023). However, it tends to overlook the human factors that can undermine these security principles, particularly in complex environments like healthcare. On the other hand, HCI Theory primarily addresses the usability of systems but often underestimates the importance of embedding robust security measures within user interfaces (Al-Jawarneh & Mohammed, 2022; Ardito et al., 2019; Gamundani, 2023; Winckler et al., 2017; Zhang & Luximon, 2021). These limitations highlight a gap in existing models, where the interplay between security and usability is not adequately addressed, leading to vulnerabilities in EMR that can result in data breaches and operational inefficiencies.

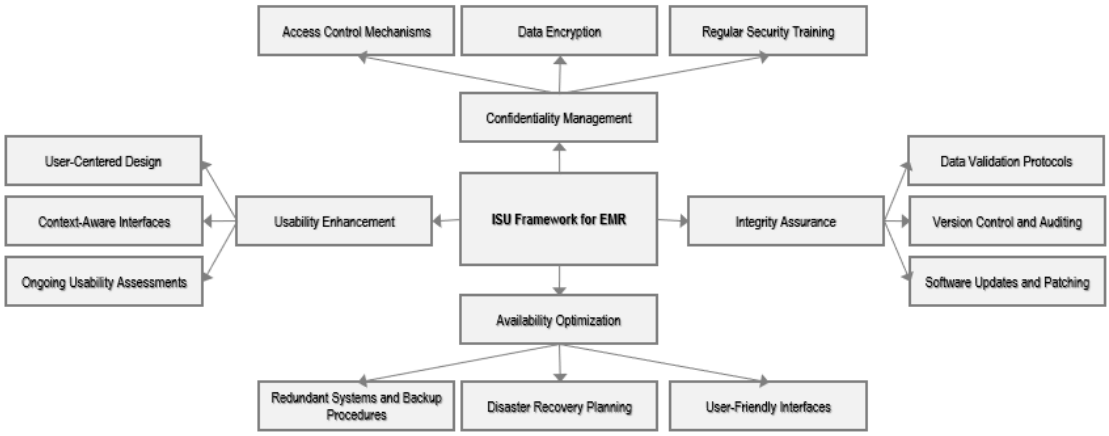

Figure 2. New Model of Framework to Integrated Security and Usability for Electronic Medical Records (a compilation from various sources by the author)

To bridge this gap, there is a pressing need for a comprehensive framework that not only secures patient data but also ensures that the systems are user-friendly and aligned with the workflows of healthcare professionals. The proposed model, the Integrated Security and Usability Framework for Electronic Medical Records (ISU-EMR), addresses this need by integrating the key elements of the CIA Triad with Human-Computer Interaction (HCI) principles. This holistic approach ensures that the protection of patient data is not compromised by poor usability and vice versa, thus providing a balanced solution to the challenges faced by healthcare facilities in managing EMR.

The ISU-EMR Framework, depicted in the diagram, is a strategic model designed to enhance both the security and usability of electronic medical records. The central element of the framework is the ISU Framework for EMR, which integrates four main components: Confidentiality Management, Integrity Assurance, Availability Optimization, and Usability Enhancement. These components are interconnected, ensuring that the EMR system is robust, secure, and user-friendly.

Each component of the framework branches out into specific actions or elements that contribute to the overall effectiveness of the system. For example, Confidentiality Management involves access control mechanisms, data encryption, and regular security training to ensure that patient data is protected from unauthorized access. Integrity Assurance focuses on maintaining the accuracy and consistency of data through data validation protocols, version control and auditing, and software updates and patching (Kalaiselvi & Sumathi, 2023). Availability Optimization ensures that the system remains operational and accessible through redundant systems and backup procedures, disaster recovery planning, and user-friendly interfaces. Lastly, Usability Enhancement incorporates user-centered design, context-aware interfaces, and ongoing usability assessments to ensure that the system meets the needs of healthcare professionals, thereby reducing the likelihood of errors that could compromise security.

This model is novel in its approach as it not only addresses the technical aspects of EMR security but also emphasizes the importance of user interaction with the system. By balancing these elements, the ISU-EMR Framework ensures that healthcare facilities can protect patient data effectively while also improving the efficiency and effectiveness of their EMR systems. This integration of security and usability is critical for modern healthcare environments, where both elements are essential for delivering high-quality care.

4. Challenges and Recommendations for Strengthening Data Protection in Indonesia

The recurrent occurrence of data breaches in Indonesian healthcare facilities (Kharisma & Diakanza, 2024) underscores the necessity of

addressing several pivotal challenges to reinforce the protection of patient data. These challenges include the lack of enforcement of existing regulations, inadequate training for healthcare workers, and the need for enhanced technical infrastructure to safeguard electronic medical records. Furthermore, the growing complexity of cyber threats necessitates that healthcare facilities maintain a dynamic approach to updating security protocols to effectively mitigate the risk of potential breaches.

