ISSN 3032-3533
Vol 2, No.1 (2025)

Professional Ethics and Health Law in the Digital Era and the Challenges of Patient Medical Data Protection In Electronic Medical Record System

1st Putro Sucy Cuts MZ
Postgraduate Student of Master Health Law
Universitas Pembangunan Panca Budi
Medan, Indonesia
putrosucirezky85@gmail.com

2nd Redyanto Sidi
Master of Health Law
Universitas Pembangunan Panca Budi
Medan, Indonesia
redysidi@gmail.com

***Abstract*— In the digital era, technological developments have brought major changes in the world of health, one of which is through the application of Electronic Medical Records (RME). This system allows for more efficient recording, storage, and access of patient medical data than conventional paper-based medical records. However, despite the benefits, the digitization of medical records poses new challenges, especially in the protection of patient data. The security of medical information is crucial because patient data is sensitive and must be protected from leaks, hacks, and misuse. In this context, medical professional ethics play an important role in ensuring that health workers comply with the principle of confidentiality, in accordance with bioethical standards such as autonomy, beneficence, nonmaleficence, and justice. On the other hand, health law has a fundamental role in regulating the protection of patient data in the RME system. Various regulations have been implemented globally, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and the Personal Data Protection Law (PDP Law) in Indonesia. This regulation aims to ensure that patient information is not misused and remains safe from cyber threats. However, challenges arise when the implementation of health laws is not balanced with the awareness of medical personnel and health facilities on the importance of regulatory compliance. The lack of cybersecurity infrastructure and weak internal policies in various health institutions further increase the risk of medical data breaches. As a solution, a comprehensive approach is needed to overcome this challenge, ranging from improving data protection policies, strengthening legal regulations, to developing information security technology in the RME system. Healthcare institutions must implement data encryption, multi-factor authentication, as well as strong firewalls to secure patient medical information. In addition, training for medical personnel on cybersecurity awareness and compliance with health laws is essential to prevent data leaks due to human negligence. With the synergy between professional ethics, health law, and more sophisticated security technology, patient data protection in the digital era can be significantly improved, thereby maintaining public trust in digital-based health services.**

Keywords: Electronic Medical Records, Medical Professional Ethics, Patient Data Protection.

I. INTRODUCTION

Digitalization in Health Services and the Implementation of RME as a Modernization Solution

The development of information technology has brought a major transformation in the health sector, one of which is through the implementation of Electronic Medical Records (RME). This system replaces the paper-based recording method with a digital format that is more efficient, accurate, and easily accessible to medical personnel. RME allows for real-time recording of patient data, speeding up the diagnosis and treatment process. In various developed countries, the digitization of the health system has become the standard, where the integration of RME with artificial intelligence (AI) technology and big data is further improving the quality of health services. The World Health Organization (WHO) emphasizes that digitalization of health can improve the accessibility of medical services, especially in the management of chronic diseases and emergency conditions that require fast and accurate medical information.[1]

Benefits of RME in Improving Health Service Efficiency

One of the main advantages of RME is its efficiency in improving healthcare services. With this system, medical personnel can easily access patients' medical history, laboratory results, and treatment recommendations without having to rely on physical documents that are vulnerable to loss or damage. In addition, RME enables collaboration between medical personnel and hospitals through a secure data sharing system, so that patients who change hospitals can still get optimal services without having to repeat the same examination.[2] The speed of data access also has an impact on reducing patient waiting times, increasing accuracy in prescribing drugs, and reducing medical errors due to incomplete or difficult to read records in manual documents.[3]

Challenges in the Implementation of RME, especially in Patient Medical Data Protection

Despite its many benefits, the implementation of RME also faces major challenges, especially in terms of patient data protection. Medical data is very sensitive information and can be misused if not properly maintained. The threat of cyberattacks, hacks, and data leaks is increasing along with the digitization of the health system. A study by the Ponemon Institute found that the healthcare sector is one of the main targets of cyberattacks, with increasing incidents of theft of patients' medical data used for various crimes, such as identity theft and insurance claims fraud.[4] In addition to external threats, internal factors such as the negligence of medical personnel in maintaining the security of data access are also a challenge in itself. Lack of awareness and understanding of digital security can increase the risk of

[1] World Health Organization. (2021). *Global Strategy on Digital Health 2020–2025*. Geneva: WHO
[2] Bates, D. W., & Sheikh, A. (2018). *Improving the Safety and Efficiency of Electronic Health Records*. *New England Journal of Medicine*, 379(16), 1589–1591.
[3] Menachemi, N., & Collum, T. H. (2011). *Benefits and Drawbacks of Electronic Health Record Systems*. *Risk Management and Healthcare Policy*, 4, 47–55.
[4] Ponemon Institute. (2022). *The Impact of Cybersecurity Threats on the Healthcare Sector*. Michigan: Ponemon Institute Research Report.

information leakage, both due to human error and the weakness of the technology systems used.[5]

