Electronic Health Records In Indonesia: A Law And Policy Analysis

Rita Komalasari[1], *Cecep Mustafa*[2]

Abstract

The Policy of Privacy of Electronic Health Records (EHRs) have transformed healthcare in Indonesia, aggregating patient data for comprehensive medical care. However, they introduce privacy concerns due to electronic data, network transmission, and multi-user access. Patients worry about unauthorized access, misuse, and digital errors, impacting their privacy, social standing, and insurance. This research explores stakeholder attitudes and risks surrounding EHR data sharing in Indonesia, with a focus on Payers, Patients, and Providers (the 3Ps). The purpose of this paper is to fill in some of the gaps in the existing research on the topic of EHR privacy and effectiveness. It incorporates a variety of research techniques, a critical realism viewpoint, insights from many stakeholders, and an examination of the trade-off between privacy and effectiveness. The purpose is to learn more about the many factors that play into EHR privacy concerns so that we may better address them via legislation and practice. A literature study is used in this research. The critical realist perspective illuminates underlying forces. Stakeholder-specific insights are drawn from Payers, Patients, and Providers. The privacy-efficacy trade-off is analyzed to comprehend its impact. This research offers a nuanced understanding of EHR privacy concerns in Indonesia. It highlights unique stakeholder perspectives, the privacy-efficacy trade-off, and the role of human factors in data breaches. Structuration Theory provides a comprehensive framework, allowing us to navigate these multifaceted issues. Ultimately, this analysis contributes to more informed policy decisions and practical solutions in Indonesia's evolving privacy data management landscape.

Keywords: data; law; privacy; healthcare; management; stakeholder

1. Introduction

In an era where technology pervades nearly every facet of our lives, the healthcare sector has not been left untouched.[3] The introduction of EHRs has radically altered the healthcare system in Indonesia by standardising the collection, storage, and dissemination of patient data. These digital repositories aggregate an individual's health data, creating a comprehensive overview of their medical history, treatments, and interactions with the healthcare system.[4] However, this transition

[1] Rita Komalasari is a lecturer at the Faculty of Medicine and Graduate School, YARSI University. The author actively writes scientific articles and is published in national, and international journals. The author is also a reviewer in several national and international journals. Please direct correspondence to rita.komalasari161@gmail.com

[2] Cecep Mustafa is a lecturer at Ibnu Chaldun University. The author actively writes scientific articles and is published in national and international journals. The author is also a reviewer in several national and international journals. Please direct correspondence to cecep.mustafa161@gmail.com

[3] Althaus, Catherine, Sarah Ball, Peter Bridgman, Glyn Davis, and David Threlfall. *The Australian policy handbook: A practical guide to the policymaking process*. Taylor & Francis, 2022.

[4] Khang, Alex, Geeta Rana, R. K. Tailor, and Vugar Abdullayev, eds. "Data-Centric AI Solutions and Emerging *Technologies in the Healthcare Ecosystem*." (2023).

from paper records to electronic systems has ushered in a new set of challenges and concerns, particularly regarding the privacy and efficacy of EHRs.[5] This essay delves into a critical examination of the privacy and efficacy of Electronic Health Records in the context of Indonesia, drawing from a comprehensive literature study.The primary motivation for this study is to learn about the perspectives of different groups and their perceptions of the risks associated with disclosing private and sensitive health and personal information to healthcare providers, which could then be disseminated widely throughout the healthcare system. To answer this, we examine the complex ecosystem of electronic health records in Indonesia from the viewpoints of the three main players involved: the payers, patients, and providers (3Ps). They have a significant impact on how people feel about the security and usefulness of electronic health records (EHRs). This essay is structured as follows: Firstly, we delve into the inherent risks associated with EHR systems, given that patient data is now in electronic form, transmitted across networks, and accessible from multiple locations by various individuals, including those who lack any direct relationship with the patient. Secondly, we explore the multifaceted concerns that patients harbor, ranging from unauthorized access to their private health information, unlawful secondary usage of data, and potential digital errors, to apprehensions about social repercussions and loss of insurance benefits. These concerns form a significant backdrop against which EHRs must be evaluated. Next, we dissect the attitudes and perspectives of each stakeholder group - Payers, Patients, and Providers - uncovering their distinct concerns and interests in the realm of EHRs. Furthermore, we examine the countermeasures employed by these groups to safeguard their private health information within EHR systems. Intriguingly, the essay highlights the nuanced perception of patients as secondary stakeholders in the EHR system by Payers, despite patients being the legal owners of their medical data. We also explore the belief among Payers that technological safeguards are sufficient to protect privacy, while acknowledging that many breaches stem from human factors that technology alone cannot eliminate. Lastly, we discuss the consequences of these privacy concerns on the efficacy of EHRs. We find that while countermeasures may protect privacy, they can inadvertently hinder the patient-centric nature of EHRs, potentially undermining the system's intended benefits for patients. This research presents a triangulation study that rigorously validates collected data, offering insights from a critical realist perspective. By shedding light on the underlying forces shaping privacy concerns for both patients and healthcare providers, this essay contributes to a deeper understanding of the intricate dynamics at play within Indonesia's evolving healthcare landscape concerning EHRs.[6]