One of the most urgent issues is the lack of uniformity in the enforcement of data protection regulations across diverse types of healthcare facilities (Natamiharja & Setiawan, 2024). While larger hospitals may possess the resources to implement comprehensive data protection measures, smaller clinics and independent practices often lack the financial and technical capacity to do so. This discrepancy gives rise to considerable vulnerabilities in the broader healthcare system, as data breaches in smaller facilities can still have far-reaching consequences, particularly when patient data is shared across networks or integrated into larger systems. To address this challenge, it is imperative that the government provides targeted support (Lawelai, 2023) to smaller healthcare facilities. This support should include funding for technical upgrades, training programs, and access to centralized resources that can help them meet regulatory requirements.

Another significant challenge is the insufficient training and awareness among healthcare professionals regarding data protection (Dhamanti et al., 2021). Notwithstanding the existence of regulations mandating data security practices, the actual implementation of these practices often falls short due to a lack of understanding or awareness among staff. For example, healthcare workers may unintentionally disseminate patient information via insecure channels, use inadequate passwords, or neglect to log out of systems after use. Such human errors can be as, if not more, dangerous than technological vulnerabilities, given that they are often more difficult to detect and prevent (Stark et al., 2021). To mitigate this risk, healthcare facilities must implement regular, mandatory training programs that educate staff on the importance of data protection, the specific risks involved, and the best practices they should follow.

The growing complexity and sophistication of cyber threats also present a considerable challenge to data protection in healthcare (Mahajan et al., 2022). The ever-changing landscape of cybercrime poses a significant challenge for healthcare facilities, as cybercriminals continually develop new methods to bypass security systems. To effectively mitigate these risks, healthcare facilities must prioritize continuous monitoring, regular updates to security protocols, and investment in advanced cybersecurity tools. However, many healthcare

facilities, particularly those in rural or under-resourced areas, may lack the necessary expertise or budget to implement these measures effectively (Assan et al., 2009). This creates a gap in the healthcare system's overall cybersecurity defense, as attackers may exploit the weakest links.

D. CONCLUSION

The findings of this research reveal significant gaps in the legal responsibilities of healthcare facilities in Indonesia regarding the protection of patient data within electronic medical records (EMR). While the legal framework, particularly the Regulation of the Minister of Health Number 24 of 2022 and Law Number 27 of 2022 concerning Personal Data Protection, sets forth clear mandates for safeguarding patient information, the implementation of these regulations remains inconsistent across various healthcare settings. Smaller clinics and independent practices, in particular, face challenges in meeting stringent requirements due to inadequate technical infrastructure and limited resources. Furthermore, the persistent occurrence of data breaches highlights the critical role of human error, which remains a significant vulnerability in data protection efforts.

The implications of this study extend both theoretically and practically. Theoretically, this research contributes to the ongoing discourse on the integration of security and usability in healthcare systems by proposing the Integrated Security and Usability Framework for Electronic Medical Records (ISU-EMR). This framework effectively bridges the gap between the technical aspects of data protection, as emphasized by the CIA Triad, and the user-centered focus of Human-Computer Interaction (HCI) Theory. The ISU-EMR model provides a balanced approach that addresses the dual challenges of safeguarding patient data while ensuring that EMR systems are accessible and user-friendly for healthcare professionals.

Practically, the ISU-EMR framework offers a strategic guide for healthcare facilities in Indonesia to enhance their data protection measures. By adopting this model, healthcare providers can implement comprehensive data security protocols that are integrated with user-friendly interfaces, thereby reducing the risk of data breaches caused by both technological vulnerabilities and human errors. The model also underscores the importance of continuous training for healthcare workers, regular system audits, and the implementation of advanced cybersecurity tools to address the evolving nature of cyber threats. For policymakers, this research provides insights into the need for targeted support for smaller healthcare facilities, including financial assistance and access to centralized resources, to ensure uniform compliance with data protection regulations.

However, this study is not without its limitations. The primary limitation lies in the scope of the research, which focuses predominantly on

the Indonesian healthcare context. While the findings and proposed framework are relevant to the challenges faced by Indonesian healthcare facilities, further research is needed to validate the applicability of the ISU-EMR model in other regions with different healthcare systems and regulatory environments. Additionally, the study's reliance on existing literature and theoretical frameworks may limit the generalizability of the findings, as real-world implementation could present unforeseen challenges. Future research should explore the practical application of the ISU-EMR framework in diverse healthcare settings and examine the long-term effectiveness of the proposed strategies in enhancing data protection.

