Patient Data Security Evaluation In Hospital To Achieve SDGs 3.8.1 “Good Health & Wellbeing” (Case Study Information Security Management Permata Hospital Cirebon”

Muhammad Fakhri Rasyad[1], Ratna Lindawati Lubis[2]
[1] Management Department, Faculty of Economy and Business, Telkom University Bandung Indonesia, fakhrirasyad@student.telkomuniversity.ac.id
[2] Management Department, Faculty of Economy and Business, Telkom University Bandung Indonesia, ratnalnugroho@telkomuniversity.ac.id

Abstract
This study examines Permata Hospital Cirebon's patient data security protocols to support SDG target 3.8.1 on excellent health care. This qualitative study used purposive sampling, participant observation, and extensive interviews with four relevant participants. Five main topics emerged from the data analysis: data security incident reporting, implementation challenges, socialization and training, incident evaluation, and data security system improvements. The biggest challenges are user adaption, vendor limitations, and technical dangers like malware and hacking. Despite data security socialization, formal training is lacking. Incidents are investigated reactively without a systematic auditing process. Regulations, data encryption, multi-factor authentication, and vendor risk management are suggested. Organized training and SOP discipline are recommended by this study. In accordance with rules, these procedures should improve patient data security and enable digital health transition in Indonesia.

Keywords*- data security evaluation, SDGs 3.8.1, health digitalization, security management*

I. INTRODUCTION

The Industrial Revolution 5.0 is a revolutionary concept that is currently in the development stage. It generally refers to technological advancements that aim to optimize automation and digitization in the production and industrial sectors. This concept emphasizes the integration of technology and humans, where the digital era's advancements have rendered the routine incorporation of high-quality data a critical element in the digitalization of the healthcare system. The rapid advancement of the current era has resulted in the internet being the sole means of accessing anything. According to data from the *Press Conference Survei Internet Indonesia (2023)* the number of internet users in Indonesia increased from 77.02% in 2022 to 78.19% in 2023. This has the potential to provide users with the convenience of accessing the personal data of others. Data security is a significant issue in the field of digitization, and it is a critical component of information security management. This security issue is also a significant concern for health care institutions, particularly hospitals, which are particularly susceptible to cybercrime. In 2021, the Indonesian population experienced the greatest leak of personal data. BPJS Health exposed a total of 279 million user records in mid-May 2021.

According to Lidwina (2021) , data including the Identification Number, name, residence, telephone number, email, and photo was sold on the Raid Forums platform for 70-80 million rupiah. Patient data is sold on dark web platforms in many nations, with an estimated starting price of 10 million rupiah. The patient data is then taken for numerous purposes (Sutandra, 2019) . Subsequently, Indonesia ranked in the top 10 countries with the highest incidence of data breaches on the internet. Surfshark, a cybersecurity firm, reported that 1.04 million accounts in the country had data breaches in the second quarter of 2022.

Law No. 11/2008 on Electronic Information and Transactions regulates cybercrime, prohibiting individuals from intentionally and unlawfully accessing computers and electronic systems by violating, breaching, or bypassing security measures, which may result in sanctions. The Electronic Information and Transactions Law aims to facilitate national growth, safeguard the rights of internet service users, and take decisive action against cybercriminals. The nature of cybercrime necessitates complicated, coordinated, and sustained measures (Widayati et al., 2020).

Data security entails safeguarding data within a system to prevent unwanted access and modifications to stored information. Every information system owner and management must guarantee the security of stored data and restrict access to authorized individuals to safeguard against purposeful or unintentional hazards. Health data is particularly susceptible to leaking, and the consequences are exacerbated when the compromised information pertains to highly personal patient data (Ravlindo, 2021). The Indonesian Ministry of Health prioritizes system security and personal data protection in system integration. The 2024 health digital transformation strategy ensures that electronic medical records are safeguarded through data security ownership and stewardship protection.

