ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

Patient Data Protection in Healthcare: Assessing Compliance and Practices Among Healthcare Workers as Basis for a Training Enhancement Program

Maria Cecilia P. Nueva[1*] and Erwin M. Faller[1]
St. Bernadette of Lourdes College
[*]*mariacecilianueva989@gmail.com*

Date Submitted:
April 18, 2026

Date Accepted:
May 24, 2026

Date Published:
July 09, 2026

DOI:
10.5281/zenodo.21280320

ABSTRACT
This study determined the compliance and practices regarding patient data privacy among healthcare workers in selected private hospitals in Dasmariñas, Cavite as basis for developing a training enhancement program. It employed a quantitative descriptive-correlational research design involving 300 healthcare workers from two private hospitals, selected through stratified and simple random sampling. Data were gathered using a validated researcher-made five-point Likert questionnaire and analyzed using frequency, percentage, mean, standard deviation, and Pearson r. Findings showed that most respondents were young to middle-aged adults, predominantly female, largely nurses, mostly bachelor's degree holders, and generally had one to five years of healthcare experience and one to two trainings related to data privacy. Healthcare workers demonstrated high levels of administrative practices (M = 3.74, SD = 1.13) and technical practices (M = 3.73, SD = 1.12). They also showed high levels of legal compliance (M = 3.78, SD = 1.13) and institutional compliance (M = 3.76, SD = 1.11). However, the relationship between overall practices and overall compliance was very weak, positive, and not statistically significant (r = 0.071, p = 0.217). The study concludes that good privacy practices do not automatically translate into stronger compliance, suggesting the influence of organizational systems, enforcement, training, and institutional support. The proposed enhancement program focuses on legal compliance, secure data handling, cybersecurity, incident reporting, and a stronger privacy culture in hospitals.

Keywords: *patient data privacy, healthcare workers, compliance, technical practices, legal compliance, training enhancement program*

INTRODUCTION

Patient data privacy has become a critical concern in healthcare because hospitals increasingly rely on electronic health records, digital platforms, and information systems to support patient care and administrative operations. These technologies improve access, efficiency, and coordination, but they also increase exposure to unauthorized access, data breaches, and improper sharing of sensitive patient information. Protecting patient data therefore requires both institutional safeguards and consistent privacy practices among healthcare workers (Afzal & Arshad, 2021; Shojaei et al., 2024).

In the Philippine setting, healthcare institutions are expected to comply with Republic Act No. 10173, or the Data Privacy Act of 2012, together with related hospital policies that govern the collection, storage, processing, and disclosure of patient information. However, compliance may vary depending on the workers' awareness, training, access to secure systems, and institutional enforcement. Local studies have reported that healthcare

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

workers may be aware of privacy requirements but still experience challenges in strict compliance because of gaps in training and administrative support (Agup, 2024).

Healthcare workers are central to patient data protection because they directly access, process, store, transmit, and release patient information as part of their daily responsibilities. Their administrative practices, such as following release protocols and avoiding public discussions of patient information, and their technical practices, such as password management and secure electronic transmission, shape how patient privacy is maintained in actual hospital operations. At the same time, compliance is also influenced by legal knowledge, institutional policies, monitoring, and the broader data privacy culture of the healthcare organization (Alhassani et al., 2024; Mikuletič et al., 2023).

Although previous studies have examined confidentiality, electronic medical records, digital health security, and data privacy regulation, limited local empirical evidence is available on the specific relationship between healthcare workers' patient data privacy practices and their compliance with patient data privacy policies in selected private hospitals in Dasmariñas, Cavite. This study addresses the gap by assessing administrative and technical practices, legal and institutional compliance, and the relationship between practices and compliance. The findings served as the basis for a Training Enhancement Program that can strengthen privacy practices and improve compliance among healthcare workers.

Literature Review

Administrative and technical practices in patient data privacy

Administrative practices refer to organizational policies, procedures, and management strategies that guide healthcare workers in protecting patient information. Previous studies show that weak privacy infrastructure, insufficient confidentiality measures, and limited training may negatively affect patient trust and quality of care. Pratiwi et al. (2022) found that inadequate privacy protection in primary healthcare settings may discourage patients from disclosing sensitive information, while Tegegne et al. (2022) emphasized the need for continuous ethics training to strengthen confidentiality knowledge and attitudes. Similarly, Mensah et al. (2024), Turkstani et al. (2025), and Oktaviana et al. (2025) highlighted the value of clear policies, access management, staff guidance, accountability, and data governance in strengthening healthcare data protection.