REFERENCES

JOURNALS

Abhishek., Tripathy, Hrudara Kumar., & Mishra, Sushruta. (2022). A Succinct Analytical Study of the Usability of Encryption Methods in Healthcare Data Security. *Studies in Computational Intelligence*, Vol. 1039,pp.105–120. https://doi.org/10.1007/978-981-19-2416-3_7

Adamu, Jibril., Hamzah, Raseeda., & Rosli, Marshima Mohd. (2020). Security issues and framework of electronic medical record: A review. *Bulletin of Electrical Engineering and Informatics*, Vol.9, No.2), pp.565–572. https://doi.org/10.11591/eei.v9i2.2064

Almuwail, Khalil Ibrahim., Albarrak, Abdulaziz Saad., Bhutta, Muhammad Nasir Mumtaz., & Wahsheh, Heider A. M. (2023). Examining the Factors for Non-Compliance of Saudi Health Organizations for E-Health Security and Privacy. *Journal of Theoretical and Applied Information Technology*, Vol.101,(No.2),pp.435–447. https://www.jatit.org/volumes/Vol101No2/5Vol101No2.pdf

Assan, Joseph K., Assan, Samuel K., Assan, Nicole., & Smith, Lauren. (2009). Health inequality in resource poor environments and the pursuit of the MDGs: Traditional versus modern healthcare in rural Indonesia. *Journal of Health Management*, Vol.11,(No.1),pp.93–108. https://doi.org/10.1177/097206340901100107

Avila-Barrientos, Eder. (2020). Analysis of the principles for the description of research data by datacite metadata schema. *Anales de Documentacion*,Vol.23,(No.1),pp.1–14. https://doi.org/10.6018/analesdoc.400341

Bastani, Peivand., Javanbakht, Mahnaz., & Ravangard, Ramin. (2019). Predicting the Potential Patients' Intention to Select Healthcare Service Providers: Application of Structural Equation Modeling Based on the Theory of Planned Behavior. *Open Public Health Journal*, Vol.12, (No.1), pp.472–481. https://doi.org/10.2174/ 18749 44501912010472

Bhardwaj, Aashish., & Kumar, Vikas. (2021). Electronic healthcare records: Indian vs. International perspective on standards and privacy. *International Journal of Service Science, Management, Engineering, and Technology*,Vol.12,(No.2),pp.44–58. https://doi.org/10.4018/IJSSMET.2021030103

Cairo, Vladimir Rodriguez., Olivares, Percy Antonio Vilchez., & Peralta, Ena Cecilia Obando. (2024). Systematic review of scientific literature applied to legal research. *Revista Pedagogia Universitaria y Didactica del Derecho*, Vol.11, (No.1), pp.63–91. https://doi.org/10.5354/0719-5885.2024. 70653

Chakraborty, Chinmay., & Rathi, Megha. (2021). Chapter 2-Smart healthcare systems using big data. *Demystifying Big Data, Machine Learning, and Deep Learning for Healthcare Analytics*, pp.17–32. https://doi.org/10.1016/B978-0-12-821633-0.00009-X

Cheng, Vivying S. Y., & Hung, Patrick C. K. (2006). Health Insurance Portability and Accountability Act (HIPPA) Compliant Access Control Model for Web Services. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*,Vol.1,(No.1),p.18.https://doi.org/10.4018/jhisi.2006010102

Cole, Alexander P., Friedlander, David F., & Trinh, Quoc-Dien. (2018). Secondary data sources for health services research in urologic oncology. *Urologic Oncology: Seminars and Original Investigations*, Vol.36,(No.4)pp.165–173. https://doi.org/10.1016/j.urolonc.2017.08.008

Dhamanti, Inge., Rachman, Taufik., Ardian CL, Muhammad., Ramadhan, Nanda Aulya., Zairina, Elida., & Fauziningtyas, Rista. (2021). Development of a patient safety-training program for health workers in Indonesia: Perspectives of health workers and hospital stakeholders. *Malaysian Journal of Medicine and Health Sciences*, Vol.17,(No.2),pp.183-188. https://medic.upm.edu.my/upload/dokumen/2021040613142925_MJMHS_0694.pdf–188.

Diana, Aly., Hollingworth, Samantha A., & Marks, Geofrey C. (2015). Effects of decentralisation and health system reform on health workforce and quality-of-care in Indonesia, 1993-2007. *International Journal of Health Planning and Management*, Vol.30,(No.1),pp.16–30. https://doi.org/10.1002/hpm.2255

Essefi, Inthidar., Rahmouni, Hanene Boussi., & Ladeb, Mohamed Fethi. (2021). Integrated privacy decision in BPMN clinical care pathways models using DMN. *Procedia Computer Science*, Vol. 196, pp. 509–516. https://doi.org/10.1016/j.procs.2021.12.043

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations

in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, Vol.25, (No.2),pp.91–109. https://doi.org/10.1057/ejis.2015.9