Permata Hospital Cirebon, as a healthcare institution, is accountable for ensuring the safety and comfort of patients during services, which includes the protection of registered patient data. The hospital is committed to enhancing health services that are safe, comfortable, and of high quality, in accordance with applicable laws, to progressively improve community health services annually. The hospital strives to protect the confidentiality of patient data.

Hoelman et al., (2015) assert that health is a significant factor that serves as a parameter of urban community welfare. All individuals possess the right to access health services. All health-related issues within the Sustainable Development Goals (SDGs) are encompassed in Goal 3, which addresses public nutrition, national health systems, family planning, and sanitation and clean water. Furthermore, the rapid development of wearable devices and health applications necessitates attention due to the potential for personal data leakage. Compliance with arrangements and procedures for protecting personal data in collaboration with hospitals will be required (Apsari et al., 2022).

This research aims to evaluate and analyze patient data security strategies in hospitals based on a review of applicable and established policies and procedural regulations. This study aims to offer valuable recommendations for Permata Hospital Cirebon to enhance the effectiveness and security of management information systems, particularly concerning SDGs 3.8.1. This research may enhance the security system implemented at Permata Hospital Cirebon for patient protection.

II. LITERATURE REVIEW

Patient Data Security Evaluation

In the context of health care, personal data refers to patient data and information, such as their complete name, national identity number, telephone number, address, and health examination history (Kautsar, 2023). Data security is the safeguarding of data within a system to prevent unauthorized users and modifications to stored data. It is the responsibility of the proprietor and manager of an information system to guarantee the security of the data stored and to restrict access to only those who are authorized to safeguard the data from intentional or unintentional threats. In the event that highly confidential patient data is released, the consequences will be even more severe (Ravlindo, 2021). Health data is one of the most susceptible to leakage.

Data security is the safeguarding of data within a system to prevent unauthorized users and modifications to stored data. It is the responsibility of the proprietor and manager of an information system to guarantee the security of stored data and to restrict access to only those who are authorized to safeguard it from intentional or unintentional threats. Health data is particularly susceptible to disclosure, and the consequences are compounded when the data is highly confidential patient information. The rules governing personal data protection in Indonesia are still weak and general in nature, as they are dispersed across several separate laws and regulations and only describe the concept of personal data protection in general (Widayati et al., 2020). The objective of personal data theft by hackers is to acquire patient data, which will subsequently be sold or disseminated for free on internet sites.

Information Security Management

Information security management encompasses a variety of measures to safeguard and prevent the misuse of information by individuals who are both internal and external to the hospital (Daniswara et al., 2023). The Hospital Management Information System (HIS) is a system that integrates and processes health service processes in the internal environment of the hospital. It is designed to be used swiftly, precisely, and accurately to function as an administrative coordination network. HIS should not be conducted in a partial manner; rather, it should be incorporated by taking into account a variety of perspectives.

Management of Information Security is the term used to describe the procedures and methodologies that are intended to safeguard the confidential digital data of individuals. The violation of the fundamental principles of information security, which include confidentiality, integrity, and availability, results in the misuse of personal data and information, including unauthorized access, disclosure, theft, destruction, and disruption, in the context of

information system security issues (Whitman & Mattord, 2018). Consequently, in order to safeguard software assets that are part of the information system, companies are obligated to implement a security system. The objective of this effort is to guarantee the confidentiality, availability, and integrity of data processing (Haqqi et al., 2022).

Hospital

Hospitals are responsible for the organisation of health recovery services and treatment in accordance with hospital service standards, as stated in Article 5 letter A of Law of the Republic of Indonesia Number 44 of 2009. In their capacity as health service providers, hospitals are obligated to deliver services with precision, speed, and accuracy. One of the obligations of hospitals is to ensure the security of personal data for patients in order to deliver top-notch service (Kemenkes RI, 2018).