Technical practices involve the use of secure systems, access controls, encryption, password protection, restricted storage, and responsible handling of electronic patient records. Afzal and Arshad (2021) reported that electronic medical records improve healthcare efficiency but introduce ethical concerns related to privacy, security, and confidentiality. Shojaei et al. (2024) identified blockchain, cloud computing, and other technologies as possible supports for health information security, while Williamson and Prybutok (2024) emphasized the importance of encryption and transparent systems in AI-enabled healthcare. The studies of İyiGün and Ergene (2025) and Karacic-Zanetti (2025) also show that technical safeguards must be paired with training, audits, and institutional support to reduce risks from unsecured platforms, weak access controls, and inadequate cybersecurity behaviors.

Legal and institutional compliance with patient data privacy policies

Legal compliance refers to adherence to laws, regulations, and ethical requirements that govern the protection of patient information. Albabtain et al. (2024) found that healthcare professionals recognize the importance of privacy protection in clinical research, but knowledge gaps remain among those with limited research or training exposure. Idoko et al. (2024) and Conduah et al. (2025) likewise emphasized that regulatory frameworks, enforcement, audits, and cross-institutional collaboration are important for securing healthcare data. In the Philippine context, Agup (2024) found that nurses were highly aware of the Data Privacy Act but faced compliance challenges related to training and administrative support.

Institutional compliance involves the hospital's capacity to implement internal rules, monitoring systems, reporting mechanisms, and support structures that help healthcare workers consistently follow privacy requirements. Semyonov-Tal (2024) reported that physicians recognize the importance of confidentiality but face

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

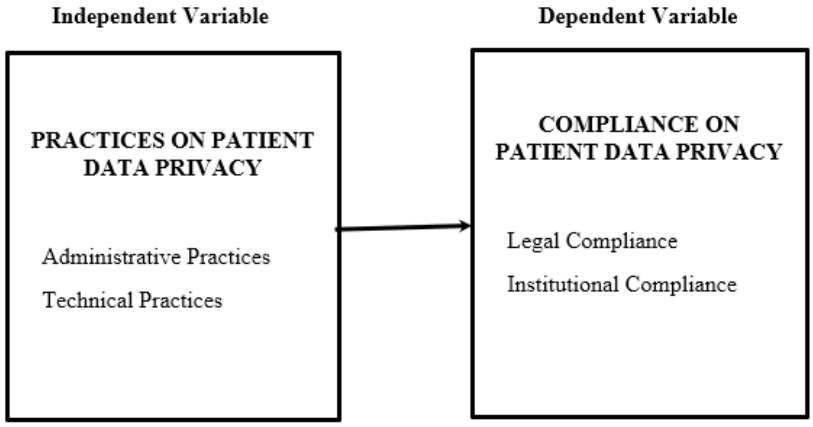
practical challenges in balancing information sharing and privacy. Msumi (2024), Hanggara et al. (2024), Abuhammad (2025), and Hamza et al. (2025) similarly noted that institutional policies, digital health governance, infrastructure, ethical oversight, and enforcement mechanisms are essential in translating legal requirements into actual practice. These studies suggest that hospitals must move beyond written rules by supporting education, monitoring, and a culture of accountability.

Relationship between privacy practices and compliance

The relationship between privacy practices and compliance is shaped by individual behavior, workplace culture, and organizational support. Xu et al. (2022) argued that privacy protection behavior is influenced by healthcare workers' awareness, perception of risks, and motivation to adopt protective actions. D'Ordine (2023) emphasized the need to balance patient privacy with responsible data access for healthcare improvement, while Mikuletič et al. (2023) showed that a strong information security culture can reduce unauthorized access to patient data among healthcare workers.