Georgiou, Dimitra., & Lambrinoudakis, Costas. (2021). Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. *Future Internet*, Vol.13,(No.3),p.66. https://doi.org/10.3390/fi13030066

Hamzani, Achmad Irwan., Widyastuti, Tiyas Vika., Khasanah, Nur., & Rusli, Mohd Hazmi Mohd. (2024). Implementation approach in legal research. *International Journal of Advances in Applied Sciences*, Vol.13, (No.2),pp.380–388. https://doi.org/10.11591/ijaas.v13.i2.pp380-388

Helou, Samar., Abou-Khalil, Victoria., Yamamoto, Goshiro., Kondoh, Eiji., Tamura, Hirosi., Hiragi, Shusuke., Sugiyama, Osamu., Okamoto, Kazuya., Nambu, Masayuki., & Kuroda, Tomohiro. (2019). Prioritizing features to redesign in an EMR system. *Studies in Health Technology and Informatics*,Vol.264,pp.1213–1217. https://doi.org/10.3233/SHTI190419

Howard, Heidi., Alder, Fritz., Ashton, Edward., Chamayou, Amaury., Clebsch, Sylvan., Costa, Manuel., Delignat-Lavaud, Antonie., Fournet, Cedric., Jeffery, Andrew., Kerner, Matthew., Kounelis, Fotios., Kuppe, Markus A., Maffre, Julien., Russinovich, Mark., & Wintersteiger, Christop M. (2023). *Proceedings of the VLDB Endowment*, Vol.17,Issue2,pp.225–240. https://doi.org/10.14778/3626292.3626304

Hwang, Hsin-Gwinn., & Lin, Yun. (2020). Evaluating people's concern about their health information privacy based on power-responsibility equilibrium model: A case of Taiwan. *Journal of Medical Systems*, Vol.44,(No.6).https://doi.org/10.1007/s10916-020-01579-6

Januarita, Ratna., Alamsyah, Indra Fajar., & Perdana, Arif. (2024). Guardians of data: TruMe Life's continuous quest for data protection. *Journal of Information Technology Teaching Cases*. https://doi.org/10.1177/20438869241242141

Jose, Nandu S. (2023). Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analysis. *Brawijaya Law Journal,*Vol.10,(No.1),pp.34-58. DOI:10.21776/ub.blj.2023.010.01.03

Kang, James Jin., Fahd, Kiran., & Venkatraman, Sitalakhsmi. (2018). Trusted time-based verification model for automatic man-in-the-middle attack detection in cybersecurity. *Cryptography*,Vol.2,(No.4),pp.1–20. https://doi.org/10.3390/cryptography2040038

Keshta, Ismail., & Odeh, Ammar. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian*

Informatics Journal, Vol.22,(No.2),pp.177–183.https://doi.org/10.1016/j.eij.2020.07.003

Kharisma, Dona Budi., & Diakanza, Alvalerie. (2024). Patient personal data protection: comparing the health-care regulations in Indonesia, Singapore and the European Union. *International Journal of Human Rights in Healthcare*,Vol.17,(No.2),pp.157–169. https://doi.org/10.1108/IJHRH-04-2022-0035

Kristanto, Asa P. (2023). Perlindungan Terhadap Data Pribadi Dalam Aplikasi Digital Sebagai Bentuk Perlindungan Hak Asasi Manusia. *Unes Law Review*, Vol.5,(No.3), pp.952–960.https://review-unes.com/ index.php/law/article/view/367

Kuiper, Malouke Esra., Chambon, Monique., de Bruijn, Anne Leonore., Folmer, Chris Reinders., Olthuis, Elke Hindia., Brownlee, Megan., Kooistra, Emmeke Barbara., Fine, Adam., van Harreveld, Frenk., Lunansky, Gabriela., & van Rooij, Benjamin. (2023). A Network Approach to Compliance: A Complexity Science Understanding of How Rules Shape Behavior. *Journal of Business Ethics*,Vol.184,(No.2),pp.479–504. https:// doi.org /10.1007/s10551-022-05128-8

Kumar, Rajeev., Baz, Abdullah., Alhakami, Hosam., Alhakami, Wajdi., Baz, Mohammed., Agrawal, Alka., & Khan, Raaes Ahmad. (2020). A Hybrid Model of Hesitant Fuzzy Decision-Making Analysis for Estimating Usable-Security of Software. *IEEE Access*, Vol.8. https://doi.org/10.1109/ACCESS.2020.2987941

Larson, Lislie., & Alexander, Susan. (2021). The Role of a Nurse Practitioner in a “Big Bang” Electronic Medical Record Implementation. *CIN - Computers Informatics Nursing*, Vol.39,(No.3),pp.113–119. https://doi.org/ 10.1097/CIN.0000000000000729