This research makes several novel contributions to the field of privacy concerns in Electronic Health Records (EHRs) within the context of Indonesia's healthcare landscape.[7] These contributions offer fresh insights and perspectives that enhance our understanding of the intricate dynamics surrounding EHR privacy concerns: By adopting a critical realist perspective, the research delves deeper into the underlying forces that shape privacy concerns among patients and healthcare providers. This perspective allows for a nuanced exploration of the interplay between social structures, individual perceptions, and technological systems, shedding light on the root causes of these concerns. The research highlights the distinct perspectives and concerns of the three key stakeholder groups: Payers, Patients, and Providers (the 3Ps). This granularity provides a

[5] Tutty, Michael A., Lindsey E. Carlasare, Stacy Lloyd, and Christine A. Sinsky. "The complex case of EHRs: examining the factors impacting the EHR user experience." *Journal of the American Medical Informatics Association* 26, no. 7 (2019): 673-677.

[6] Kandasamy, Kamalanathan, Sethuraman Srinivas, Krishnashree Achuthan, and Venkat P. Rangan. "Digital healthcare-Cyber Attacks in Asian organizations: an analysis of vulnerabilities, risks, NIST perspectives, and recommendations." *IEEE Access* 10 (2022): 12345-12364.

[7] Klecun, Ela, Ya Zhou, Atreyi Kankanhalli, Yap Hwee Wee, and Ralph Hibberd. "The dynamics of institutional pressures and stakeholder behavior in national electronic health record implementations: A tale of two countries." *Journal of Information Technology* 34, no. 4 (2019): 292-332.

unique insight into how different stakeholders perceive and navigate the privacy challenges posed by EHRs. Understanding these variations is crucial for developing targeted strategies to address privacy concerns. The research uncovers an important trade-off between privacy protection measures and the patient-centric nature of EHRs. This nuanced insight reveals that while privacy countermeasures are essential, they may unintentionally hinder the original purpose of EHRs, which is to provide efficient and patient-focused healthcare. This perspective adds depth to discussions about EHR system design and implementation. The research illuminates the perception among Payers that patients are secondary stakeholders in the EHR system, despite patients being the legal owners of their medical information. This finding challenges traditional power dynamics in healthcare and raises questions about patient empowerment and agency in the digital age. By acknowledging that many data breaches are caused by human factors rather than technological deficiencies, the research introduces a critical dimension to the discussion of EHR security. This perspective underscores the need for comprehensive privacy training and awareness programs for healthcare personnel. This research offers a multifaceted exploration of privacy concerns in EHRs within the Indonesian healthcare context. Its unique contributions lie in the triangulation study design, critical realist perspective, stakeholder-specific insights, and the nuanced understanding of the interplay between privacy protection and EHR efficacy. These contributions collectively advance our comprehension of the complex dynamics shaping EHR privacy concerns, ultimately contributing to more informed policy decisions and practical solutions in the evolving landscape of healthcare data management in Indonesia.