Other studies suggest that compliance is not only a matter of individual practice. Ibrahim et al. (2024) reported that privacy management practices are positively associated with compliance in electronic health record and cybersecurity contexts, while Alhassani et al. (2024) identified confidence, competence, environmental support, perceived usefulness, fear of consequences, and social expectations as drivers of compliance intentions. Siregar and Astuti (2025) further showed that formal regulations may not guarantee compliance when staff awareness, security infrastructure, and institutional readiness are limited. Thus, examining both practices and compliance in local hospital settings can help identify whether training and institutional supports are needed to improve patient data protection.

Figure 1. *Conceptual Paradigm of the Study*



METHODS

Research Design

The study employed a quantitative descriptive-correlational research design. The descriptive component described the demographic profile of the respondents, their practices regarding patient data privacy, and their compliance with patient data privacy policies. The correlational component determined whether a significant relationship existed between healthcare workers' privacy practices and their compliance. This design was appropriate because the study examined existing conditions and associations without manipulating the variables (Ahmad et al., 2019; Siedlecki, 2020).

Research Locale

The study was conducted in two selected private hospitals in Dasmariñas, Cavite. The hospitals were selected because they are large private healthcare institutions that handle a substantial volume of patient information and employ diverse healthcare workers who regularly process patient data.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

Participants and Sampling Technique

The respondents were 300 healthcare workers from the two participating hospitals. Hospital A had a total eligible population of 1,043 healthcare workers and Hospital B had 268, for a combined population of 1,311. A total of 150 respondents were selected from each hospital. The participants included doctors, nurses, medical technologists, administrative staff, and other healthcare workers who handled patient information. The study used stratified sampling by hospital and simple random sampling within each stratum to provide equal representation and reduce selection bias.

Research Instrument

The study used a researcher-made survey questionnaire consisting of 28 Likert-scale items. The instrument contained three sections: demographic profile, practices on patient data privacy, and compliance with patient data privacy policies. Practices were measured through administrative and technical practices, with seven items per dimension. Compliance was measured through legal and institutional compliance, also with seven items per dimension. Responses were interpreted using a five-point Likert scale ranging from Strongly Disagree to Strongly Agree.

Validation of Research Instrument

The questionnaire was reviewed by three experts, namely a Data Protection Officer, a Compliance Officer, and a Medical Director, to establish face validity and ensure alignment with the study objectives. Pilot testing was also conducted, and Cronbach's alpha reliability testing was used to determine the internal consistency of the instrument.

Data Gathering Procedure

The researcher secured approval from the administrations of the selected private hospitals before distributing the questionnaires. Eligible healthcare workers received an informed consent form explaining the purpose of the study, voluntary participation, confidentiality measures, and their rights as respondents. Completed questionnaires were collected through the agreed hospital process, organized, and prepared for statistical analysis.

Data Analysis

Frequency and percentage were used to describe the demographic profile of the respondents. Mean and standard deviation were used to determine the levels of practices and compliance. Pearson r correlation was used to test the relationship between healthcare workers' practices and compliance with patient data privacy policies at the 0.05 level of significance.

Ethical Consideration

The study followed the ethical standards of St. Bernadette of Lourdes College Institutional Research Ethics Committee and complied with Republic Act No. 10173 or the Data Privacy Act of 2012. Participation was voluntary, informed consent was obtained, no identifying information was collected, and data were securely stored and accessible only to authorized persons. Respondents were informed that they could withdraw from the study at any time without negative consequences.

RESULTS AND DISCUSSION

Demographic profile of the respondents

The respondents were composed of 300 healthcare workers from two selected private hospitals in Dasmariñas, Cavite, with 150 respondents from each hospital. Table 1 summarizes the dominant demographic categories in both hospitals. The results show that the workforce was mainly composed of young to middle-aged adults, predominantly female, mostly bachelor's degree holders, and largely nurses. Most respondents had one to five years of healthcare experience, had attended one to two data privacy-related trainings, and were commonly assigned to the Outpatient Department.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

Table 1. *Summary of the Demographic Profile of Respondents*

Profile Variable	Hospital A	Hospital B	Interpretation
Age	26–35 years: 50 (33.3%)	26–35 years: 55 (36.7%)	Most respondents were young to middle-aged adults.
Sex	Female: 90 (60.0%)	Female: 95 (63.3%)	Female healthcare workers predominated in both hospitals.
Educational attainment	Bachelor's degree: 85 (56.7%)	Bachelor's degree: 90 (60.0%)	Most respondents met the basic academic requirement for healthcare work.
Designation/Role	Nurse: 60 (40.0%)	Nurse: 65 (43.3%)	Nurses formed the largest respondent group.
Years of experience	1–5 years: 60 (40.0%)	1–5 years: 65 (43.3%)	Most respondents were early-career healthcare workers.
Trainings attended	1–2 trainings: 65 (43.3%)	1–2 trainings: 70 (46.7%)	Exposure to data privacy training was present but limited.
Department	Outpatient Department: 40 (26.7%)	Outpatient Department: 45 (30.0%)	Many respondents worked in high-traffic patient-facing units.

