Available at https://journalenrichment.com/index.php/jr/

Enrichment
Journal of Multidisciplinary Research and Development

Enrichment: Journal of Multidisciplinary Research and Development

HOSPITAL PATIENT DATA SECURITY EVALUATION TO ACHIEVE SDGs 3.8.1 "GOOD HEALTH AND WELLBEING"

Muhammad Fakhri Rasyad*, Ratna Lindawati Lubis
Telkom University, Bandung, Indonesia
Email: fakhrirasyad@student.telkomuniversity.ac.id*

ABSTRACT

One of the major problems in health digitalization is data security, especially in hospitals, which are highly vulnerable to cybercrime, such as patient data leaks. This concern also affects Permata Cirebon Hospital in its efforts to achieve quality healthcare services aligned with SDG 3.8.1. This research aims to evaluate patient data security based on existing hospital policies and procedures. A qualitative method with an evaluative approach was used, involving interviews with four informants, observations, and documentation reviews. Data were analyzed thematically to identify patterns and issues. The evaluation found that Permata Cirebon Hospital has implemented several key measures, including VPN usage, access restrictions, and dashboard-based monitoring. However, significant gaps remain. Incident reporting is conducted but lacks standardized procedures and is largely reactive. The hospital does not perform routine audits, and evaluations are not guided by specific performance indicators. Staff training on data security is minimal and inconsistent, raising concerns about human error risks. Additionally, cryptographic techniques for protecting sensitive data remain underdeveloped. These findings indicate that while initial efforts toward securing patient data exist, they are insufficient to meet modern data security standards. The research recommends enhancing system resilience through blockchain-based encryption, establishing a formal incident response protocol, conducting regular audits, and providing comprehensive training for staff. Strengthening these areas is essential to ensure sustainable, secure, and high-quality healthcare services.

Keywords: *data security; SDGs 3.8.1; health digitalization; security management*

INTRODUCTION

The rapid advancement of digitalization in healthcare has significantly transformed hospital operations, improving efficiency and accessibility. However, this transformation also brings substantial challenges, particularly regarding patient data security. Hospitals manage vast amounts of sensitive medical information, making them prime targets for cyber threats, including data breaches, ransomware attacks, and unauthorized access. In Indonesia, multiple cases of patient data leaks have raised serious concerns about the effectiveness of existing security measures. A notable example was the 2021 data breach, where millions of government health insurance records were compromised and sold on illegal platforms. These incidents highlight the urgent need for stronger cybersecurity frameworks in healthcare institutions to ensure compliance with regulations and maintain patient trust. This research evaluates the data security management practices at Permata Cirebon Hospital, assessing their effectiveness in safeguarding patient information and identifying areas for improvement.

One of the big problems in digitalization is data security, which is an important aspect of information security management. The phenomenon of the Indonesian population's largest leak of personal data occurred in 2021. A total of 279 million Government Health Insurances user data were leaked in mid-May 2021. According to Lidwina (2021), data including Population Identification Number (PIN-ID), name, location, phone number, email, and photo were sold on the Raid Forums platform for 70-80 million rupiah. Patient information is sold on dark web platforms in various countries, with an estimated starting price of 10 million rupiah. Patient data is then used for various purposes (Sutandra, 2019). Subsequently, Indonesia was ranked among the top 10 countries with the highest incidence of data breaches on the internet.

Surfshark, a cybersecurity company, reported that 1.04 million accounts in Indonesia experienced data breaches in the second quarter of 2022.

The Law is expected to ensure the smooth process of national development, guarantee and protect the rights of Internet service users, and take firm action against cybercrime perpetrators. Based on the nature of cybercrime, which includes unlimited crimes, complex, integrated, and sustainable measures are needed (Widayati et al., 2020). The Electronic Information and Transaction Law No. 11/2008 regulates cybercrime, which prohibits people from intentionally and without right accessing computers and electronic systems by violating, breaking through, or bypassing security, which is subject to sanctions. The Law aims to facilitate national, protect the rights of Internet service users, and take decisive action against cybercriminals. The nature of cybercrime requires coordinated & sustained action due to its unlimited scope.