The existing literature on Electronic Health Records (EHRs) in Indonesia, while informative, presents several notable gaps that this essay aims to address through its multifaceted exploration of privacy concerns in EHRs within the Indonesian healthcare context:[8] The majority of existing literature tends to focus on surface-level observations and descriptive analysis of privacy concerns. In contrast, this essay adopts a critical realist perspective, aiming to uncover the underlying structures and mechanisms that drive these concerns. This shift from descriptive to explanatory analysis contributes significantly to the depth of understanding in the field. Many studies may overlook the distinct perspectives of different stakeholder groups within the EHR ecosystem. [9]By emphasizing the unique concerns of Payers, Patients, and Providers (the 3Ps), this essay addresses a gap in the literature by recognizing the diversity of interests and attitudes among these critical actors. Existing research often lacks an in-depth exploration of the trade-off between privacy protection measures and the efficacy of EHR systems. This essay's nuanced examination of how privacy countermeasures can inadvertently impact the patient-centric nature of EHRs provides a deeper understanding of the practical challenges faced by healthcare institutions and policymakers. The literature often does not adequately address the perception among Payers that patients are secondary stakeholders in EHR systems. This essay highlights this important power dynamic, filling a gap in the literature and sparking discussions about the need to empower patients in the digital healthcare landscape. The role of human factors in data breaches within EHR systems is not always sufficiently emphasized in existing research. Recognizing that many breaches are caused by human actions rather than solely by technological vulnerabilities contributes to a more holistic understanding of EHR security. This essay bridges several significant gaps in the existing literature on EHRs in Indonesia by adopting a multifaceted approach that combines diverse research methods, a critical realist perspective, stakeholder-specific insights, and

[8] Talwar, Shalini, Amandeep Dhir, Nazrul Islam, Puneet Kaur, and Ahlam Almusharraf. "Resistance of multiple stakeholders to e-health innovations: Integration of fundamental insights and guiding research paths." *Journal of Business Research* 166 (2023): 114135.

[9] Konopik, Jens, and Dominik Blunck. "Development of an Evidence-Based Conceptual Model of the Health Care Sector Under Digital Transformation: Integrative Review." Journal of Medical Internet Research 25 (2023): e41512.

an exploration of the privacy-efficacy trade-off. These results, taken as a whole, expand our knowledge of the many factors that influence EHR privacy concerns and provide the framework for more well-informed legislative decisions and practical solutions in Indonesia's fast expanding healthcare data management environment.

2. Method

A comprehensive literature review served as the foundation for this inquiry into the complexities of Electronic Health Records (EHRs) and privacy problems in the Indonesian healthcare system. A thorough grasp of the issue at hand was compiled by specialists in the area after a thorough assessment of the related literature. By reviewing the current literature on EHRs and privacy, our investigation may help close important knowledge gaps. The literature-based strategy created a firm foundation for the research questions, hypotheses, and data collection that followed. It allowed for an in-depth analysis of the Indonesian healthcare system from the three most crucial stakeholder vantage points (payers, patients, and providers).

3. Findings and Discussion

3.1. Structural Analysis

Considering the complexities of the privacy-efficacy trade-off in the context of Electronic Health Records (EHRs) in Indonesia, which necessitates numerous research techniques, a critical realism perspective, stakeholder-specific insights, and more, the Structuration Theory may be instructive. Anthony Giddens's Structuration Theory offers a powerful framework for analyzing how social norms, regulations, and institutions interact with agency (individual acts and choices) in every given setting. This theory proposes that social practices are molded by the interplay between structure and agency, and it provides a lens through which to analyze the ways in which people and institutions both affect and are affected by the contexts in which they function. To analyze EHR privacy issues in Indonesia thoroughly, Structuration Theory may be used as follows: Researchers interested in the interactions between EHRs and its various stakeholder groups (Payers, Patients, and Providers) may do so with the help of Structuration Theory. This sheds light on the ways in which these techniques affect societal norms related to privacy issues and EHR use. Some methods that can be used to fully capture the intricacies of these activities include surveys, interviews, and ethnographic study. The theory is compatible with a critical realism worldview since it allows for the possibility of change within structures. This provides an opportunity for study of the influence of changing attitudes about privacy in electronic health records (EHRs) on Indonesia's cultural norms and institutional frameworks. When it comes to rules and norms, Structuration Theory places an emphasis on the agency of various actors. Using this structure, researchers may investigate the diverse perspectives of Payers, Patients, and Providers, and better understand how each group influences the dynamics of EHR privacy. The hypothesis gives us a starting point from which to investigate the potential trade-off between patient privacy and the efficiency of EHR systems. This facilitates studies into the effects of individual and institutional decisions within the EHR ecosystem on privacy risks and healthcare delivery efficiency. This all-encompassing study makes use of Structuration Theory to provide light on the complex dynamics of EHR privacy issues in Indonesia, including the role that interactions between structures and agency play. It's useful for grasping not only the current situation, but also the room for growth and change in healthcare data management. This knowledge may influence policy choices and concrete solutions that strike a compromise between patient privacy and the effective use of electronic health records in the Indonesian healthcare system.