Hospitals are one of the sources of national health data (Aini et al., 2022). The hospital's responsibility is to prioritize healing and recovery efforts that are seamlessly incorporated with improvement and prevention, as well as to make referrals, in order to conduct health initiatives in an efficient and effective manner. These efforts and the hospital's ability to continue to accommodate the changing requirements of patients and society necessitate the integration of hospital components into an information security management system (Listyorini & Sintya, 2021).

SDGs 3.8.1 : Quality Healthcare Services

SDGs 3 is a program aimed at delivering comprehensive health services, ensuring accessibility for all societal members, offering affordable healthcare, implementing disease and mortality prevention strategies, particularly for mothers and children, encouraging community comfort and security in health services, and affirming the right to a healthy and productive life. (Hoelman et al., 2015) assert that health is a significant factor that can serve as a parameter for assessing urban community welfare. All individuals possess the right to access health services. The involvement of government and health facility providers is essential when individuals in poverty require assistance. Goal 3 consolidates all health-related issues within the Sustainable Development Goals (SDGs), including community nutrition, national health systems, family planning, and access to sanitation and clean water. Furthermore, attention must be directed towards the swift advancement of wearable devices and health applications, which pose risks for personal data leakage. These technologies will need to adhere to established protocols and procedures with healthcare institutions to safeguard personal data (Apsari et al., 2022).

To achieve this goal, several measures can be implemented, including the adoption of comprehensive information security management aligned with national regulations governing digital technology security in healthcare, hospital policies aimed at preventing and mitigating patient data breaches, and initiatives to educate and raise awareness regarding the sharing of personal data. The involvement of the community, stakeholders, and government is crucial for implementing measures to mitigate the adverse effects of personal data leakage.

III. METHODS

The research on the evaluation and strategy for patient data security in hospitals was conducted in a methodical, multi-stage process. Researchers employ qualitative methodologies with an evaluative framework. Nasution (2023) asserts that qualitative researchers function as human instruments, employing observation and interview methodologies to engage directly with data sources. Qualitative research is comprehensive and prioritizes the process, so it facilitates an interactive examination of the relationships between variables within the subject of study, where they mutually influence one another. This research used a purposive sampling technique. Purposive sampling is a method for selecting participants based on specific factors pertinent to the research aims, such as job experience, type of work unit, or the participant's access level to patient data.

The authors employed a non-contrived setting technique, depending upon the research context. As stated by (Sekaran & Bougie, 2016), this methodology is implemented in a natural setting where the observed occurrences are consistent. The research employs a cross-sectional technique during its implementation period. The research data points to a particular time period. In this study, the authors applied participant observation methods for data collection, actively engaging in ongoing activities. The author thereafter conducted interviews to acquire the anticipated information within the current circumstances.

This study used a purposive sample technique, also known as judgment sampling, which involves the intentional selection of individuals based on their specific attributes (Etikan et al., 2016). It is a non-random methodology that does not necessitate grounded theory or a predetermined participant count. Purposive sampling is commonly employed

in research papers, as it is present across various research paradigms. This method ensures that the sample is capable of yielding quality data and is readily accessible without bias (Nyimbili & Nyimbili, 2024).

Four participants were chosen as samples according to the inclusion criteria, specifically being healthcare professionals engaged in patient data management, possessing a minimum of one year of experience at Permata Hospital Cirebon, and demonstrating a willingness to share information candidly and transparently.

The author formulates questions based on previous research hrough the observation and interviewing of entities associated with information security management in hospitals. Guidelines for the ISO 27002 information security management standard were established through the preparation of interview questions.

This study involved data collection through in-depth interviews with four selected participants who were a representative part of Permata Hospital Cirebon. The four interviewees were selected based on predetermined inclusion criteria to provide in-depth information related to the research topic in the following Table 1.

Tabel 1 Data Participants

Participant	Position	Duration of Interview
ZR	Director of Security and General Affairs	60 minutes
DW	IT Manager	34 minutes
DC	System Analyst	33 minutes
WA	Head of Medical Records Installation	21 minutes

Sources: Author's data (2024)

Data collection accompanied by documentation is conducted to review and analyse previously acquired data, ensuring that the data utilized in the research is more thorough and comprehensive.