Data security is the process of protecting the data in a system to prevent unauthorized access to and modification of the stored information. Every information system owner and manager must ensure the security of stored data and restrict access to authorized individuals to protect against intentional or unintentional harm. Health information is particularly vulnerable to leaks, and the consequences are even more severe when the compromised information involves highly personal patient information (Ravlindo, 2021). The Indonesian Ministry of Health prioritizes system security and personal data protection in system integration. The Health Digital Transformation Strategy of 2024 ensures that electronic health records are protected through data security ownership and stewardship protection in any healthcare institution.

The SDGs program continues the Millennium Development Goals (MDGs) that operated from 2000 to 2015 with its 5 principles of people, planet, prosperity, peace, and partnership. These five principles are believed to balance economic, social, and environmental aspects. Digital transformation in healthcare has experienced a significant increase along with the major goal of the SDGs 3.8.1 program to create quality health services with a fairly high level of risk occurring in healthcare facilities such as hospitals (Oluomachi & Ahmed, 2024). Health is an important factor that serves as a parameter of the welfare of an urban community. All individuals have the right to access health services. All health-related issues in the Sustainable Development Goals (SDGs) are included in Goal 3, which addresses public nutrition, national health systems, family planning, sanitation, and clean water. In addition, the rapid development of wearable devices and health applications requires attention due to the potential for personal data leakage. Adherence to procedures for protecting personal data in hospitals will be required for the protocol (Apsari et al., 2022).

Hospitals have made several efforts to secure patient data, so evaluating and researching the use of an integrated system is imperative because patient data has legal value in hospitals. Current hospital policies are considered unable to properly regulate patient data security in Indonesia. This research aims to evaluate the effectiveness of patient data security management at Permata Cirebon Hospital by assessing existing policies, identifying vulnerabilities, and proposing improvements to enhance data protection. Specifically, it seeks to analyze the hospital's compliance with security standards, the effectiveness of current incident reporting mechanisms, the adequacy of staff training, and the implementation of encryption technologies. Through this evaluation, the research provides recommendations to strengthen data security and align hospital practices with modern cybersecurity frameworks. Given the legal and ethical implications of data breaches in healthcare, a structured approach to data security management is essential to safeguard patient privacy and trust.

METHOD

Design and Approach

Researchers employed qualitative methodologies characterized by an evaluative framework. Qualitative research is inherently holistic, placing significant emphasis on processes; this method facilitates an interactive examination of the relationships between the variables involved in the subject of study, as they mutually influence one another. The author's investigation adopts an event-based case study approach, cultivating an understanding of the operational dynamics and functionalities of the subject within its authentic context. Case studies are systematically developed through three distinct stages according to:

A. Collecting raw data about the written case research program

B. Shortening the raw data for classification and processing of manageable data

C. Writing a descriptive case research narrative for the reader based on all the information needed to understand the program holistically

Observation can be done with or without participation. In this research, the authors used a participant observation technique in which they participated in ongoing activities. Then, the author conducted interviews with the aim of obtaining the expected information under the existing conditions. Data collection with documentation is carried out to view and analyze previously obtained data so that the data used in the research is complete and more comprehensive. According to Wahyuni (2022), documents can be in the form of writings, pictures, and works; they can also be life histories, biographies, regulations, policies, and stories. Documents can also be in the form of works such as works of art, live pictures, or sketches. Document research complements the other two methods in qualitative research, namely observation and interviews.

Based on the research setting, the authors used an uncontrived setting approach. This approach is conducted in a natural setting where the occurring phenomena are regular (going on as usual). The implementation time of this research uses a cross-sectional approach. Research data that shows a certain point in time Nasution (2023). According to Rodliyah & Saraswati (2022), Purposive sampling is a technique used to achieve specific goals and objectives. This technique identifies stages based on the case to be studied.

Tabel 1. Data Participants

Participant	Role	Duration of Interview
ZR	Director of Finance & General Affairs	60 minutes
DW	IT Manager	34 minutes
DC	System Analyst	33 minutes
WA	Head of Medical Records Unit	21 minutes

Documentary data collection is used to review and analyze previously collected data to ensure that the data used in the research is more thorough and comprehensive. This research uses both primary and secondary data. Primary data were obtained through interviews with four hospital staff directly involved in data security, participant observation of hospital operations, and internal documents such as SOPs and incident reports. Secondary data were gathered from literature reviews, including academic journals, books, previous studies, and relevant legal and policy documents on data security and SDG 3.8.1. These sources support data triangulation and provide a comprehensive view of the hospital's data security practices.