3.1.1. Inherent Risks of Electronic Health Records

The policy adoption of Electronic Health Records (EHRs) represents a pivotal shift in healthcare, promising significant improvements in patient care, operational efficiency, and the accessibility of medical data.[10] However, this digital transformation brings with it a set of inherent risks that necessitate close examination and careful consideration. Paper-based records were formerly used in the healthcare industry; although flawed, they were physical and localized. Patient records used to be paper papers kept in medical offices, with access restricted to those who really cared for the patient. However, electronic health records have come along and completely changed the game. Electronic health records (EHRs) are databases that store patient data digitally. There is no denying the benefits of digitalization, such as easy access and real-time information, but there are also risks associated with it. Now, information that used to be stored in secure locations may be intercepted and seen by anybody with access to the appropriate networks. There are several pathways by which this spreads, increasing the number of possible weak spots. In addition, electronic health records (EHRs) are developed to be accessed from many places and by various parties involved in the healthcare ecosystem. This openness improves teamwork and information sharing, yet others worry about their personal information being compromised. It is important to note that EHRs may be accessed by parties with no direct link to a patient, such as administrators, insurers, researchers, and others. The electronic nature of EHRs and the decentralization of data access provide a new front in privacy and security concerns. These challenges include safeguarding patient information against unauthorized access, ensuring the integrity and accuracy of the data, and protecting against digital breaches that could compromise the confidentiality of sensitive health records. In the following sections of this essay, we will delve into the multifaceted concerns that patients harbor regarding the privacy of their health data within EHR systems. Additionally, we will explore the perspectives of key stakeholders, including Payers, Patients, and Providers (the 3Ps), to gain a more comprehensive understanding of the complex dynamics surrounding EHR privacy concerns in Indonesia.

[10] Cerchione, Roberto, Piera Centobelli, Emanuela Riccio, Stefano Abbate, and Eugenio Oropallo. "Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem." *Technovation* 120 (2023): 102480.

3.1.2. Patient Concerns and Privacy

A critical aspect of the Electronic Health Records (EHRs) landscape in Indonesia revolves around the genuine and multifaceted concerns that patients harbor regarding the privacy of their health information within EHR systems. These concerns, deeply rooted in issues of confidentiality and data security, underscore the intricate challenges associated with the digitization of healthcare data. The literature consistently highlights the authentic nature of patients' worries. Foremost among these concerns is the fear of unauthorized access to their sensitive medical data. Patients recognize the profound implications that unauthorized access can have on their personal lives and overall well-being. The prospect of their health information falling into the wrong hands, where it could be exploited for malicious purposes, is a source of significant anxiety. A particularly pressing concern revolves around the unlawful secondary use of patients' health data. Patients worry that their health data may be used without their knowledge or agreement for research, commercial interests, or other unknown reasons. Because of this worry, electronic health record (EHR) systems must have very robust data security mechanisms and ethical concerns. In addition, there is an extra level of complication when it comes to data quality and security because of the digital nature of EHRs. The potential ramifications of EHR data mistakes or security breaches are not lost on patients. Possible negative health effects include inaccurate diagnosis and misdirected treatment regimens. Patients' worries about data integrity and security are amplified by the fact that such vulnerabilities in EHRs constitute a direct danger to patient health. Patients are worried about the disclosure of their personal health information for reasons outside the healthcare system. The leak of private medical information might cause humiliation, prejudice, or stigma. Moreover, patients recognize the potential for their health data to be used against them in contexts beyond healthcare, such as insurance assessments. This realization underscores the far-reaching implications of EHR privacy concerns, extending into various aspects of patients' lives. Patients grapple with a complex tapestry of worries when entrusting their health data to EHR systems. These concerns are rooted in the fundamental principles of privacy, consent, and data security, and they emphasize the critical importance of addressing EHR privacy in a comprehensive and patient-centered manner. In the subsequent sections of this essay, we will explore how these concerns interact with the perspectives of other key stakeholders, including Payers, Patients, and Providers (the 3Ps), to gain a more holistic understanding of the dynamics shaping EHR privacy in Indonesia.