The Importance of Professional Ethics and Health Law Perspectives in Regulating the Use of RME

In the face of these challenges, an approach from the perspective of medical profession ethics and health law is urgently needed to maintain a balance between data accessibility and patient privacy protection. In terms of professional ethics, the principle of confidentiality in bioethics emphasizes that medical personnel have a moral responsibility to maintain the confidentiality of patient information, so that access to medical data should only be given to the authorities and for legitimate medical interests.[6] On the other hand, legal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and the Personal Data Protection Law (PDP Law) in Indonesia serve as legal instruments in ensuring the security of patient data from the threat of misuse.[7] Therefore, strengthening regulations, increasing awareness of medical personnel, and adopting security technologies such as data encryption, multi-factor authentication, and advanced firewalls are steps that must be implemented immediately to create a safe and reliable digital health system.[8]

Problem Formulation

1. What are the main challenges in the implementation of electronic medical records related to patient data protection?
2. What is the relationship between professional ethics and health law in ensuring the security of medical data?
3. What are the solutions that can be implemented to improve patient data protection in the RME system?

Research Objectives

The purpose of this study is to analyze the ethical and legal challenges that arise in the implementation of electronic medical records (RME), identify applicable legal regulations related to the protection of patient medical data, and provide policy recommendations that can improve the security of patient data in the RME system. This research aims to explore ethical issues such as data privacy and confidentiality, as well as legal challenges related to compliance with existing regulations. In addition, this study will also examine the effectiveness of applicable legal regulations in protecting patient medical data and provide policy advice that can assist health institutions in improving the security and integrity of patient data, thereby creating a safer and more reliable system.

Research Benefits

The theoretical benefit of this research is to add academic references related to professional ethics and health law in the digital era. With the rapid development of technology, it is important to understand how professional ethics and health laws should be applied in the context of the use of electronic medical records (RME). This research is expected to provide deeper insights into the challenges and complexities that arise, as well as the role of regulation in protecting patient medical data. In addition, this research can also be a reference for future studies that discuss ethics and law in the field of digital health, enriching the existing literature.

Practically, this study provides benefits by providing guidelines for medical personnel in managing electronic medical records ethically and in accordance with applicable regulations. Medical professionals can use the results of this study to improve their understanding of managing patient data, both in terms of privacy and legal compliance. For health institutions, this research can be a reference to improve patient data protection policies, so as to create a safer and more efficient system. In addition, this study also provides input for the government in the formulation of health law policies related to medical data security, strengthening existing regulations to be more effective in overcoming threats to patient data.

II. LITERATURE REVIEW

Professional Ethics in Medical Practice in the Digital Era

Professional ethics in medical practice has a very fundamental role in maintaining moral standards and professionalism of medical personnel. One of the main frameworks in medical ethics is the principle of bioethics, which includes autonomy, beneficence, nonmaleficence, and justice. The principle of autonomy emphasizes that patients have the right to make decisions regarding their own health based on clear information and without coercion. Meanwhile, beneficence requires medical personnel to always prioritize the patient's welfare in every medical procedure. The principle of nonmaleficence emphasizes that medical personnel must avoid actions that can harm patients, either directly or indirectly. Finally, the principle of justice demands a fair and non-discriminatory distribution of health resources for all patients.[9]

In the digital era, the application of bioethical principles is increasingly complex, especially in the context of electronic medical records (RME) and the digitization of health services. The principle of autonomy requires medical personnel to ensure that patients understand how their medical data will be used, especially regarding privacy policies in digital systems. The principles of beneficence and nonmaleficence face challenges when patient data stored in electronic systems is vulnerable to leakage or misuse, which can cause negative impacts on patients. In addition, the principle of justice is relevant in ensuring that the digital system used in medical services is accessible to all levels of society, without any inequality in the application of health technology.[10]

One of the important aspects of medical professional ethics that is increasingly tested in the digital era is the confidentiality of patient medical information.

[5] Rimmer, A. (2019). *Cybersecurity in Healthcare: The Role of Human Factors*. *BMJ*, 366, l5043.
[6] Beauchamp, T. L., & Childress, J. F. (2019). *Principles of Biomedical Ethics (8th ed.)*. Oxford University Press.
[7] European Commission. (2018). *General Data Protection Regulation (GDPR)*. Brussels: EU Publications.
[8] Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). *Security Techniques for the Electronic Health Records*. *Journal of Medical Systems*, 41(8), 127.
[9] Beauchamp, T. L., & Childress, J. F. (2019). *Principles of Biomedical Ethics (8th ed.)*. Oxford University Press.
[10] Gillon, R. (1994). *Medical Ethics: Four Principles Plus Attention to Scope*. BMJ, 309(6948), 184-188.