Lawelai, Herman., Iswanto., & Raharja, Nia Maharani. (2023). Use of Artificial Intelligence in Public Services: A Bibliometric Analysis and Visualization. *TEM Journal*, Vol.12,(No.2), pp.798–807. https://doi.org/10.18421/TEM122-24

Mahfuth, Amjad., Dhillon, Jaspaljeet Singh., & Drus, Sulfeeza Mohd. (2016). A systematic review on data security and patient privacy issues in electronic medical records. *Journal of Theoretical and Applied Information Technology*, Vol.90, (No.2), pp.106–115. https://www.jatit.org/ volumes/ Vol90No2/12Vol90No2.pdf

Marotta, Angelica., & Madnick, Stuart. (2022). Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case. *Issues in Information Systems*,Vol.23,(No.1),pp.102–116. https://doi.org/10.48009/1_iis_2022_108

Mbonihankuye, Scholas., Nkunzimana, Athanase., Ndagijimana, Ange., & García-Magariño, Ivan. (2019). Healthcare Data Security Technology: HIPAA Compliance.

Wireless Communications and Mobile Computing.https://doi.org/10.1155/2019/1927495

Naqvi, Bilal., Clarke, Nathan., & Porras, Jari. (2020). Incorporating The Human Facet of Security In Developing Systems And Services. *Information and Computer Security*,Vol.29,(No.1),pp.49–72. https://doi.org/10.1108/ICS-11-2019-0130

Natamiharja, Rudi., & Setiawan, Ikhsan. (2024). Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France. *Jambe Law Journal*, Vol.7, (No.1), pp.233–251. https://doi.org/10.22437/home.v7i1.349

Njotini, Mzukisi N. (2018). Preserving the Integrity of Medical-Related Information – How "Informed" is Consent? *Potchefstroom Electronic Law Journal*, Vol.21, pp.1–20. https://doi.org/10.17159/1727-3781/ 2018/ v21i0a3400

Patel, Hiral., Patel, Meghna., & Parikh, Satyen. (2020). Fundamentals of health-care system and general rules for security and privacy. *Security and Privacy of Electronic Healthcare Records* (pp.43–60). https://doi.org/10.1049/PBHE020E_ch3

Peat, Daniel., Fikfak, Veronika., & Van Der Zee, Eva. (2022). Behavioural Compliance Theory. *Journal of International Dispute Settlement*,Vol.13,(No.2),pp.167–178. https://doi.org/10.1093/jnlids/idab033

Price, Morgan., Weber, Jens H., Davies, Iryna., & Bellwood, Paule. (2015). Lead User Design: Medication Management in Electronic Medical Records. *Studies in Health Technology and Informatics*, Vol.216,pp.237–241. https://doi.org/10.3233/978-1-61499-564-7-237

Schulman, R. (2006). HIPAA privacy and security implications for field triage. *Prehospital Emergency Care*, Vol.10, (No.3), pp.340–342.https://doi.org/10.1080/10903120600728771

Sher, Ming-Ling., Talley, Paul C., Cheng, Tain Jun., & Kuo, Kuang-Ming. (2017). How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. *Health Information Management Journal*, Vol.46,(No.2),pp.87–95. https://doi.org/10.1177/1833358316671264

Solehudin, Herlan., & Ruhaeni, Neni. (2022). Perlindungan Hukum Atas Kebocoran Data Pribadi Ditinjau dari Undang Undang Nomor 19 Tahun 2019 tentang Informasi dan Transaksi Elektronik dan Implementasinya terhadap Kebocoran Data Pengguna Electronic Healcth Alert Card. *Bandung Conference Series: Law Studies*,Vol.2,(No.2),pp.981–988. https://doi.org/10.29313/bcsls.v2i2.2520

Solihin, Firdaus., Budi, Indra., Aji, Rizal Fathoni., & Makarim, Edmon. (2021). Advancement of information extraction use in legal

documents. *International Review of Law, Computers and Technology*, Vol.35, (No.3), pp.322–351. https://doi.org/10.1080/13600869.2021.1964225

Stark, Benjamin., Gewald, Heiko., Lautenbacher, Heinrich., Haase, Ulrich., & Ruff, Seigmar. (2021). Misuse of 'Break-the-Glass' Policies in Hospitals: Detecting Unauthorized Access to Sensitive Patient Health Data. *Research Anthology on Privatizing and Securing Data*, p.26. https://doi.org/10.4018/978-1-7998-8954-0.ch058

Sudarwanto, Al Sentot., & Kharisma, Dona Budi Budi. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, Vol.29, (No.4), pp.1443–1457.https://doi.org/10.1108/JFC-09-2021-0193

Suwantika, Auliya A., Zakiyah, Neily., Abdulah, Rizky., & Diantini, Ajeng. (2023). Assessment of childhood immunization services at private healthcare facilities in Indonesia: a case study in a highly-populated city. *Frontiers in Public Health*, Vol.11.https://doi.org/10.3389/fpubh.2023.1093387