3.2. Payers, Patients, Providers

Comprehensive analysis of Electronic Health Records (EHR) privacy concerns necessitates an exploration of the distinct perspectives of key stakeholders within the EHR ecosystem: Payers, Patients, and Providers (the 3Ps). These stakeholder groups wield significant influence over how EHRs are utilized and how privacy concerns are perceived and addressed.

3.2.1. Payers

Payers, such as insurance companies and government healthcare agencies, occupy a pivotal role in the healthcare landscape.[11] They often consider patients as secondary stakeholders within the EHR system. Although patients have the right to the records of their medical treatment, insurers and other payers often see themselves as the most important parties involved. This kind of thinking may create a hierarchical dynamic in which insurers

[11] Pidun, Ulrich, Niklas Knust, Julian Kawohl, Evangelos Avramakis, and Andreas Klar. "*The untapped potential of ecosystems in health care*." Boston Consulting Group (2021).

put their needs above those of their patients. Payors often highlight the importance of technology in ensuring the confidentiality of electronic health records. They think patient information can be kept safe with only technology safeguards. However, this viewpoint might fail to account for the crucial role that humans play in data breaches, rendering only technology remedies ineffective. Payers, which include insurance corporations and governmental healthcare organizations, have a vantage point inside the complex terrain of EHRs that may greatly affect the dynamics of privacy within the EHR system. Despite being the rightful owners of their own medical records, patients are typically treated as secondary stakeholders by Payers in this ecosystem. The way in which privacy issues are seen and handled is profoundly affected by the power balance between Payers and patients. The Payers' viewpoint stands out because of the stress placed on technological solutions as the principal means of protecting the confidentiality of electronic health records (EHRs). They tend to believe that robust technological security measures, such as encryption and access controls, are sufficient to protect patient data. While technology undoubtedly plays a crucial role in securing EHRs, this perspective tends to overlook a critical factor: the human element in data breaches. In reality, many data breaches within EHR systems occur due to human factors rather than inherent technological deficiencies. Instances of employees mishandling patient data, unintentional disclosures, or even insider threats reveal that privacy breaches often result from human actions. This nuanced understanding of data breaches challenges the efficacy of purely technological solutions advocated by Payers. Moreover, the hierarchical stance that considers patients as secondary stakeholders can have significant consequences. Patients legally own their medical information, and their rights to privacy should be paramount. However, the perception that Payers hold primary control over healthcare data can sometimes lead to decisions and policies that prioritize financial interests over patients' privacy and consent. The Payers' perspective, while focusing on the importance of technology in safeguarding EHR privacy, underscores the need for a more comprehensive approach that considers both technological and human factors. This realization highlights the importance of educating and training all stakeholders, including Payers, on the critical role they play in maintaining data security. Furthermore, it calls for a shift in mindset towards recognizing patients as primary stakeholders in the EHR ecosystem, reinforcing the ethical principles of patient privacy and autonomy. In the subsequent sections of this essay, we will continue to explore the multifaceted perspectives of Patients and Providers (the 3Ps) to gain a comprehensive understanding of how various stakeholders shape the landscape of EHR privacy concerns in Indonesia.[12]

3.2.2. Patients

Each Patients, as the subjects of healthcare, hold a primary interest in the privacy and security of their health information.[13] Their concerns, as discussed earlier, revolve around unauthorized access, unlawful secondary use of data, potential digital errors, and the repercussions of their health data becoming public knowledge. Patients see their health data as deeply personal and are rightfully apprehensive about its protection. Patients, as the central figures in the healthcare narrative, harbor deep and legitimate concerns regarding the security and privacy of their health information within Electronic Health Records (EHRs). These worries originate from the fact that individuals rightfully see their health records as private property, the security of which they place in the hands of the healthcare system. Patients' primary worry is that someone may steal or otherwise improperly obtain their personal health information. Patients are aware that their health records include personal information about their physical and mental

[12] Solove, Daniel J., and Paul M. Schwartz. *Information privacy law*. Aspen Publishing, 2020.