Confidentiality is the main principle in maintaining trust between patients and medical personnel, where every health information provided by patients must be kept confidential and can only be accessed by authorized parties. In traditional systems, this principle is relatively easier to apply because a patient's medical record is physical and can only be accessed in a limited way. However, with the digitization of medical data, the risk of confidentiality violations is getting higher due to the threat of hacking, unauthorized access, and data leakage due to weaknesses in the cybersecurity system.[11]

The biggest challenge in maintaining confidentiality in the digital era is how to ensure that patient medical data remains safe without hindering the accessibility of medical personnel who need it for medical purposes. Beauchamp and Childress in *Principles of Biomedical Ethics* emphasize that the principle of confidentiality is not only about closing information, but also how data can be managed safely for the benefit of patients.[12] Therefore, a balance is needed between ease of access for medical personnel and the protection of patient privacy through strict regulations, such as the use of encryption systems, multi-factor authentication, and medical data access audits. By implementing strong bioethical principles and strengthening regulations related to medical data protection, challenges in the digital age can be overcome without sacrificing patient rights and safety.

Health Law and Medical Data Protection

The protection of medical data is an important aspect of health law, as it contains sensitive information about an individual's health condition. In Indonesia, efforts to protect personal data, including medical data, have been accommodated through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law provides a legal basis to protect individuals' privacy rights and provide greater control over personal data.[13] In addition to the PDP Law, the health sector in Indonesia is also regulated by specific regulations such as Law Number 17 of 2023 concerning Health and Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records. These regulations provide guidelines on how patient data should be stored, who has the right to access it, and under what conditions medical information can be disclosed to other parties.[14]

When compared to international regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, there are differences in approaches. The GDPR has broad scope and applies to all types of personal data, providing individuals with comprehensive rights, including the right to access, correct, and delete their data. Meanwhile, HIPAA is more specific about regulating health data and setting standards for protecting individual health information, including strict security and privacy requirements for entities that handle such data.

In Indonesia, although the PDP Law has been passed, its implementation is still in the development stage. One of the main challenges is the establishment of an independent supervisory agency that will be responsible for the supervision and enforcement of the PDP Law. Until now, the institution has not been fully operational, so supervision of compliance is still limited.[15]

Challenges in Electronic Medical Data Protection

The protection of electronic medical data faces significant challenges as cyber threats to electronic medical records (RME) increase. Cyberattacks such as system hacking, malware, ransomware, and phishing are the main threats that can compromise the integrity and confidentiality of patient information. For example, ransomware attacks can encrypt critical medical data and demand large ransoms, while targeted phishing can trick healthcare staff into revealing sensitive information.[16] Cases of medical data leaks have occurred in various countries, highlighting the vulnerability of health systems to cyber threats. In May 2021, Health Service Executives in the Republic of Ireland suffered a ransomware attack that resulted in patient data, including admission records and test results, being stolen and published online. In Singapore, in July 2018, the data of 1.5 million SingHealth patients, including Prime Minister Lee Hsien Loong's personal medical records, was stolen by hackers who used sophisticated tools to penetrate security systems.[17]

Indonesia is also not spared from this threat. In early 2022, around six million medical record data of Covid-19 patients were allegedly leaked and sold on the RaidForums website, showing that public institutions have not fully implemented the principles of personal data protection. In addition, in May 2021, around 279 million BPJS Kesehatan participant data was reported to have been leaked and traded on online forums, indicating a weak data security system in Indonesia's health sector.[18] Cyber threats to RME not only threaten patient privacy but can also disrupt healthcare operations. Systems that lack modern security features, the multitude of connected devices as potential entry points, and limited downtime for critical security updates make the healthcare sector vulnerable to cyberattacks.[19]

To address these challenges, strategic measures are needed, including the use of strong passwords, data encryption, avoiding account sharing, regular system updates, and effective system monitoring. Additionally, the implementation of digital certificates can strengthen the security of patient data by ensuring that only authorized users can access sensitive information.[20]

Solutions in Patient Data Protection

Patient data protection is a very important issue in the modern health care system. With the increasing amount of data being collected and processed, including medical history, diagnoses, and treatments, it is important to ensure that this information remains safe from unauthorized access. One solution that can be implemented is the use of advanced security technologies such as encryption and multi-factor

[11] Appari, A., & Johnson, M. E. (2010). *Information Security and Privacy in Healthcare: Current State of Research*. International Journal of Internet and Enterprise Management, 6(1), 4-17.
[12] Beauchamp, T. L., & Childress, J. F. (2013). *Ethical Issues in Modern Medicine: Contemporary Readings in Bioethics*. McGraw-Hill Education.
[13] https://siplawfirm.id/pentingnya-perlindungan-data-kesehatan-pribadi/?lang=id
[14] Siplawfirm (2025, February 26). The importance of protecting personal health data. https://siplawfirm.id/pentingnya-perlindungan-data-kesehatan-pribadi/?lang=id
[15] https://www.kompas.id/baca/polhuk/2024/08/02/
[16] Hastin Atas Asih, Indrayadi, Soraya, Khairunnisa (2024). *Evaluation of Patient Data Security on Electronic Medical Records with Systematic Literature Review* Scientific Journal fifo, 16(2), 104-110
[17] https://en.wikipedia.org/wiki/Medical_data_breach
[18] https://www.kompas.id/baca/polhuk/2022/01/07/data-rekam-medis-pasien-covid-19-diduga-bocor-segera-tuntaskan-ruu-perlindungan-data-pribadi
[19] https://www.kesia.id/?p=711
[20] https://www.kesia.id/?p=711