Healthcare workers' practices regarding patient data privacy

Table 2 shows that respondents had high levels of both administrative and technical practices. Administrative practices obtained a composite mean of 3.74 (SD = 1.13), while technical practices obtained a composite mean of 3.73 (SD = 1.12). These findings suggest that healthcare workers generally practiced confidentiality, proper record handling, and secure electronic data behaviors. However, lower item ratings in following release policies and regularly updating strong passwords indicate areas that require additional reinforcement.

Table 2. *Summary of Patient Data Privacy Practices among Healthcare Workers*

Dimension	Highest-Rated Indicator	Mean	Lowest-Rated Indicator	Mean	Composite Mean	Interpretation
Administrative Practices	Avoiding discussion of patient information in public areas	3.85	Following hospital policies regarding the release of patient information	3.62	3.74 (SD = 1.13)	High
Technical Practices	Verifying the identity of individuals requesting patient information before providing access	3.89	Using strong passwords and updating them regularly	3.61	3.73 (SD = 1.12)	High

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

The results are consistent with studies showing that privacy practices require both administrative safeguards and technical controls. Pratiwi et al. (2022), Tegegne et al. (2022), and Mensah et al. (2024) emphasized that organizational privacy procedures, training, and clear guidance improve confidentiality practices. Likewise, Afzal and Arshad (2021), Shojaei et al. (2024), and Karacic-Zanetti (2025) showed that secure handling of electronic records, access controls, and cybersecurity behaviors are necessary in protecting patient information. The lower rating in password management is particularly important because weak authentication practices may expose healthcare systems to unauthorized access.

Compliance with patient data privacy policies

Table 3 shows that respondents also had high levels of compliance with patient data privacy policies. Legal compliance obtained a composite mean of 3.78 (SD = 1.13), while institutional compliance obtained a composite mean of 3.76 (SD = 1.11). These results suggest that healthcare workers were generally aware of legal requirements and hospital policies. However, comparatively lower ratings in avoiding unauthorized sharing and collaborating in policy improvement suggest that compliance may still be strengthened through clearer policy engagement and workplace accountability.

Table 3. *Summary of Compliance with Patient Data Privacy Policies*

Dimension	Highest-Rated Indicator	Mean	Lowest-Rated Indicator	Mean	Composite Mean	Interpretation
Legal Compliance	Reporting any violations of patient data privacy to appropriate authorities	3.85	Avoiding sharing patient information without proper legal authorization	3.73	3.78 (SD = 1.13)	High
Institutional Compliance	Following hospital internal policies on handling patient records	3.87	Collaborating with the institution to improve compliance with data privacy policies	3.73	3.76 (SD = 1.11)	High

These findings support the view that compliance depends on legal awareness, policy enforcement, and institutional support. Albabtain et al. (2024), Idoko et al. (2024), Conduah et al. (2025), and Lakoro et al. (2025) emphasized the importance of regulations, governance, enforcement, and continuing education in healthcare data protection. Institutional studies also show that written policies alone are not enough; hospitals must provide monitoring, training, reporting systems, infrastructure, and ethical support to sustain compliance (Abuhammad, 2025; Hamza et al., 2025; Hanggara et al., 2024; Semyonov-Tal, 2024).