[13] Bani Issa, W., I. Al Akour, A. Ibrahim, A. Almarzouqi, S. Abbas, F. Hisham, and J. Griffiths. "Privacy, confidentiality, security and patient safety concerns about electronic health records." *International nursing review* 67, no. 2 (2020): 218-230.

health, and they understandably want that this information remain confidential. Many people worry that their personal health information, including past diagnoses, treatments, and procedures, might get into the wrong hands. Patients' privacy, relationships, and feelings of safety might all be jeopardized as a result of such access. Patients also have a keen awareness of the risks associated with the improper use of their personal health information. Patients fear that their health data is being used without their knowledge or permission for reasons such as research and marketing. The betrayal of this confidence compromises patient independence and raises ethical questions concerning the management of medical information. Furthermore, patients are conscious of the potential for digital errors within EHRs. These errors could range from inaccuracies in medical histories to security breaches that compromise data integrity. Patients understand the gravity of such errors and the far-reaching consequences they could have on their health and well-being. A misdiagnosis or erroneous treatment due to a data error could significantly impact a patient's health outcomes. These multifaceted concerns highlight the deeply personal and vital nature of health information to patients. Privacy, trust, and data accuracy are core tenets of patients' expectations within the healthcare system. Patients are not merely passive subjects; they are active participants who entrust their data to the system with the understanding that it will be handled with the utmost care and respect. In the subsequent sections of this essay, we will continue to explore the perspectives of Providers (healthcare professionals) and Payers, adding layers to our understanding of EHR privacy concerns and the interplay between different stakeholders within the Indonesian healthcare context.

3.2.3. Providers

Healthcare providers, including physicians, nurses, and other medical professionals, also play a crucial role in the EHR ecosystem.[14] They are responsible for inputting and managing patient data within the EHR system. While providers share similar privacy concerns to patients, they have unique anxieties about the privacy of their own notes and observations. The shift from traditional paper records, where providers had more direct control over who accessed their notes, has raised concerns about the visibility and accessibility of their private observations. Healthcare providers, including physicians, nurses, and other medical professionals, are central actors within the Electronic Health Records (EHRs) ecosystem. Employees' views on EHR privacy issues are influenced by the fact that they are the ones responsible for entering and maintaining patient data. Concerns concerning the confidentiality of patients' health records are shared by their providers. Protecting the confidentiality of doctors' notes and interviews is a major issue for them. These records are crucial because they include important observations, diagnoses, and recommendations for patient treatment. When moving from paper records to electronic health records (EHRs), however, doctors must frequently adjust to a situation in which their notes are accessible to a wider audience within the healthcare network, a change they may have not anticipated. Concerns have been voiced by medical practitioners due to the increased availability of provider notes. They fear what others may do with their personal medical records if they become public knowledge. Electronic health records (EHRs) bring a degree of openness and transparency that may be both helpful and troublesome, as opposed to paper data, which could be physically maintained and sealed away. While providers acknowledge the value of sharing patient data to improve care coordination, they also value protecting the privacy of patients' sensitive clinical information. Concerns regarding the unintended implications of wider data sharing, including as breaches of patient-provider confidentiality, have arisen in response to the change in who has access to their records. In addition, clinicians, patients, and Payers all worry about the same thing: the possibility of digital mistakes inside EHRs. They are keenly aware that inaccuracies or security breaches could compromise patient care, leading to incorrect diagnoses or treatment decisions that could harm patients. Providers, like other stakeholders, are not opposed to the adoption of EHRs; they recognize the potential benefits in terms of efficiency and information sharing. However, they seek a balance that ensures the privacy of sensitive clinical information while facilitating collaborative care. Understanding these stakeholder-specific perspectives is essential for a holistic examination of EHR privacy concerns. These distinct viewpoints contribute to the intricate dynamics shaping the privacy landscape within EHRs. By recognizing the interests and concerns of Payers, Patients, and Providers (the 3Ps), it becomes possible to develop more targeted strategies and policies that balance the competing priorities within the EHR ecosystem. In the subsequent sections, we will further delve into these stakeholder perspectives and explore how they intersect with the broader dynamics of privacy and efficacy in EHR systems.[15]

3.3. The Privacy-Efficacy Trade-off in EHRs

An intriguing revelation stemming from this research is the recognition of a delicate and often challenging trade-off that exists between privacy protection measures and the efficacy of Electronic Health Records (EHR) systems.[16] This trade-off raises

[14] Cloninger, C. Robert, Drozdstoj Stoyanov, Kristina K. Stoyanova, and Kimberly K. Stutzman. "Empowerment of health professionals: Promoting well-being and overcoming burn-out." In *Person Centered Medicine*, pp. 703-723. Cham: Springer International Publishing, 2023.