authentication. Encryption allows sensitive patient data to be encrypted at rest or in transit, so that only authorized parties can access it. Multi-factor authentication, on the other hand, provides an additional layer of security by requiring users to verify their identity through more than one method, such as a password and a physical device.[21]

In addition to the implementation of security technologies, clear policies and regular training for medical personnel also play an important role in protecting patient data. This policy should include strict guidelines regarding how patient data should be stored, accessed, and shared. Medical personnel must be regularly trained on the importance of maintaining the confidentiality of patient data and the steps to be taken to prevent data breaches. This training includes an introduction to the latest cybersecurity threats, as well as how to respond in the event of a data breach.[22]

The role of policy and training of medical personnel is not only limited to data protection in the digital context, but also touches on direct interaction with patients and the management of physical documents. Medical personnel must ensure that patients' physical records are kept safe, both through an organized archival system and strict access controls. Through strict policies and good training, medical personnel can be the first line of defense in protecting patient data from internal and external threats. With a combination of the implementation of robust security technologies and the strengthening of policy roles and training of medical personnel, healthcare institutions can create more effective patient data protection systems. This not only protects patient privacy, but also builds trust between patients and healthcare providers. Given the importance of medical data, these preventive measures will help maintain the integrity of the health system and improve the quality of services provided to patients.

III. METHOD

The research method used in this study is a qualitative approach with a literature study method. This approach was chosen to delve deeply into various aspects of professional ethics, health law, and patient medical data protection policies in the context of the use of electronic medical records (RME). This research will collect and analyze information from various relevant sources, including scientific journals, academic books, applicable regulations, as well as case reports related to medical data leaks. With this method, the study aims to gain a comprehensive understanding of the challenges faced by RME systems in terms of patient data protection.

The analysis will cover several dimensions, including legal regulations that govern medical data protection, professional ethics theories in the world of health, and various cases of medical data leaks that occur in practice. The data sources used will ensure the diversity of perspectives and depth of analysis required, by leveraging existing literature to understand issues related to patient data security. Thus, this research aims to contribute to understanding and compiling recommendations related to medical data protection in the digital era.

IV. RESULT AND DISCUSSION

Data Protection Challenges in RME

In the era of digitalization, Electronic Medical Records (RME) have become the backbone in the management of patient data in various health facilities. However, the implementation of RME cannot be separated from significant challenges, especially related to data protection. One of the main threats is the risk of data leakage due to cyberattacks and lack of system security. Attacks such as ransomware can encrypt medical data, resulting in loss of access to patients' vital information and the potential for large financial losses. For example, a ransomware attack against Change Healthcare in 2024 caused losses of up to 100 million USD per day. In addition, the theft of medical data is a serious concern because patient data has a high value on the black market. A report from Cyberhub Indonesia (2024) shows that cyberattacks on the health sector in Indonesia have increased by 45% in the last two years. Weaknesses in security systems, such as lack of encryption and inadequate access policies, magnify this risk. Therefore, the implementation of strong encryption and strict security policies is crucial to protect the integrity and confidentiality of patient data. However, advanced technology alone is not enough without being supported by the awareness and understanding of medical personnel regarding the importance of patient data protection. There are still many medical personnel who do not have awareness of the importance of maintaining the confidentiality of patient data.[23]

This lack of understanding can lead to negligence in handling data, such as the use of insecure devices or the practice of sharing information without permission, which ultimately increases the risk of data leaks. The case of medical record data leaks of COVID-19 patients in Indonesia in early 2022 is a serious warning about the importance of safe and ethical data management. As many as 6 million COVID-19 patient data, including sensitive information such as names, laboratory test results, and medical photos, was leaked to cyberspace. This incident reveals the weak digital security system, the lack of supportive regulations, and the low awareness of health workers, including nurses, about the importance of maintaining medical data.[24] To address these challenges, a holistic approach is needed that includes improving technology security infrastructure and ongoing education for medical personnel. The government also has an important role to play in educating the public and raising awareness about the importance of patient data privacy.[25]

Analysis of Professional Ethics in RME

In the era of digitalization of health services, the application of Electronic Medical Records (RME) has become the standard in patient information management. However, this transformation poses ethical challenges, especially regarding the gap between bioethical principles and data sharing practices in RME systems. Bioethical principles, such as autonomy, beneficence, non-maleficence,