Data Analysis

Data analysis facilitates the understanding of text, sound, and other types of data. The first step involves collecting and preparing data for subsequent analysis. This included transcribing interviews, processing field notes, and categorizing visual materials from various data sources. Interviews were conducted in Indonesian and then translated into English.

Interview transcripts or drafts were reviewed to identify important words, phrases, or sentences related to the research questions. These words or phrases were then coded. The codes were used to describe the setting, participants, categories, and themes for analysis. Interpretation in qualitative research aims to provide an explanatory analysis of the data collection results that have been processed. This includes discussions that explain the chronology of events, comprehensive analysis of various themes accompanied by sub-themes, specific illustrations, different perspectives, various quotes, and examination of interrelated themes presented through figures or tables related to the research material.

RESULT AND DISCUSSION

Data was collected for this research through in-depth interviews with four resource persons designated as representatives of Permata Cirebon Hospital.

Table 2. Information of the Interview

Code	Role	Responsibility
ZR	Director of Finance & General Affairs	Experienced in leading Permata Cirebon Hospital for 9 years as Director of Finance & General Affairs. He has a role in overseeing finance & general affairs, making strategic business decisions, as well as conducting evaluations of database security and technology information systems at the hospital
DW	IT Manager	Responsibility as Tech & Information Manager at Raudhatussyfaa Sehat Bersama, Ltd., which is also the holding company of Permata Cirebon Hospital. Since 2022, He was responsible for managing technology information system development strategies in the hospital, focusing on data and system security.
DC	System Analyst	As a system analyst staff at Raudhatussyfaa Sehat Bersama, Ltd., He has role in creating systems and business workflows for Permata Cirebon Hospital, as well as monitoring and controlling the front end of the Hospital Information System (HIS)
WA	Head of Medical Records Unit	Head of the Medical Records Department, responsible for monitoring and ensuring that patient medical record workflows and procedures operate optimally in accordance with applicable Standard Operating Procedures (SOP). He has been working at Permata Cirebon Hospital since 2015, previously role as a front office service officer

Predetermined inclusion criteria were employed to select the four respondents who provided comprehensive information about the research subject. Five themes addressed data security.

Theme 1: Reporting of Patient Safety Incidents

*"…Documentation (of information security events) is in the form of a chronology from us, a sequence of events in the form of an initial report, and when it is over (the incident), there will be another report…" **(DW)***

*"…Information security events are documented in incident reports or chronological reports of data security breach incidents…" **(ZR)***

*"…There are penalties (for those who make mistakes), but only after a case audit has been completed…" **(WA)***

*"…For example, when our system is hacked, we are afraid that our data will be used (by irresponsible people). We will try to report (to the authorities) or, for example, our employees sell data…" **(DW)***

*"…But if, for example, it happens (a data security incident), maybe we should consult the vendor too because almost everything is already systemized, so it should be anticipated for the time, date, and the last update that we can see…" **(DC)***

Theme 2: Challenges to the Implementation of Patient Data Security

*"…The challenges at the beginning of the implementation were doctors who did not want to use (the information system provided by the hospital) and also the adaptation of implementers in units that took time…" **(ZR)***

*"…In the beginning, the system was slow, especially at the beginning of socialization; the system was down during services with patients in the polyclinic." **(DW)***

*"…The main challenge is actually because we use vendors, so it takes time to communicate if there is an incident. Our vendors are used in not only Permata Hospital Cirebon but also other hospitals…" **(WA)***

*"…So sometimes there are cases that are formed from SOP errors. If from outside, there are usually viruses, malware, and others…" **(DC)***

Theme 3: Socialization and Training Regarding Patient Data Security

*"…For awareness (about the importance of data security), we have often explained it to all officers; if there is a change, we remind them again. But if there is training from outside, we have never participated in it, but if it is internal, we adjust it to the relevant units…" **(DW)***

*"…Staff are rarely trained on data security…" **(ZR)***

*"…In the Medical Records Unit, we have monthly meetings (to socialize procedures to all Medical Records Unit staff), evaluate what cases have occurred, and convey that data in the hospital is confidential…" **(WA)***

