Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 22 No. 8 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v22i08.62320

PAPER

Regulation of Mobile Technologies in Biomedical Systems: Data Governance, Compliance, and Digital Oversight

Ade Ikhlas Amal Alam[1] (✉), Khairunnisa Azrin[2], Fakhrul Indra Hermansyah[1], Syamsu Alam[1], Andi Raina Ananda Herdiyana[1]

[1]Hasanuddin University, Makassar, Indonesia

[2]Management and Science University, Selangor, Malaysia

adeikhlas@unhas.ac.id

ABSTRACT

This study examines the impact of data governance (DG), compliance (COM), and digital oversight (DO) on system performance (SP) and security within mobile biomedical systems in Indonesia's healthcare sector. Employing Socio-Technical Systems Theory, the study investigates the role of regulations in enhancing operational efficiency and strengthening cybersecurity in digital healthcare. A quantitative cross-sectional design was utilised, with data collected from 200 healthcare and biomedical technology professionals through an online questionnaire. Relationships among variables were analysed using multiple linear regression. The results showed that DG had the greatest positive effect on both SP and security, followed by COM and DO. All these relationships were statistically significant ($p < 0.001$). This study shows that adopting integrated governance frameworks, complying with regulations and maintaining ongoing monitoring are important for making mobile biomedical technologies more reliable and secure. It also adds new evidence by examining operational performance and system security (SS) as distinct outcomes in mobile biomedical systems.

KEYWORDS

mobile biomedical systems, data governance (DG), compliance (COM), digital oversight (DO), system performance (SP), regression analysis

1 INTRODUCTION

Mobile technologies have rapidly transformed healthcare by enabling real-time patient monitoring [1], remote consultations, and ongoing biomedical data collection [2]. Mobile health (mHealth) apps and smart biomedical devices have made healthcare more accessible [3], efficient and engaging for patients, especially in connected healthcare systems [1]. However, these advances bring complex challenges in data security [3], regulatory compliance (COM), and organisational control, especially given the sensitivity of biomedical data and the increasing frequency of cybersecurity threats [4]. Building secure and reliable mobile biomedical systems requires

Alam, A. I. A., Azrin, K., Hermansyah, F. I., Alam, S., Herdiyana, A. R. A. (2026). Regulation of Mobile Technologies in Biomedical Systems: Data Governance, Compliance, and Digital Oversight. *International Journal of Online and Biomedical Engineering (iJOE)*, 22(8), pp. 47–58. https://doi.org/10.3991/ijoe.v22i08.62320

Article submitted 2026-03-18. Revision uploaded 2026-05-01. Final acceptance 2026-05-09.

strong governance, strict COM and effective monitoring [5]. Biomedical systems handle sensitive patient information [1], so weaknesses in mobile platforms can lead to data breaches, disrupt operations and compromise patient safety [3].

Healthcare organisations and regulatory authorities have increasingly prioritised data governance (DG), COM management, and DO as critical mechanisms to ensure the security and reliability of biomedical systems [4–6]. DG encompasses the policies, standards and organisational structures that ensure data quality, integrity, accessibility and confidentiality throughout the data lifecycle. COM involves adherence to legal, ethical, and regulatory rules like the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union [7–8], and national healthcare data protection laws that control how biomedical information is collected, stored, processed and shared in Indonesia [9]. DO means ongoing monitoring, auditing, and supervision to spot irregularities, enforce security measures and ensure accountability in digital healthcare systems [8]. Together, these regulatory tools are now seen as key factors for both performance and security in mobile biomedical technologies [9].

Although more studies are focusing on healthcare DG and digital regulation, most studies still treat governance, COM and oversight separately rather than as interconnected regulatory mechanisms [10]. This gap matters because mobile biomedical environments operate within fast-changing, distributed digital systems. These systems need to balance operational efficiency, regulatory accountability and cybersecurity resilience simultaneously [10]. As a result, there are still insufficient studies on how governance practices together affect system performance (SP) and security in mobile biomedical technologies.

This study contributes to the digital health governance literature in several ways. First, it develops an integrated regulatory framework that simultaneously addresses governance, COM and oversight for mobile biomedical systems. Second, it extends existing research by demonstrating, through empirical data, that operational performance and system security (SS) are distinct yet interrelated technological outcomes. This study provides practical guidance for healthcare administrators, biomedical technology providers and policymakers aiming to enhance digital healthcare governance, regulatory COM, and cybersecurity resilience within increasingly mobile healthcare ecosystems.

2 RELATED LITERATURE

Mobile technologies have greatly changed how healthcare is delivered, how patients are monitored, and how clinical decisions are made [11–12]. mHealth tools such as wearable sensors, apps and cloud-based platforms help collect biomedical data in real time, provide remote care and support personalised treatments [13]. These technological advancements have improved healthcare accessibility and operational efficiency while enabling continuous patient engagement across digital healthcare environments. However, the growing dependence on mobile biomedical technologies has also intensified concerns regarding cybersecurity, patient privacy, data protection and regulatory accountability [14]. The distributed architecture, reliance on wireless communication networks and integration with third-party platforms render mobile biomedical systems especially susceptible to cyber threats, unauthorised access and data breaches [15]. As a result, healthcare institutions must implement robust governance structures, enforce regulatory COM, and maintain continuous DO to safeguard system reliability and patient data security [10].