Relationship between practices and compliance

The relationship between healthcare workers' overall practices and their overall compliance with patient data privacy policies was tested using Pearson r. As shown in Table 4, the relationship was very weak, positive, and not statistically significant ($r = 0.071$, $p = 0.217$). Since the p-value was greater than 0.05, the null hypothesis was not rejected. This indicates that higher reported practices were not significantly associated with higher compliance among the respondents.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

Table 4. *Relationship between Healthcare Workers' Practices and Compliance with Patient Data Privacy Policies*

Variables	n	Pearson r	df	p-value	95% CI	Interpretation	Decision
Practices Overall vs. Compliance Overall	300	0.071	298	0.217	-0.042 to 0.183	Very weak positive, not significant	Fail to reject H0

This result suggests that good privacy practices alone may not automatically lead to stronger compliance. The finding may reflect the influence of other factors, such as organizational culture, leadership support, availability of resources, monitoring mechanisms, workload, and policy enforcement. This interpretation is consistent with Alhassani et al. (2024), Mikuletič et al. (2023), and Siregar and Astuti (2025), who emphasized that compliance with patient data privacy policies is shaped by both individual behaviors and institutional conditions. Therefore, improving compliance requires not only training healthcare workers but also strengthening organizational systems that support and monitor data privacy practices.

Proposed training enhancement program

Based on the results, a training enhancement program was proposed to address identified gaps in privacy practices and compliance. The program focuses on legal compliance, proper handling and release of patient information, cybersecurity and password management, data breach reporting, and institutional compliance culture. These areas directly correspond to the lower-rated indicators and the study's conclusion that compliance requires both individual competence and institutional support.

Table 5. *Proposed Enhanced Patient Data Privacy and Cybersecurity Training Program*

Training Area	Learning Objective	Topics	Strategies/Activities	Duration	Expected Outcomes
Patient Data Privacy Fundamentals and Legal Compliance	Explain privacy responsibilities and legal requirements	Data Privacy Act of 2012, confidentiality, and legal consequences	Lecture, discussion, case analysis	2–3 hours	Increased awareness of legal responsibilities
Secure Handling and Release of Patient Information	Apply correct procedures in managing patient records	Authorized access, release of information, and avoiding unauthorized sharing	Role-playing and case scenarios	2–3 hours	Improved handling of patient information
Cybersecurity and Password Management	Strengthen technical privacy practices	Strong passwords, phishing awareness, access control, and secure system use	Demonstration and hands-on activities	2 hours	Improved password and cybersecurity practices
Data Breach Reporting and Incident Response	Improve reporting and response practices	Breach identification, reporting procedures, and hospital response protocols	Simulation and guided exercises	2 hours	Improved breach reporting awareness
Strengthening Compliance Culture	Encourage continuous policy engagement	Workplace accountability, teamwork, monitoring, and continuous improvement	Workshop and group discussion	2 hours	Increased participation in compliance efforts

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 7 (July 2026)

CONCLUSION

The study concludes that healthcare workers in the two selected private hospitals in Dasmariñas, Cavite generally demonstrated high levels of patient data privacy practices. They performed well in administrative practices such as avoiding public discussion of patient information and in technical practices such as verifying the identity of individuals requesting access to patient data. Nevertheless, password management and strict adherence to patient information release policies require reinforcement.

The study also concludes that healthcare workers had high levels of legal and institutional compliance. They generally understood their responsibilities under patient data privacy policies and followed internal hospital procedures. However, lower involvement in policy improvement and slightly weaker ratings in avoiding unauthorized sharing indicate the need for stronger institutional engagement and continuing education.

The relationship between privacy practices and compliance was very weak, positive, and not statistically significant. This means that good reported practices do not necessarily lead to higher compliance. Compliance appears to be influenced by broader organizational factors such as policy enforcement, monitoring, training support, reporting systems, and data privacy culture. The proposed training enhancement program is therefore necessary to strengthen both individual competencies and institutional mechanisms for protecting patient information.

Recommendation

Selected private hospitals in Dasmariñas, Cavite should conduct regular and structured data privacy training for healthcare workers, with emphasis on patient information release procedures, password management, secure file transfer, breach reporting, and legal responsibilities under the Data Privacy Act of 2012.

Hospital administrators, Data Protection Officers, compliance offices, and human resource departments should strengthen policy enforcement and monitoring systems. Regular audits, policy reminders, confidential reporting mechanisms, and compliance feedback may help ensure that healthcare workers consistently apply patient data privacy rules in daily practice.

Healthcare workers should continue practicing proper confidentiality measures, including verifying identities before releasing patient information, avoiding public discussions of patient cases, logging out of systems when not in use, using secure communication methods, and avoiding the use of personal devices or unapproved cloud storage for patient information.