*"…I personally have not participated in any training related to data security protection. I don't know about other staff, but I usually go online to find out and upgrade data protection information..." **(DC)***

Theme 4: Evaluation of Patient Data Security Incidents

> *"…There is no specific method (for evaluating information security incidents). Customized to the reported incident…"* ***(ZR)***
> *"…We don't have a specific time (for evaluation), but there must be one day for us to discuss, which may not only be patient data security but, in general, is not fixed to one day or one week depending on the conditions of the case in the real area…"* ***(DC)***
> *"…In the medical record unit itself, there is no (periodic audit mechanism from IT); every time there is a problem, we ourselves report it to the IT unit…"* ***(WA)***
> *"…While there is no monitoring system for improvements to the weaknesses that have been identified, daily monitoring and evaluation are only from internal IT…"* ***(DW)***

Reporting of Patient Safety Incidents

The findings indicated that reporting patient data security incidents was conducted systematically from workers to the head of the relevant unit. Furthermore, the unit head delivers the report to the Hospital Quality Committee for an audit, which is forwarded to the Hospital Board of Directors thereafter. The Incident Chronological Report contains a written account of the cause, the implemented solution, and the final case report. The incident reporting system is very important because it lets you compare how well different systems are working, find problems with the systems, and gather information about how often and how bad incidents are to improve performance.

The hospital implemented penalties on persons identified as delinquent following a case audit. The hospital will report to the authorities following a breach occurrence, including system hacking, data hacking, data sales, or when evidence of the perpetrator is available. Notifying authorities and regulators is a crucial measure to avert data breaches. Evaluate and enhance legal and regulatory frameworks to tackle the challenges posed by contemporary digital health systems and enhance their security against potential data (Hossain & Hong, 2019).

The hospital has not established a unique Standard Operating Procedure (SOP) for handling data security incidents; nonetheless, vendors frequently assist with technical system concerns. This reporting approach emphasizes the significance of interdivisional collaboration, systematic recording, vendor participation, and the necessity to establish a specific SOP for information security incidents.

Challenges to the Implementation of Patient Data Security Management

Numerous challenges emerge in the implementation of information systems and data security within hospital settings. This situation includes physicians who encounter difficulties with the Hospital Information System (HIS) provided by the institution when compared to systems employed in other healthcare establishments. Furthermore, challenges manifest in the form of personnel acclimatization, which necessitates time to fully comprehend the new system, as well as technological issues such as intermittent system sluggishness and outages. Research by Chakraborty (2023) underscores several technological obstacles faced during system implementation, including users' unfamiliarity with hospital information systems, the duration required to attain proficiency in system utilization, and the integration of HIS into the daily operations of the hospital. Challenges concerning data security in the adoption of Hospital Management Information Systems encompass the risk of data breaches and cybercriminal activity, thereby necessitating the enhancement of protocols related to data accessibility. Additionally, health-related information remains vulnerable to hacking or leakage, prompting the need for robust cybersecurity measures prior to the comprehensive digitization of the healthcare system.

SOPs remain challenging for users to implement. Meanwhile, SOPs are established to provide guidelines for implementing information security tasks and to mitigate and prevent information security threats (Ardianto & Nurjanah, 2024). Consequently, the oversight and enhancement of officer discipline must always be maintained.

The vendor system has advantages, yet it prolongs communication regarding changes or issues within the system. Connecting patient data with regulators facilitates data exposure without the hospital's awareness. External risks, including viruses, malware, hacking, and data theft, pose significant hurdles for hospitals in safeguarding patient data security. Extensive health data is susceptible to breaches or leaks that may expose patients' personal information (Indriyajati et al., 2023). These challenges require a focus on enhancing discipline regarding SOPs, facilitating user adaptation to the new system, and ensuring effective interaction with relevant vendors.

Socialization and Training Regarding Patient Data Security

The socialization and training of human resources about patient data security at Permata Hospital Cirebon have demonstrated a commendable starting attempt; nonetheless, substantial enhancement is still necessary. Socialization has typically occurred inside various units, encompassing regular internal meetings, monitoring, and reviewing data security incidents to enhance staff understanding of the significance of patient data protection. The socialization of data security is seen as crucial as it enhances user awareness regarding dangers to patient data security. Enhanced user comprehension can mitigate the danger of cybercrime and the inappropriate use of patient data that contradicts the objectives of health services. Socialization aids users in comprehending the significance of upholding data confidentiality, accuracy, and accessibility, which are fundamental to electronic medical record administration (Pradita et al., 2022). The examination of the interview findings indicates that this socialization effort has not been executed systematically and uniformly across all units, particularly between the IT team and the Medical Records Installation.