Data Analysis

Data analysis facilitates the comprehension of textual, image, sound, and other data types (Creswell & Creswell, 2018). The initial steps in data analysis involve the collection and preparation of data for subsequent analysis. This involves transcribing interviews, processing field notes, and categorizing visual materials from diverse data sources. Interviews were performed in Indonesian and subsequently translated into English.

The transcripts or drafts of the interviews were reviewed to identify significant words, phrases, or sentences pertinent to the research questions. The words or phrases were subsequently coded. Codes serve to delineate the setting, participants, categories, and themes for analysis.

Interpretation in qualitative research aims to offer an explanatory analysis of the processed data collection results. Incorporating discussions that elucidate the chronology of events, comprehensive analyses of multiple themes accompanied by subthemes, specific illustrations, diverse perspectives, various quotations, and examinations of interconnected themes presented through images or tables pertinent to research materials.

IV. RESULTS AND DISCUSSION

Data was collected for this study through in-depth interviews with four resource persons who were designated as representatives of Permata Hospital Cirebon. Predetermined inclusion criteria were employed to identify the four respondents who were selected to furnish comprehensive information regarding the research subject. There were five themes that addressed data security.

Results

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, and our vendors are not only used in 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 just 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), where we evaluate what cases have occurred, and we 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)***

Discussion

Reporting of Patient Safety Incidents

The findings indicated that the reporting of 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 thereafter forwarded to the Hospital Board of Directors. 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 so that performance can be improved (Stavropoulou et al., 2015).

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 breaches (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

Numerous challenges arise during the implementation of information systems and data security in hospitals. This encompasses physicians that struggle with the HIS offered by the hospital in comparison to systems utilized in other healthcare institutions. Moreover, there are challenges including personnel acclimatization, which requires time to comprehend the new system, as well as technological issues such as intermittent system sluggishness and outages. Chakraborty (2023) research highlights several technological challenges encountered during system implementation, including users' unfamiliarity with hospital information systems, the time needed to gain proficiency in system usage, and the integration of HIS into routine hospital operations. Data security challenges in the adoption of Hospital Management Information Systems include the threat of data breaches and cybercrime, necessitating improved protocols for data accessibility. Moreover, health-related information is susceptible to hacking or leakage, necessitating strong cybersecurity measures prior to the complete 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 (BPJS/MoH) 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 SPOs, 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 review of 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 in a systematic and uniform manner 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 the prevention of 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.

There is a deficiency of specialized training regarding patient data security. Despite the institution not prioritizing formal training, some staff members have gained knowledge through self-directed learning or minimal internal initiatives. Implementing patient data security awareness training and simulation exercises, including phishing tests, enhances employees' ability to identify and react to suspicious activities, therefore mitigating the risk of patient data breaches (Oluomachi & Ahmed, 2024). 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 the development of 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. Evaluation remains predominantly reactive, conducted exclusively in response to patient data security incidents or alterations in regulatory policy. (Peña et al., 2019) state that the evaluation of patient data security events requires an assessment of vulnerabilities and disregards that may threaten the confidentiality, integrity, and availability of clinical information.

No regular audit or risk assessment mechanism has been implemented on a regular basis. The research indicates that periodic audits are crucial for detecting patient data breaches, as they offer a systematic method for monitoring and identifying unauthorized access to sensitive information. Audits function as a proactive measure to safeguard patient data through the regular assessment of system configurations and data management practices. This process aids in the identification of anomalies or suspicious activities that may suggest a breach. Periodic audits are recognized as an effective method for detecting breaches and establishing a comprehensive approach to data protection. Health agencies should prioritize regular audits to timely prevent breaches and enhance information security (Oluomachi & Ahmed, 2024).