[15] Tutty, Michael A., Lindsey E. Carlasare, Stacy Lloyd, and Christine A. Sinsky. "The complex case of EHRs: examining the factors impacting the EHR user experience." *Journal of the American Medical Informatics Association* 26, no. 7 (2019): 673-677. https://doi.org/10.1093/jamia/ocz021

[16] Ojokoh, Bolanle Adefowoke, Benjamin Aribisala, Oluwafemi A. Sarumi, Arome Junior Gabriel, Olatunji Omisore, Abiola Ezekiel Taiwo, Tobore Igbe et al. "Contact tracing strategies for

fundamental questions about how to strike the right balance between safeguarding patient data and ensuring that EHRs serve their intended purpose effectively. Privacy protection measures within EHRs, such as stringent access controls, encryption, and data anonymization, are essential for preserving the confidentiality of patient information. These measures are vital in preventing unauthorized access, minimizing data breaches, and upholding patient privacy rights. However, implementing stringent privacy controls might add layers of complexity to EHR systems, diminishing their overall effectiveness. The context of access control presents a substantial difficulty. Strict access restrictions improve data security, but they might obstruct the free exchange of information among healthcare professionals, which could slow down or prevent the making of well-informed, timely decisions. In the event of an emergency, quick access to patient records is crucial for providing treatment. Delays and friction caused by too rigorous access constraints might possibly compromise patient treatment. Data encryption is essential for security, but it may make it hard to access and share information. When patient data is encrypted, it may be more difficult for healthcare providers to access the data and share it, which can have a negative influence on the quality of treatment patients get. Anonymization of data, although essential for protecting personal information, is not without its drawbacks. Patients' privacy will be preserved, but the data may lose some of their therapeutic and scientific value. Anonymization removes identifying information from data, which might reduce the usefulness of electronic health records (EHRs) as a source of information. For healthcare organizations and governments, balancing privacy with effectiveness is a difficult problem. It is important to strike a balance between the need for fast and effective healthcare delivery and the requirement for strong privacy protections to protect patients' rights and data. To achieve this equilibrium, one must adopt a sophisticated strategy that takes into account the specifics of EHR systems as well as the varied requirements of all relevant parties. The trade-off between privacy and effectiveness in healthcare data management highlights the need for constant discussion and new approaches. It requires an all-encompassing viewpoint that accounts for the need of privacy protection and the requirement of effective EHR systems that enable high-quality patient care.[17]

4. Conclusion

The central thesis of this research posited that understanding the intricate dynamics at play within Indonesia's healthcare landscape concerning EHRs is essential for more informed policy decisions and practical solutions. To this end, we have unearthed several key insights: Firstly, patients' concerns about unauthorized access, misuse of data, digital errors, and the potential for exposure have illuminated the profound importance of privacy protection in EHR systems. Patients view their health data as intensely personal and are rightfully vigilant about its security. Secondly, the perspectives of Payers have highlighted the need for a holistic approach that recognizes the interplay between technology and human factors in safeguarding EHR privacy. The perception of patients as secondary stakeholders underscores the necessity of rebalancing the power dynamic in favor of patient autonomy. Thirdly, healthcare Providers have raised concerns about the privacy of their clinical observations within EHRs. The shift from traditional paper records has introduced new challenges in controlling access to sensitive clinical judgments, prompting the need for more nuanced privacy controls. In light of these findings, it is crucial for healthcare providers, government agencies, and EHR system developers in Indonesia to take

COVID-19 prevention and containment: A scoping review." *Big Data and Cognitive Computing* 6, no. 4 (2022): 111.