The proposed Enhanced Patient Data Privacy and Cybersecurity Training Program may be adopted and implemented in the participating hospitals. The program should include pre-test and post-test assessments, quarterly refresher sessions, incident-report monitoring, and evaluation of compliance improvement indicators.

Future researchers may examine other factors that influence patient data privacy compliance, such as organizational culture, leadership support, workload, availability of secure technologies, and cybersecurity infrastructure. Future studies may also use qualitative or mixed-method designs to gain deeper insight into healthcare workers' actual experiences with patient data privacy compliance.

References

Abuhammad, S. (2025). Strengthening ethical practices of patient data confidentiality and sharing among nurses in the artificial intelligence-driven healthcare era. SAGE Open Nursing, 11, 23779608251398113. https://doi.org/10.1177/23779608251398113

Afzal, S., & Arshad, A. (2021). Ethical issues among healthcare workers using electronic medical records: A systematic review. Computer Methods and Programs in Biomedicine Update, 1, 100030. https://doi.org/10.1016/j.cmpbup.2021.100030

Agup, R. (2024). Data Privacy Act: Awareness, compliance, and challenges of nurses of government hospitals in Northern Philippines. SEEJPH. Source details require verification.

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Farheen, Z. (2019). Qualitative v/s. quantitative research: A summarized review. Journal of Evidence Based Medicine and Healthcare, 6(43), 2828–2832. https://doi.org/10.18410/jebmh/2019/587

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-t

Albabtain, M. A., AlOtaibi, D., AlMazial, N., Aloudah, N., Alghosoon, H. M., & Arafat, A. A. (2024). Healthcare professional's knowledge, awareness, and attitude toward patients' data privacy and security in clinical research. Saudi Journal of Health Systems Research, 4(2), 92–102. https://doi.org/10.1159/000538617

Alhassani, N. D., Windle, R., & Konstantinidis, S. T. (2024). A scoping review of the drivers and barriers influencing healthcare professionals' behavioral intentions to comply with electronic health record data privacy policy. Health Informatics Journal, 30(4), 14604582241296398. https://doi.org/10.1177/14604582241296398

Conduah, A. K., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. Digital Health, 11, 20552076251343959. https://doi.org/10.1177/20552076251343959

D'Ordine, K. (2023). HIPAA vs. medical research: Improving patient care through integration of data privacy and data access (Senior Honors Project, Bryant University). Bryant Digital Repository. https://digitalcommons.bryant.edu/cgi/viewcontent.cgi?article=1008&context=honors_data_science

Gibbs, J. P. (1975). Crime, punishment, and deterrence. Elsevier.

Hamza, A., Adamu, A., & Sauwa, S. H. (2025). Assessment of confidentiality of patients' health records among health information professionals at Usmanu Danfodiyo University Teaching Hospital, Sokoto. Zenodo. https://doi.org/10.5281/zenodo.17626794

Hanggara, I. B. U., Kuswardhani, T., & Hartawan, G. A. G. U. (2024). Roles of law on medical records for data and information security: A systematic literature review. Journal of Law Politic and Humanities, 5(2). https://doi.org/10.38035/jlph.v5i2

Ibrahim, A. M., Abdel-Aziz, H. R., Mohamed, H. A. H., Zaghamir, D. E. F., Wahba, N. M. I., Hassan, G. A., Shaban, M., El-Nablaway, M., Aldughmi, O. N., & Aboelola, T. H. (2024). Balancing confidentiality and care coordination: Challenges in patient privacy. BMC Nursing, 23(1), 564. https://doi.org/10.1186/s12912-024-02231-1

Idoko, N. B., Alakwe, N. J. A., Ugwu, N. O. J., Idoko, N. J. E., Idoko, N. F. O., Ayoola, N. V. B., Ejembi, N. E. V., & Adeyinka, N. T. (2024). Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria. Magna Scientia Advanced Research and Reviews, 11(2), 151–167. https://doi.org/10.30574/msarr.2024.11.2.0110

İyiGün, U., & Ergene, D. (2025). Legal and ethical breaches in personal health data handling among cardiologists: A multicenter survey on compliance gaps and forensic risk. Forensic Science International Reports, 13, 100444. https://doi.org/10.1016/j.fsir.2025.100444