[21] World Health Organization. (2019). Health Data Privacy and Security. WHO.
[22] National Institute of Standards and Technology (NIST). (2020). *Cybersecurity Framework for Healthcare*. NIST.
[23] Rita Puspita Sari (2025, February 02). https://cyberhub.id/berita/tata-kelola-data-layanan-kesehatan Compliance and Data Governance in Healthcare
[24] Aqilla Dwi Febrianti (2025, January 9). The Role of Nurses in Protecting Patient Privacy: https://kumparan.com/aqilla-dwi/peran-perawat-dalam-melindungi-privasi-pasien-solusi-kebocoran-data-rekam-medis-24GkZWG4KAQ Medical Record Data Leak Solution?
[25] Administrator (2024, February 12). Patient Data Privacy Policy: Carefully Protecting Personal Information https://praktekdokter.info/kebijakan-privasi-data-pasien/

and fairness, demand respect for the privacy and confidentiality of patient information. However, the need to share medical data for the sake of service efficiency is often contrary to this principle. For example, the use of cloud services for RME storage requires special considerations regarding privacy data, including the types of data that can be shared and to whom that data can be accessed.[26] This gap is exacerbated by the lack of clear guidelines regarding the limits and mechanisms for data sharing in the RME system. Without strict regulation, there is a risk of misuse of patient data, which can undermine public trust in the health system. Therefore, a balance is needed between the use of technology for the improvement of health services and respect for the rights of patients in accordance with the principles of bioethics.[27]

The role of medical personnel in ensuring the confidentiality of patient information is very crucial. The code of ethics for healthcare workers emphasizes the importance of maintaining patient privacy as the basis of professional relationships. When patients are confident that their data is safe, they are more open in providing important information, which has a direct impact on the quality of diagnosis and treatment.[28]For this reason, medical personnel must be given adequate training on ethics in RME management. In addition, health institutions need to implement periodic monitoring to ensure compliance with ethical and legal standards, as well as establish strict sanctions for data integrity violations. These measures are essential to maintain patient trust and ensure that information technology is used ethically in healthcare.[29] Thus, the implementation of RME must be accompanied by serious efforts in bridging the gap between bioethical principles and data sharing practices, as well as strengthening the role of medical personnel in maintaining the confidentiality of patient information. Only with this holistic approach can digital transformation in the healthcare sector run effectively and ethically.

Evaluation of Health Law Regulations

Health law regulations play an important role in ensuring access and quality of health services for the community. In Indonesia, this legal basis is contained in *the 1945 Constitution of the Republic of Indonesia*, especially Article 28H paragraph (1), which guarantees the right of every individual to proper health services. This foundation is the basis for the formation of various laws and regulations that govern the health care system in Indonesia.[30] The advantages of health law regulation in Indonesia include providing a clear framework for the implementation of health services and guaranteeing the rights of patients. However, there are weaknesses such as overlapping regulations, lack of synchronization between regulations, and suboptimal implementation. For example, despite the various laws governing the health sector, implementation on the ground often faces bureaucratic bottlenecks and a lack of resources.[31]

Several developed countries have successfully implemented effective health regulations. For example, health systems in countries such as the United Kingdom and Canada emphasize universality of access and high standards of care. They have comprehensive and integrated regulations, which ensure that every citizen gets quality health care without discrimination.[32] Lessons for Indonesia include the need to simplify regulations to avoid overlap, improve coordination between institutions, and adjust regulations to the development of health technology. In addition, it is important to increase the capacity of human resources in the health sector in order to implement regulations effectively. The COVID-19 pandemic has emphasized the need for countries to implement and scale up the core capacities of the International Health Regulation (IHR) at the national and regional levels in preventing, detecting, and responding to public health emergencies that plague the world.[33] By learning from the best practices of other countries and evaluating existing regulations, Indonesia can strengthen its health legal system. This will ensure that every individual gets proper health services, in accordance with the mandate of the constitution, and improves the welfare of society as a whole.

Solutions and Recommendations

In the era of digitalization of healthcare services, medical data security is a top priority to protect patient privacy and maintain the integrity of the health system. Increased regulation and compliance with medical data security standards is a crucial step in achieving this goal. In Indonesia, regulations such as Minister of Health Regulation No. 24 of 2022 concerning Medical Records and Law No. 27 of 2022 concerning Personal Data Protection have been passed to regulate the storage, protection, and access to electronic medical records (RME). In addition, Presidential Regulation No. 39 of 2019 concerning One Data Indonesia requires data interoperability between health systems with high security standards.[34] However, regulation alone is not enough without effective implementation. Healthcare institutions must ensure compliance with data integrity standards in the management of RMEs. This compliance has a direct impact on the quality of health services, patient privacy, and information security. Inaccurate or unprotected data can lead to misdiagnosis or treatment that puts patient safety at risk.[35] In addition to regulations, the development of security technologies also plays an important role in protecting medical data. Innovations in information technology, such as data encryption, multi-factor authentication systems, and real-time network monitoring, can improve the security of patient data in the healthcare industry. Investments in this technology not only ensure regulatory compliance but also build patient trust in the

[26] Media Penerbit Indonesia https://repository.mediapenerbitindonesia.com/374/1/

[27] Rani Tiyas Budiyanti, Excavator of Mahardika Herlambang, Nurhasmadiar Nandini, (2019). *Ethical and Legal Challenges in the Use of Electronic Medical Records in the Era of Personalized Medicine* , Journal of Vocational Health, 4 (1), 49-54.