Syahputra, Alfin Reza., & Munandar, Adis Imam. (2021). The Hike in BPJS Kesehatan's Premiums based on The principle of Justice in Service Regulation of Healthcare Insurance. *Law Reform,*Vol.17,(No.1),pp.1-12. https://doi.org/10.14710/lr.v17i1.37548

Vimalachandran, Pasupathy., Wang, Hua., & Zhang, Yanchun. (2015). Securing electronic medical record and electronic health record systems through an improved access control. In *International Conference on Health Information Science*, Vol.9085, pp.17–30. https://doi.org/10.1007/978-3-319-19156-0_3

Widianto, Sunu., Kautsar, Angga Prawira., Sriwidodo., Abdulah, Rizky., & Ramadhina, Rakhma. (2021). Pro-environmental behaviour of healthcare professionals: A study applying theory of planned behaviour. *International Journal of Business and Globalisation*, Vol.28, (No.3), pp.219–232. https://doi.org/10.1504/ijbg.2021.115562

Williams, Colleen C. (2020). Discovering and Identifying Grey Literature in the Field of Law. *Serials Librarian*, Vol.79, issue 3–4, pp.245–251. https://doi.org/10.1080/0361526X.2020.1847741

Xiang, Xinying., Cao, Jin., & Fan, Weiguo. (2022). Decentralized authentication and access control protocol for blockchain-based e-health systems. *Journal of Network and Computer Applications*, Vol.207. https://doi.org/10.1016/j.jnca.2022.103512

Yeng, Phosper Kandabongee., Szekeres, Adam., Yang, Bian., & Snekkenes, Einar Arthur. (2021). Mapping the psychosocialcultural aspects of healthcare professionals'

information security practices: Systematic mapping study. *JMIR Human Factors*, Vol.8,(No.2). https://doi.org/10.2196/17604

Yeo, Liu Hua., & Banfield, James. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, Vol.19. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/

Zhang, Jiaxin., & Luximon, Yan. (2021). Interaction design for security based on social context. *International Journal of Human Computer Studies*, Vol.154. https://doi.org/10.1016/j.ijhcs.2021.102675

Zielińska-Tomczak, Łucja., Cerbin-Koczorowska, Magdalena., Przymuszała, Piotr., & Marciniak, Ryszard. (2021). How to effectively promote interprofessional collaboration? – a qualitative study on physicians' and pharmacists' perspectives driven by the theory of planned behavior. *BMC Health Services Research*, Vol.21, (No.1). https://doi.org/10.1186/s12913-021-06903-5

CONFERENCES & PROOCEDINGS

Al-Far, Anas., Qusef, Abdallah., & Almajali, Sufyan. (2018). Measuring Impact Score on Confidentiality, Integrity, and Availability Using Code Metrics. *In International Arab Conference on Infirmation Technology (ACIT) 2018.* Lebanon: IEEE. https://doi.org/10.1109/ACIT.2018.8672678

Al-Jawarneh, Loui., & Mohammed, Tareq Abed. (2022). Service Quality in eLearning. *In International Conference on Engineering & MIS (ICEMIS 2022)* Istanbul: IEEE. https://doi.org/10.1109/ICEMIS56295.2022.9914135

Ardito, Carmelo., Bernhaupt, Regina., Palanque, Philippe., & Sauer, Stefan. (2019). Handling Security, Usability, User Experience and Reliability in User-Centered Development Processes. In *IFIP WG 13.2 and WG 13.5 Workshop at INTERACT 2019* (pp. 759–762). Springer: Verlag. https://doi.org/10.1007/978-3-030-29390-1_76

Azadi, Mojgan., Zare, Hossein., & Zare, Mohammad Jalal. (2018). Confidentiality, Integrity and Availability in Electronic Health Records: An Integrative Review. In *Advances in Intelligent Systems and Computing (Conference Paper)*, Vol.738, pp.745–748).https://doi.org/10.1007/978-3-319-77028-4_97

Costa, Antonio Pedro., Moresi, Eduardo Dutra., Pinho, Isabel., & Halaweh, Mohanad. (2023). Integrating Bibliometrics and Qualitative Content Analysis for Conducting a Literature Review. In *24th International Arab Conference on Information Technology (ACIT 2023)*. Ajman: IEEE. https://doi.org/10.1109/ACIT58888.2023.10453680

Cybenko, George., & Hughes, Jeff. (2014). No free lunch in cyber security. *Proceedings of the ACM Conference on Computer and Communications Security* (pp.1–12). https://doi.org/10.1145/2663474.2663475

Firmansyah, Warmanto., Mantoro, Teddy., & Persadha, Pratama Dahlian. (2022). Regulatory Support to Prevent Health Data Breaches. *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED 2022)*, pp.1–4. https://doi.org/10.1109/ICCED56140.2022.10010539