Karacic-Zanetti, J. (2025). Challenges and solutions for patient data protection in large healthcare databases. Preprints.org. https://doi.org/10.20944/preprints202504.1650.v1

Lakoro, D. D. K., Jumrati, & Jamaludin, A. (2025). Legal responsibility of health professionals in protecting patient data. Research Horizon, 5(3), 869–878. https://doi.org/10.54518/rh.5.3.2025.657

Mensah, N. K., Adzakpah, G., Kissi, J., Taylor-Abdulai, H., Johnson, S. B., Agbeshie, P. A., Opoku, C., Abakah, J., Osei, E., Agyekum, A. Y., & Boadu, R. O. (2024). Health professionals' ethical, security, and patient safety concerns using digital health technologies: A mixed-method research study. Health Services Insights, 17, 11786329241303379. https://doi.org/10.1177/11786329241303379

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2023). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. Computers & Security, 136, 103489. https://doi.org/10.1016/j.cose.2023.103489

Msumi, M. M. (2024). Protection of personal data in e-health: A comparative perspective between Tanzania and Germany (Doctoral dissertation, The Open University of Tanzania). The Open University of Tanzania Institutional Repository. https://repository.out.ac.tz/4718/1/MBIKI%20MKUDE%20MSUMI-PhD%20Thesis-01-11-2024.pdf

Oktaviana, S. O., Handayani, P. W., Hidayanto, A. N., & Siswanto, B. B. (2025). Healthcare data governance assessment based on hospital management perspectives. International Journal of Information Management Data Insights, 5(1), 100342. https://doi.org/10.1016/j.jjimei.2025.100342

Pratiwi, A. B., Padmawati, R. S., & Willems, D. L. (2022). Behind open doors: Patient privacy and the impact of design in primary health care, a qualitative study in Indonesia. Frontiers in Medicine, 9. https://doi.org/10.3389/fmed.2022.915237

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Semyonov-Tal, K. (2024). Keeping medical information safe and confidential: A qualitative study on perceptions of Israeli physicians. Israel Journal of Health Policy Research, 13(1). https://doi.org/10.1186/s13584-024-00641-9

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. (2024). Security and privacy of technologies in health information systems: A systematic literature review. Computers, 13(2), 41. https://doi.org/10.3390/computers13020041

Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. Clinical Nurse Specialist, 34(1), 8–12. https://doi.org/10.1097/nur.0000000000000493

Siregar, R. A., & Astuti, N. K. (2025). Assessing legal and institutional readiness for patient data protection in the age of big health data: An empirical study of health facilities in Indonesia. International Journal of Law, Policy and Social Review, 7(3), 15–21. https://www.lawjournals.net/assets/archives/2025/vol7issue3/7062.pdf

Tegegne, M. D., Melaku, M. S., Shimie, A. W., Hunegnaw, D. D., Legese, M. G., Ejigu, T. A., Mengestie, N. D., Zemene, W., Zeleke, T., & Chanie, A. F. (2022). Health professionals' knowledge and attitude towards patient confidentiality and associated factors in a resource-limited setting: A cross-sectional study. BMC Medical Ethics, 23(1). https://doi.org/10.1186/s12910-022-00765-0

Turkstani, H. A., Almutawah, F. N., AlZamel, N. A., Alshammari, M. Z., Alhamadi, A. A., Algharbi, M. T., Alsuayri, A. M., Gong, M. B., Alqahtani, J. S., Alnemer, A. F., & Aljuwayed, N. H. (2025). Privacy and confidentiality in healthcare: Best practices for protecting patient information. Journal of Healthcare Sciences, 5(1), 49–54. https://doi.org/10.52533/johs.2025.50106

Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. Applied Sciences, 14(2), 675. https://doi.org/10.3390/app14020675

Xu, J., Lu, L., Xing, K., Shi, H., Chen, R., Yao, Y., Liu, S., Xiao, Z., Peng, X., Luo, S., & Zhong, Y. (2022). Theoretical approach and scale construction of patient privacy protection behavior of doctors in public medical institutions in China: Pilot development study. JMIR Formative Research, 6(12), e39947. https://doi.org/10.2196/39947