[28] So Health Workers (2024) Code of Ethics for Health Workers Who Regulate Patient Privacy, Surprising Facts That Must Be Understood! https://jadinakes.id/kode-etik-tenaga-kesehatan-yang-mengatur-privasi-pasien/

[29] Annisa Yolanda (2024, December 11) Ethics in Managing the Integrity of Patient Data in Electronic Medical Records https://klikmedika.id/etika-dalam-pengelolaan-integritas-data-pasien-dalam-rekam-medis-elektronik/

[30] Irma Yani Sitompul (2024, October 6) The Role of Law in Guaranteeing the Right to Health Services in Indonesia https://pelitaharian.id/peran-hukum-dalam-menjamin-hak-atas-pelayanan-kesehatan-di-indonesia/

[31] Ruli Agustin, Taufiqurrohman Syahuri (2024). Implementation of the Health Law: Implications for Community Welfare and Perspectives of Health Workers in Indonesia BACARITALaw Journal , 4(2), 65-76.

[32] Dani Habibi, (2020). Reconstruction of the Health Legal System in Indonesia with a Comparative Approach to Health Systems in Developed Countries. Journal of Medika Hutama 1(3),156-162.

[33] World Health Organization (2024 January 11) Strengthening Health Security: International Experts Review the Core Capacity of Indonesia's International Health Regulation https://www.who.int/indonesia/id/news/detail/

[34] Annisa Yolanda (2025, February 6). Data Security Standards in RME Connected to SATUSEHAT. https://klikmedika.id/standar-keamanan-data-dalam-rme-yang-terhubung-dengan-satusehat/

[35] Annisa Yoanda (2024, December 10). The Importance of Compliance with Data Integrity Standards in the Management of Electronic Medical Records https://klikmedika.id/kepentingan-kepatuhan-terhadap-standar-integritas-data-dalam-pengelolaan-rekam-medis-elektronik/

healthcare system.[36] The importance of training for medical personnel cannot be ignored. Medical personnel must have competence in using health technology and understand best practices in maintaining the security of patient data. Simulation-based training has proven to be effective in improving clinical skills and response to emergency situations, ultimately positively impacting the quality of care and patient safety in hospitals.[37]

In addition, increasing security awareness through training for medical personnel and hospital staff on cybersecurity practices, such as how to identify phishing or manage credentials securely, is essential. RME implementations are often accompanied by this training to ensure that all parties involved understand their role in keeping data secure.[38] With a combination of strong regulations, advanced security technology, and effective training for medical personnel, healthcare institutions can create a secure environment for medical data. These measures not only protect patient privacy but also improve operational efficiency and overall healthcare quality. Therefore, collaboration between the government, healthcare providers, and medical personnel is urgently needed to achieve optimal medical data security standards.

V. CONCLUSION

Conclusion

Digitalization in healthcare provides tremendous benefits, including improved efficiency, coordination, and quality of medical services. However, along with these advances, there are major risks related to patient data protection that must be carefully managed. Therefore, professional ethics and health law play an important role in maintaining a balance between ease of access to data and protection of patient privacy. Without proper regulation, sensitive medical data can be misused, threatening patients' right to privacy and undermining trust in the healthcare system. To ensure that the Electronic Medical Record (RME) system can run properly and in accordance with ethical principles, stricter and comprehensive regulations are needed. These regulations should involve strong protection of patients' personal data, ensuring that medical information is only used for legitimate and beneficial purposes for patients. In addition, ongoing education for medical personnel regarding data protection and the safe use of technology is essential to ensure that they can act in accordance with applicable ethical and legal standards. With stricter policies and support for the development of safer technologies, RME systems can be implemented more effectively, without compromising patient privacy. Clear regulations and adequate training will help medical personnel to better understand their responsibilities in maintaining the confidentiality of patient information. This will strengthen public trust in the digitalization system of health services, as well as minimize potential risks that can arise due to data leakage or misuse.

Overall, while digitalization in the healthcare sector offers great potential to improve the quality of services, it is important to always prioritize ethical principles and data protection. Only in this way can we ensure that technology works properly for the benefit of patients, without neglecting their basic rights that must always be guarded and respected.