Hossain & Hong (2019) asserted that the deficiency of adequate resources constitutes a significant obstacle to preventing data security breaches. These resources encompass personnel capable of proficiently employing health data management technologies while ensuring data safety and security are not compromised. Incorporating data security competencies into educational and training programs is essential, as is fostering a workplace culture that values data security. The lack of training may result in incompetence, particularly among new employees or those without prior medical experience. Arefin (2024) emphasized that equipping personnel with essential skills develops a culture of creativity and adaptability, thus enhancing overall security protocols. To resolve this issue, enhancements are required in formal training, structured periodic socializing, and developing a more comprehensive SOP in compliance with relevant rules. A sustained collaborative strategy is the solution to this difficulty.

Evaluation of Patient Data Security Incidents

The hospital's evaluation process remains unstructured and unscheduled. It is predominantly reactive, conducted exclusively in response to patient data security incidents or alterations in regulatory policy. Peña et al. (2019) state that evaluating patient data security events requires assessing vulnerabilities and disregards that may threaten the confidentiality, integrity, and availability of clinical information.

A regular audit or risk assessment mechanism has not been implemented. Research indicates that periodic audits are essential for detecting patient data breaches, as they provide a systematic approach for monitoring and identifying unauthorized access to sensitive information. Audits serve as a proactive measure to protect patient data by regularly evaluating system configurations and data management practices. This process helps identify anomalies or suspicious activities that may indicate a breach. Periodic audits are acknowledged as an effective strategy for detecting breaches and establishing a comprehensive approach to data protection. Healthcare should prioritize regular audits to timely prevent breaches and enhance the security of information and patient data in hospitals (Oluomachi & Ahmed, 2024).

Tabel 3. Data Security Standard

Object	Status	Indicators
Policies	There are no specifics yet; the policy is still in general aspect	It needs to be prepared by management because it is special and absolutely serves as a guide for user use
SOP	Done	• SOP for User Access Rights • SOP for Information Data Security • SOP for Reporting HIS Problems
Limited Access Control	Done	Users are categorized into:

		• Superadmin • Management • Staff (Tech Information & Medical Records Department) • Doctors, nurses, laboratory analyst, pharmacy, etc.
Security Management	Done	Firewall, anti-virus protection external device (USB)
Information security incident management	Done	Structured from existing reports, then to the Tech Information department, and next to management
Crypto graphy	The requirements have not yet been met	• Data encryption has been carried out by the IT unit • Use of digital signatures its been gradual, but still less at the verification stage and authentication • Cryptographic techniques for incident reports • User authentication at will perform login access, and exiting the system is still not done

Source: ISO/IEC 27002 (2013)

The IT team primarily conducts the evaluation process internally, with external parties involved only when vendor assistance is necessary for specific events. The effectiveness of improvement initiatives is not evaluated through specific KPIs (Key Performance Indicators) but rather assessed based on the successful execution of system trials, including the "User Acceptance Test". This indicates the necessity for a more organized evaluation system, particularly in establishing audit mechanisms, ongoing monitoring, and definitive performance indicators to guarantee optimal patient data security.

CONCLUSION

This research highlights several critical gaps in patient data security management at Permata Cirebon Hospital. Although basic measures such as VPN usage, access control, and internal reporting are in place, the absence of structured evaluation, formal incident response protocols, and consistent staff training undermines the effectiveness of these efforts. The findings show that data security is still treated reactively rather than proactively, with evaluations conducted only after incidents occur and without performance indicators to track improvements.

A key contribution of this research is the identification of interrelated weaknesses—where technical measures are not supported by policy enforcement or staff competency and where SOPs exist but lack integration across departments. These gaps indicate the need for a more holistic and strategic approach to data protection in hospitals. To enhance data security, the hospital should implement regular audits and risk assessments, develop clear SOPs for incident response, invest in advanced encryption methods such as blockchain, and provide mandatory, periodic training for all staff. Additionally, establishing a dedicated data protection unit could help monitor compliance and respond swiftly to security incidents. These recommendations are essential for protecting sensitive health information and achieving the broader goal of SDG 3.8.1—ensuring quality healthcare through secure and trusted systems.