The evaluation process is primarily conducted internally by the IT team, 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 the establishment of audit mechanisms, ongoing monitoring, and definitive performance indicators to guarantee optimal patient data security.

V. CONCLUSION

This study reveals that patient data security management at Permata Hospital Cirebon encounters numerous problems, including technical threats such as hacking, staff discipline issues, and insufficient organized training pertaining to data security. Despite the implementation of an incident reporting system, the process remains reactive and lacks systematic periodic assessment.

The study aims to improve the security of patient data and contribute to the achievement of SDGs target 3.8.1, which concerns the provision of quality health services. This strategy should encompass the following: the reinforcement of policies, the enhancement of security infrastructure, such as firewalls and server protection, the implementation of consistent staff training, and the scheduled and comprehensive evaluation of the data security system.

REFERENCES

Aini, Z., Nurwijayanti, N., Supriyanto, S., & Susanto, H. E. (2022). Strategi Pengembangan Transformasi Sistem Informasi Manajemen Rumah Sakit (SIM-RS) di RSUD dr. Iskak Tulungagung. *Journal of Community Engagement in Health*, *5*(2), 128–139. https://doi.org/10.30994/jceh.v5i22.383

APJII. (2023). *SURVEI INTERNET TAHAP 1*. https://apjii.or.id/download_survei/0ceedf78-5c53-4435-9462-472ef2644077

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

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. In H. Salmon & C. Neve (Eds.), *SAGE Publications* (Fifth Edit). SAGE Publications, Inc.

Daniswara, M. C., Putrawanto, D. I., Najib, M., Achmadha, Z., Chairuladanan I, M. S., & Mukaromah, S. (2023). Evaluasi Keamanan Informasi di Lingkungan Rumah Sakit: Pendekatan Audit ISO 27001 di RS Rahman Rahim Sidoarjo. In *Journal of Digital Ecosystem for Natural Sustainability (JoDENS)* (Vol. 3, Issue 2).

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

Haqqi, D. P., Ghozali, K., & Ginardi, R. V. H. (2022). Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 dengan Menggunakan Model SSE-CMM. *Jurnal Teknik ITS*, *11*(2). https://doi.org/10.12962/j23373539.v11i2.91532

Hoelman, M. B., Parhusip, B. T., Parlinggoman Eko, S., Bahagijo, S., & Santono, H. (2015). *Panduan SDGs Untuk Pemerintah Daerah (Kota dan Kabupaten) dan Pemangku Kepentingan Daerah* (Issue November). Infid.

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

Kautsar, T. R. (2023). *Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi dan Regulasi Perlindungan Data Pribadi*. UIN Ar-Raniry.

Kemenkes RI. (2018). *Peraturan Kementrian Kesehatan Republik Indonesia Nomor 4 Tahun 2018 Tentang Kewajiban Rumah Sakit dan Kewajiban Pasien*.

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

Listyorini, P. I., & Sintya, I. (2021). Sistem Keamanan SIMRS di Rumah Sakit. *Prosiding Seminar Informasi Kesehatan Nasional (SIKesNas)*, 234–240.

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

Nyimbili, F., & Nyimbili, L. (2024). Types of Purposive Sampling Techniques with Their Examples and Application in Qualitative Research Studies. *British Journal of Multidisciplinary and Advanced Studies*, *5*(1), 90–99. https://doi.org/10.37745/bjmas.2022.0419

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

Sekaran, U., & Bougie, R. (2016). Research Methods for Business: A Skill-Building Approach. In *Journal of Physics A: Mathematical and Theoretical* (Fifth Edit, Vol. 44, Issue 8). John Wiley & Sons, Ltd.

Stavropoulou, C., Doherty, C., & Tosey, P. (2015). How Effective Are Incident-Reporting Systems for Improving Patient Safety? A Systematic Literature Review. *Milbank Quarterly*, *93*(4), 826–866. https://doi.org/10.1111/1468-0009.12166

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

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. *Cengage Learning*, *September*, 11. www.cengage.com.

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