Suggestion

As a step towards safer and more efficient management of patient data, healthcare institutions must improve their data security policies by implementing better protection systems. This step is important to protect highly sensitive medical information from the threat of leakage or misuse. In addition to adopting stronger encryption technologies, institutions also need to implement strict access control procedures, such as layered authentication and data access restrictions based on need. Data security should be a top priority, given the potential for a huge impact on patient privacy and trust in the event of a breach. In addition, the government also has a key role in overcoming security challenges in the Electronic Medical Record (RME) system. Given the rapid development of technology and increasingly sophisticated cyber threats, existing regulations need to be updated to remain relevant to new challenges in the digital world. Governments must ensure that regulations related to medical data security include adequate standards to deal with cyber threats, with special attention paid to the security of patients' personal data as well as their rights. This policy must also provide clear sanctions for parties proven to have committed violations, to encourage stricter implementation in the field.

Periodic training for medical personnel is also very important to strengthen understanding of professional ethics and medical data security. Medical personnel who have a good understanding of the importance of maintaining the confidentiality of patient information will be more careful in using the RME system and maintaining data integrity. This training should cover topics such as best practices in data management, how to protect patient information from potential leaks, and an understanding of applicable regulations and professional codes of ethics. With continuous training, medical personnel can be better prepared to face the challenges of the digital age and ensure that they act in accordance with high ethical standards.

REFERENCES

Buku

1. World Health Organization. (2021). *Global Strategy on Digital Health 2020–2025*. Geneva: WHO.
2. Ponemon Institute. (2022). *The Impact of Cybersecurity Threats on the Healthcare Sector*. Michigan: Ponemon Institute Research Report.
3. Rimmer, A. (2019). *Cybersecurity in Healthcare: The Role of Human Factors*. *BMJ*, 366, l5043.
4. Beauchamp, T. L., & Childress, J. F. (2019). *Principles of Biomedical Ethics (8th ed.)*. Oxford University Press.
5. European Commission. (2018). *General Data Protection Regulation (GDPR)*. Brussels: EU Publications.
6. Beauchamp, T. L., & Childress, J. F. (2019). *Principles of Biomedical Ethics (8th ed.)*. Oxford University Press.
7. Beauchamp, T. L., & Childress, J. F. (2013). *Ethical Issues in Modern Medicine: Contemporary Readings in Bioethics*. McGraw-Hill Education.

Website

[36] Admin (2024, July 8) Information Technology Innovation in Improving Patient Data Security in the Health Industry https://ilmusisteminfo.com/2024/07/08/inovasi-teknologi-informasi-dalam-meningkatkan-keamanan-data-pasien-di-industri-kesehatan/

[37] https://www.persi.or.id/wp-content/uploads/2024/11/

[38] Annisa Yolanda (2024, December 24). Electronic Medical Records: Improving the Security of Patient Data https://klikmedika.id/rekam-medis-elektronik-meningkatkan-keamanan-data-pasien/

8. Siplawfirm (2025, Februari 26). Pentingnya Perlindungan Data Kesehatan Pribadi. https://siplawfirm.id/pentingnya-perlindungan-data-kesehatan-pribadi/?lang=id
9. https://setjen.kemkes.go.id/berita/detail/menavigasi-privasi-data-kesehatan-melalui-pia
10. SSL (2025, Januari 1). Serangan Kesehatan Healthcare Sedang Berkembang - Sertifikat Digital Dapat Membantu. https://www.ssl.com/id/artikel/serangan-siber-di-bidang-kesehatan-semakin-meningkat-sertifikat-digital-dapat-membantu/
11. https://en.wikipedia.org/wiki/Medical_data_breach
12. Rini Kustiasih (2022, Januari 7) Data Rekam Medis Pasien Covid-19 Diduga Bocor, Segera Tuntaskan RUU Perlindungan Data Pribadi https://www.kompas.id/baca/polhuk/2022/01/07/data-rekam-medis-pasien-covid-19-diduga-bocor-segera-tuntaskan-ruu-perlindungan-data-pribadi
13. Kesia (2024, Januari 24) Tips Menjaga Keamanan Rekam Medis Elektronik Pasien https://www.kesia.id/?p=711
14. Rita Puspita Sari (2025, Februari 02). Kepatuhan dan Tata Kelola Data dalam Layanan Kesehatan https://cyberhub.id/berita/tata-kelola-data-layanan-kesehatan?
15. Aqilla Dwi Febrianti (2025, Januari 9). Peran Perawat dalam Melindungi Privasi Pasien: Solusi Kebocoran Data Rekam Medis https://kumparan.com/aqilla-dwi/peran-perawat-dalam-melindungi-privasi-pasien-solusi-kebocoran-data-rekam-medis-24GkZWG4KAQ?
16. Administrator (2024, Februari 12). Kebijakan Privasi Data Pasien: Melindungi Informasi Pribadi dengan Cermat https://praktekdokter.info/kebijakan-privasi-data-pasien/
17. Media Penerbit Indonesia.com https://repository.mediapenerbitindonesia.com/374/1/
18. Jadi Nakes (2024) Kode Etik Tenaga Kesehatan yang Mengatur Privasi Pasien, Fakta Mengejutkan yang Wajib Dipahami! https://jadinakes.id/kode-etik-tenaga-kesehatan-yang-mengatur-privasi-pasien/
19. Annisa Yolanda (2024, Desember 11) Etika dalam Pengelolaan Integritas Data Pasien dalam Rekam Medis Elektronik https://klikmedika.id/etika-dalam-pengelolaan-integritas-data-pasien-dalam-rekam-medis-elektronik/
20. Irma Yani Sitompul (2024, Oktober 6) Peran Hukum dalam Menjamin Hak atas Pelayanan Kesehatan di Indonesia https://pelitaharian.id/peran-hukum-dalam-menjamin-hak-atas-pelayanan-kesehatan-di-indonesia/
21. World Health Organization (2024 Januari 11) Memperkuat Keamanan Kesehatan: Pakar Internasional Mengkaji Kapasitas Inti International Health Regulation Indonesia https://www.who.int/indonesia/id/news/detail/
22. Annisa Yolanda (2025, Februari 6). Standar Keamanan Data dalam RME yang Terhubung dengan SATUSEHAT. https://klikmedika.id/standar-keamanan-data-dalam-rme-yang-terhubung-dengan-satusehat/
23. Annisa Yolanda (2024, Desember 10). Kepentingan Kepatuhan terhadap Standar Integritas Data dalam Pengelolaan Rekam Medis Elektronik https://klikmedika.id/kepentingan-kepatuhan-terhadap-standar-integritas-data-dalam-pengelolaan-rekam-medis-elektronik/
24. Admin (2024, Juli 8) Inovasi Teknologi Informasi dalam Meningkatkan Keamanan Data Pasien di Industri Kesehatan https://ilmusisteminfo.com/2024/07/08/inovasi-teknologi-informasi-dalam-meningkatkan-keamanan-data-pasien-di-industri-kesehatan/
25. https://www.persi.or.id/wp-content/uploads/2024/11/
26. Annisa Yolanda (2024, Desember 24). Rekam Medis Elektronik: Meningkatkan Keamanan Data Pasien https://klikmedika.id/rekam-medis-elektronik-meningkatkan-keamanan-data-pasien/