REFERENCES

Apsari, A. F., Lutfiyah, A., Khalifatullah, A. W., Nugrahaningtyas, E., Qoriah, E. A., Zukhri, G. S., & Ridho, M. R. R. (2022). Perlindungan Data Pribadi Pasien Terhadap Serangan Cyber Crime. *Sanskara Hukum Dan HAM*, *01*(02), 47–53.

Ardianto, E. T., & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X. *Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan*, *3*(2), 18–30. https://doi.org/https://doi.org/10.47134/rammik.v3i2.541

Arefin, S. (2024). Strengthening Healthcare Data Security with Ai-Powered Threat Detection. *International Journal of Scientific Research and Management (IJSRM)*, *12*(10), 1477–1483. https://doi.org/10.18535/ijsrm/v12i10.ec02

Chakraborty, R. (2023). A Research of Digital Transformation in Healthcare & Its Trends. *International Journal of Science and Research (IJSR)*, *12*(8), 1218–1255. https://doi.org/10.21275/SR23812143349

Hossain, M. M., & Hong, Y. A. (2019). Trends and characteristics of protected health information breaches in the United States. *AMIA ... Annual Symposium Proceedings. AMIA Symposium*, *2019*, 1081–1090.

Indriyajati, F., Jawa, M. M. S. D., & Utomo, H. (2023). Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia. *Sanskara Manajemen Dan Bisnis*, *2*(01), 59–66. https://doi.org/10.58812/smb.v2i01.130

ISO/IEC 27002. (2013). *Information technology-Security techniques-Code of practice for information security controls*.

Lidwina, A. (2021). Kebocoran Data Pribadi yang Terus Berulang. In *Katadata*. https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yang-terus-berulang

Nasution, A. F. (2023). Metode Penelitian Kualitatif. In M. Albina (Ed.), *Harfa Creative*. http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI

Oluomachi, E., & Ahmed, A. (2024). *Securing the Future of Healthcare: Building a Resilient Defense System for Patient Data Protection*. 27–39. https://doi.org/10.5121/csit.2024.141303

Peña, C. A. N., Díaz, A. E. G., Aguirre, J. A. A., & Molina, J. M. M. (2019). Security model to protect patient data in mHealth systems through a Blockchain network. *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology*, *2019-July*(July), 24–26. https://doi.org/10.18687/LACCEI2019.1.1.285

Pradita, R., Kusumo, R., & Rahmawati. (2022). Pentingnya Aspek Keamanan Informasi Data Pasien pada Penerapan RME di Puskesmas. *Journal of Sustainable Community Service*, *2*(2), 52–62. https://doi.org/10.55047/jscs.v2i2.437

Ravlindo, E. (2021). Perlindungan Hukum Terhadap Data Kesehatan Melalui Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi. *Jurnal Hukum Adigama*, *4*(2), 2021. https://doi.org/https://doi.org/10.24912/adigama.v4i2.18028

Rodliyah, I., & Saraswati, S. (2022). Komparasi Sistem Pembelajaran Offline, Semi Offline, dan Online Pada Hasil Belajar Mata Kuliah Metode Numerik. *Jurnal Axioma : Jurnal Matematika Dan Pembelajaran*, *7*(2), 4.

Sutandra, L. (2019). Pengaruh Sistem Pengamanan Data Pasien di Rumah Sakit Menuju Era Revolusi Industri 4.0. *Journal of Health Science and Physiotherapy*, *1*(2), 106–114. https://doi.org/10.35893/jhsp.v1i2.20

Wahyuni, S. (2022). *Metodologi Penelitian Kualitatif*. PT. Global Eksekutif Teknologi. www.globaleksekutifteknologi.co.id

Widayati, L. S., Novianti, N., Kurnianingrum, T. P., & Nola, L. F. (2020). *Politik Hukum Pelindungan Data Pribadi* (B. Nadapdap, Ed.). Yayasan Pustaka Obor Indonesia. https://berkas.dpr.go.id/pusaka/files/buku_tim/buku-tim-public-147.pdf