[17] Upadhyay, Soumya, and Han-fen Hu. "A qualitative analysis of the impact of electronic health records (EHR) on healthcare quality and safety: Clinicians' lived experiences." *Health Services Insights* 15 (2022): 11786329211070722. https://doi.org/10.1177/11786329211070722

a nuanced stance on EHR privacy. This method should guarantee that EHR systems promote efficient and effective healthcare delivery while simultaneously protecting patient privacy and data security

References

Althaus C, Ball S, Bridgman P, Davis G, Threlfall D. *The Australian policy handbook: A practical guide to the policymaking process*. Taylor & Francis; 2022 Dec 21. https://doi.org/10.4324/9781003351993

Bani Issa, W., I. Al Akour, A. Ibrahim, A. Almarzouqi, S. Abbas, F. Hisham, and J. Griffiths. "Privacy, confidentiality, security and patient safety concerns about electronic health records." *International nursing review* 67, no. 2 (2020): 218-230. https://doi.org/10.1111/inr.12585

Cerchione, Roberto, Piera Centobelli, Emanuela Riccio, Stefano Abbate, and Eugenio Oropallo. "Blockchain's coming to hospitals to digitize healthcare services: Designing a distributed electronic health record ecosystem." *Technovation* 120 (2023): 102480. https://doi.org/10.1016/j.technovation.2022.102480

Cloninger, C. Robert, Drozdstoj Stoyanov, Kristina K. Stoyanova, and Kimberly K. Stutzman. "Empowerment of health professionals: Promoting well-being and overcoming burn-out." In *Person Centered Medicine*, pp. 703-723. Cham: Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-17650-0_42

Kandasamy, Kamalanathan, Sethuraman Srinivas, Krishnashree Achuthan, and Venkat P. Rangan. "Digital healthcare-Cyberattacks in Asian organizations: an analysis of vulnerabilities, risks, NIST perspectives, and recommendations." *IEEE Access* 10 (2022): 12345-12364. https://doi.org/10.1109/ACCESS.2022.3145372

Khang, Alex, Geeta Rana, R. K. Tailor, and Vugar Abdullayev, eds. "*Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem*." (2023). https://doi.org/10.1201/9781003356189

Klecun, Ela, Ya Zhou, Atreyi Kankanhalli, Yap Hwee Wee, and Ralph Hibberd. "The dynamics of institutional pressures and stakeholder behavior in national electronic health record implementations: A tale of two countries." *Journal of Information Technology* 34, no. 4 (2019): 292-332. https://doi.org/10.1177/0268396218822478

Kolasi, Klevis. "Structuration theory." *The Palgrave Encyclopedia of Global Security Studies*. Palgrave Macmillan. https://doi. org/10.1007/978-3-319-74336-3_360-1 (2020). https://doi.org/10.1007/978-3-319-74336-3_360-1

Konopik, Jens, and Dominik Blunck. "Development of an Evidence-Based Conceptual Model of the Health Care Sector Under Digital Transformation: Integrative Review." *Journal of Medical Internet Research* 25 (2023): e41512. https://doi.org/10.2196/41512

Ojokoh, Bolanle Adefowoke, Benjamin Aribisala, Oluwafemi A. Sarumi, Arome Junior Gabriel, Olatunji Omisore, Abiola Ezekiel Taiwo, Tobore Igbe et al. "Contact tracing strategies for COVID-19 prevention and containment: A scoping review." *Big Data and Cognitive Computing* 6, no. 4 (2022): 111. https://doi.org/10.3390/bdcc6040111

Pidun, Ulrich, Niklas Knust, Julian Kawohl, Evangelos Avramakis, and Andreas Klar. "*The untapped potential of ecosystems in health care*." Boston Consulting Group (2021). https://doi.org/10.1515/9783110775167-014

Solove, Daniel J., and Paul M. Schwartz. *Information privacy law*. Aspen Publishing, 2020.

Tutty, Michael A., Lindsey E. Carlasare, Stacy Lloyd, and Christine A. Sinsky. "The complex case of EHRs: examining the factors impacting the EHR user experience." *Journal of the American Medical Informatics Association* 26, no. 7 (2019): 673-677. https://doi.org/10.1093/jamia/ocz021

Upadhyay, Soumya, and Han-fen Hu. "A qualitative analysis of the impact of electronic health records (EHR) on healthcare quality and safety: Clinicians' lived experiences." *Health Services Insights* 15 (2022): 11786329211070722. https://doi.org/10.1177/11786329211070722