Fischer-Hübner, Simon., Pettersson, John Soren., & Angulo, Julio. (2015). HCI requirements for transparency and accountability tools for cloud service chains. In *Summer School on Accountanbility and Security in The Cloud* (Conference Paper), Vol.8937, pp.81–113. https://doi.org/10. 1007/978-3-319-17199-9_4

Fuad, Anis., Putri, Siti Setyawati Mulyono., Sitaresmi, Mei Neni., & Puspandari, Diah Ayu. (2019). Financial Sources Options for Telemedicine Program within Universal Health Coverage (UHC) Era in Indonesia. *In 1st International Conference on Bioinformatics, Biotechnology, and Biomedical Engineering (BioMIC 2018)*. Yogyakarta: IEEE. https://doi.org/10.1109/BIOMIC.2018.8610595

Gamundani, Attlee M. (2023). Unmasking the Potential of Usable Security and Privacy Technologies in Empowering African Digital Landscapes. In *Proceedings of the 4th African Human Computer Interaction Conference* (pp.201-207). https://doi.org/10.1145/3628096.3629057

Gunawan, Ali., Richard, Given Name., Susanto, Gabriele Aurellia., Saputra, Aldo., & Rizal, Arthea Callista. (2023). Understanding the Use of Blockchain in Medical Data Security: A Systematic Literature Review. In *ICBTA '22: Proceedings of the 2022 5th International Conference on Blockchain Technology and Applications* (pp.170-174). DOI: 10.1145/3581971.3581995

Hausawi, Yasser M., & Allen, William H. (2015). Usable-Security Evaluation. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Vol.9190,pp.335–346. https://doi.org/10.1007/978-3-319-20376-8_30

Horcher, Ann Marie., & Tejay, Gurvirender. (2013). The Convergence of Security And Usability: Defining A Framework For Mobile Design. In *International Conference on Human-Computer Interaction,* pp.119–123. https://doi.org/10.1007/978-3-642-39473-7_25

Humaidi, Norshima., Balakrishnan, Vimala., & Shahrom, Mellisa. (2014). Exploring user's compliance behavior towards Health Information System security policies based on extended Health Belief Model. In *IEEE Conference on e-Learning, e-Management*

and e-Services (IC3e), pp.30–35. https://doi.org/10.1109/IC3e.2014.7081237

Jones, C. (2022). Bioinformatics, Medical Informatics and the European General Data Protection Regulation. In *Bioinformatics, Medical Informatics and the Law* (pp. 248–268). Edward Elgar Publishing.https://doi.org/10.4337/9781839105951.00022

Kapila, Aarus., & Pillai, Samaya. (2023). Healthcare Information Privacy: Growing Need for Security Techniques in Healthcare Systems. In *AIP Conference Proceedings*, Vol. 2523, Issue 1. https://doi.org/10.1063/5.0110487

Lawelai, H. (2023). Understanding Digital Governance in Smart Cities: In-Depth Study Utilizing VOSviewer and CiteSpace. In *International Conference on Environment and Smart Society (ICEnSO 2023),*Vol.440.https://doi.org/10.1051/e3sconf/202344007003

Mahajan, Navita., Garg, Seema., Pandita, Shreyas., & Sehgal, Geetansh. (2022). Smart healthcare and digitalization: Technological and cybersecurity challenges. In *Cross-Industry Applications of Cyber Security Frameworks* (pp.124–147). https://doi.org/10.4018/978-1-6684-3448-2.ch007

Mukhachev, Igor V., Gondarenko, Alexander S., & Gryaznov, Denis G. (2022). The Importance of Non-structural Elements in Normative Regulation in Constitutional Law. In *Advances in Science, Technology and Innovation* (pp. 1069–1073). Springer Nature. https://doi.org/10.1007/978-3-030-90324-4_177

Naqvi, Bilal., & Seffah, Ahmed. (2019). Interdependencies, Conflicts and Trade-Offs Between Security and Usability: Why and How Should We Engineer Them? In *International Conference on Human-Computer Interaction,* Vol.11594,pp.314–324).https://doi.org/10.1007/978-3-030-22351-9_21

Noor, Muhammad Usman., & Darmaningrat, Eko Wahyu Tyas. (2023). Critical Realism as Innovative Approach for Social Science Research: Information Governance Practices Context. In *Proocedings of the 6th International Conference on Vocational Education Applied Science and Technology (ICVEAST 2023)* (pp.612–624). Springer: Atlantis Press. https://doi.org/10.2991/ 978-2-38476-132-6_53