Jurnal

27. Guswan Hakim, Jabalnur, Oheo Kaimuddin Haris, Ruliah, Sukring, Muthaharry Mohammad, (2023). *Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa dan Indonesia*. Halu Oleo Legal Research Vol.5, No.2, 443-453.
28. Bates, D. W., & Sheikh, A. (2018). *Improving the Safety and Efficiency of Electronic Health Records*. *New England Journal of Medicine*, 379(16), 1589–1591.
29. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). *Security Techniques for the Electronic Health Records*. *Journal of Medical Systems*, 41(8), 127.
30. Appari, A., & Johnson, M. E. (2010). *Information Security and Privacy in Healthcare: Current State of Research*. International Journal of Internet and Enterprise Management, 6(1), 4-17.
31. Gillon, R. (1994). *Medical Ethics: Four Principles Plus Attention to Scope*. BMJ, 309(6948), 184-188.
32. Menachemi, N., & Collum, T. H. (2011). *Benefits and Drawbacks of Electronic Health Record Systems*. *Risk Management and Healthcare Policy*, 4, 47–55.
33. Hastin Atas Asih, Indrayadi, Soraya, Khairunnisa (2024). *Evaluasi Keamanan Data Pasien Pada Rekam Medis Elektronik Dengan Systematic Literature Review* Jurnal ilmiah fifo, 16(2), 104-110.
34. World Health Organization. (2019). *Health Data Privacy and Security*. WHO.
35. National Institute of Standards and Technology (NIST). (2020). *Cybersecurity Framework for Healthcare*. NIST.
36. D. C. L. P. Lee et al., *Cybersecurity and Privacy Issues in Healthcare: A Survey of Current and Future Challenges*, Journal of Medical Internet Research, 2020.
37. R. K. Gupta, *Privacy and Security in Health Information Systems*, Health Information Management Journal, 2021.
38. Rani Tiyas Budiyanti, Penggalih Mahardika Herlambang, Nurhasmadiar Nandini, (2019). *Tantangan Etika dan Hukum Penggunaan Rekam Medis Elektronik dalam Era Personalized Medicine.* Jurnal Kesehatan Vokasional, 4 (1), 49-54.
39. Ruli Agustin, Taufiqurrohman Syahuri (2024). *Implementasi Undang-Undang Kesehatan: Implikasi Terhadap Kesejahteraan Masyarakat Dan Perspektif Tenaga Kesehatan Di Indonesia*. BACARITALaw Journal , 4(2), 65-76.
40. Dani Habibi, (2020). *Rekonstruksi Sistem Hukum Kesehatan Di Indonesia Dengan Pendekatan*

Perbandingan Sistem Kesehatan Di Negara Maju. Jurnal Medika Hutama 1(3),156-162.