Obeng, Osborne., & Paul, Souren. (2019). Understanding HIPAA compliance practice in healthcare organizations in a cultural context. *25th Americas Conference on Information Systems, AMCIS 2019*. https://www.semanticscholar.org/paper/Understanding-HIPAA-Compliance-Practice-in-in-a-Obeng-Paul/98eff336e32aab86281299af6abb3f4ac3bf3afc

Padrão, Pascoal., Ribeiro, Maria Isabel., & Lopes, Isabel. (2024). Implementation of the General Regulation on Data Protection – In the Intermunicipal Community of Douro, Portugal. In *International Conference on Management, Tourism and Technologies*, Vol.773,pp.360–367. https://doi.org/10.1007/978-3-031-44131-8_35

Santos, Jose Amancio Macedo., Santos, Alcemir Rodrigues., & De Mendonça, Manoel Gomes. (2015). Investigating bias in the search phase of Software Engineering secondary studies. *CIBSE 2015 - XVIII Ibero-American Conference on Software Engineering*,pp.488–501. https://eventos.spc.org.pe/cibse2015/pdfs/03_ESELAW15.pdf

Shahri, Ahmad Bakhtiyari., & Mohanna, Shahram. (2016). The Impact of the Security Competency on "Self-efficacy in Information Security" for Effective Health Information Security in Iran. In *Advances in Intelligent Systems and Computing*, Vol.445,pp.51–61. https://doi.org/10.1007/978-3-319-31307-8_6

Shanmugam, Divya., Diaz, Fernando., Shabanian, Samira., Finck, Michele., & Biega, Asia. (2022). Learning to Limit Data Collection via Scaling Laws: A Computational Interpretation for the Legal Principle of Data Minimization. *In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp.839–849). https://doi.org/10.1145/3531146.3533148

Sharma, Priynka., Bir, Jasvir., & Prakash, Surya. (2024). Navigating Privacy and Security Challenges in Electronic Medical Record (EMR) Systems: Strategies for Safeguarding Patient Data in Developing Countries – A Case Study of the Pacific. In *International Conference on Medical Imaging and Computer-Aided Diagnosis*, Vol.1166,pp.375–386. https://doi.org/10.1007/978-981-97-1335-6_33

Sumra, Irsyad Ahmed., Hasbullah, Halabi Bin, & AbManan, Jamalul-Lail Bin. (2015). Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey. *Advances in Intelligent Systems and Computing*, Vol.306,pp.51–61 (Conference Paper). https://doi.org/10.1007/978-981-287-158-9_5

Vaishnavi, P., Sam Nithish, K. C., & Parvathi, S. (2024). Secure Data Sharing Using an Elliptic Curve Cryptography Method for Medical Mecord Transactions in Cloud Environment. In *International Conference on Reliability, Safety, and Hazard*, pp.821–827). https://doi.org/10.1007/978-981-97-3087-2_73

van Boom, Willem H., Desmet, Pieter., & Mascini, Peter. (2018). Empirical legal research in

action: Reflections on methods and their applications. In *Empirical Legal Research in Action: Reflections on Methods and their Applications*. Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781785362750

Wang, Xianping., Qiu, Hao., Shen, Jiayue., & Chen, Weiru. (2023). A Survey on the Cybersecurity of IoT From The Perspective of SoC. In *10th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2023* (pp. 66–71). https://doi.org/10.1109/IOTSMS59855.2023.10325724

Winckler, Marco., Larusdottir, Marta., Kuusinen, Kati., Bogdan, Cristian., & Palanque, Phillipe. (2017). Dealing with conflicting user interface properties in user-centered development processes. In *16th Conference on Human-Computer Interaction (INTERACT)*, Sep 2017, Bombay, India. pp.521-523. https://hal.science/hal-01680275/

Zalloum, Mutaz., & Alamleh, Hosam. (2020). Privacy Preserving Architecture for Healthcare Information Systems. *2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat 2020)* pp.429-432. *DOI: 10.1109/Comnetsat50391.2020.*

Zoghlami, Meryem., Ayeb, Salma., & Rached, Kaouter Saied. Ben. (2021). Using e-health in the prevention against covid-19: An approach based on the theory of planned behavior. In International Conference on Human-Computer Interaction, pp.507–517. Conference Paper https://doi.org/10.1007/978-3-030-78465-2_37

BOOK SECTIONS

Kalaiselvi, R., & Sumathi, V. P. (2023). Encountering Privacy – Sensitive Information in Medical Documents. In *Sustainable Digital Technologies for Smart Cities: Healthcare, Communication, and Transportation* (pp. 213–220). CRC Press. https://doi.org/10.1201/9781003307716-21

Kesale, Anosisye Mwandulusya., & Swai, Idda Lyatonga. (2023). Management and Governance of Health Facilities. In *Leadership and Governance in Primary Healthcare: An Exemplar for Practice in Resource Limited Settings* (pp.13–26). CRC Press. https://doi.org/10.1201/9781003346821-2