2.1 Data governance

Data governance plays a key role in ensuring the security of biomedical information [15]. It includes the policies, standards, and accountability systems that guide how data is handled from start to finish [2]. Good governance keeps data accurate, clarifies operations, and helps organisations comply with regulations [7]. In mobile biomedical systems, these practices reduce risk by ensuring that data from mobile devices remains reliable and secure [10–12]. Strong governance also encourages standardisation and interoperability through clear management. However, there is still little research on how governance directly impacts SP and security in mobile environments.

2.2 Regulatory compliance

Compliance plays a key role in making mobile biomedical systems trustworthy by adhering to legal frameworks such as HIPAA, GDPR and Indonesia's Personal Data Protection Law. Protecting the confidentiality, integrity, and availability of information helps build institutional legitimacy and patient trust [8]. On the other hand, not following these rules can lead to financial penalties, damage to reputation and more cybersecurity risks. COM is important, but it needs to be part of a wider approach that includes governance and oversight to work well. Right now, there is little quantitative evidence linking COM practices to measurable performance and security outcomes in mHealth technologies [16].

2.3 Digital oversight

Digital oversight connects high-level governance with real-time COM [17]. It involves ongoing monitoring, auditing, access controls and the detection of unusual activity to keep biomedical technologies secure. Studies show that strong oversight lowers cybersecurity risks and makes healthcare systems more reliable [18]. Oversight helps organisations identify weaknesses and enforce standards, keeping them accountable under regulations [19]. In mobile biomedical settings, where data is distributed and patient interactions occur in real time, ongoing oversight is crucial for managing ongoing changes [20]. Still, most research has examined oversight in isolation, without considering how it works alongside governance and COM. Although some studies have examined governance, COM and oversight separately, there is little empirical research on how these factors, taken together, affect the performance and security of mobile biomedical technologies. Most existing literature focuses on traditional healthcare IT or theoretical discussions, leaving a shortage of quantitative evidence on integrated regulatory frameworks in today's mHealth systems [21–22]. Mobile technologies also bring specific challenges, such as remote access and ongoing data transmission, which set them apart from older systems [23]. This study aims to fill these gaps by conducting a comprehensive empirical investigation into the influence of interconnected socio-technical mechanisms on operational outcomes.

3 METHODOLOGY

3.1 Research design

This study used a quantitative cross-sectional design to explore how DG, COM and DO affect SP and security in mobile biomedical systems. It was based on

Socio-Technical Systems Theory, which examines how organisational governance and regulations shape technology outcomes.

3.2 Population and sampling

The target population comprised healthcare professionals, IT managers, COM officers, DG specialists and biomedical technology administrators engaged in mobile healthcare systems in Indonesia. Respondents were selected from hospitals, biomedical firms, digital healthcare providers and organisations involved in regulatory activities. The study used purposive sampling to select respondents from hospitals, biomedical companies, digital healthcare providers and regulatory organisations in Indonesia, resulting in 200 valid responses.

3.3 Data collection and ethical consideration

We collected data using an online questionnaire shared through professional healthcare networks and institutional email. The survey focused on professionals working with mobile biomedical technologies and healthcare information management. Data collection lasted four weeks.

Participation was voluntary. Before starting the survey, respondents were told about the study's goals, confidentiality and anonymity. We did not collect any personally identifiable information, and all responses were stored securely for research purposes only.

3.4 Instrument design and reliability

We collected data using a structured questionnaire based on established studies in healthcare governance, digital COM, and biomedical system regulation. The instrument was designed to measure five constructs: DG, COM, DO, SP, and SS. Table 1 shows that all measurement constructs had acceptable internal consistency and were suitable for regression analysis. In this study, a Likert scale of 5, where 1 = strongly disagree and 5 = strongly agree.

Table 1. Instrument construct and reliability

Construct	Reference	Items	Cronbach's Alpha
Data Governance	Sharma [2], Tiffin [16]	5	0.88
Compliance	Sarabdeen [7]; Kharisma and Diakanza [9]	5	0.85
Digital Oversight	Vadisetty [10]; Anioke and Atima [20]	5	0.83
System Performance	Tsvetanov and Pandurski [1]	3	0.86
System Security	Baig et al. [5]	3	0.89

3.5 Data analysis

We analysed the data using SPSS software. Descriptive statistics and Pearson correlation analysis were used to examine respondent characteristics and the

relationships among variables. We also ran two separate multiple linear regression analyses. Before doing this, we checked that the data met the assumptions of normality, linearity, homoscedasticity, and multicollinearity. To assess the significance and strength of the relationships, we reported standardised beta coefficients (β), t-values, p-values, and R^2 values.

4 FINDINGS AND DISCUSSION

4.1 Descriptive statistics

Table 2 indicates that respondents are from the diverse professional and organisational backgrounds associated with the governance of mobile biomedical systems in Indonesia. The majority were male (59%), and the predominant age group was 31–40 years (39.5%). These findings indicate that the sample primarily consisted of mid-career professionals engaged in digital healthcare management and regulation. Most respondents were IT managers (31.5%), followed by COM officers (26%) and DG specialists (24%). This means the sample included people with direct experience in healthcare technology, regulatory COM, and biomedical DG. Participants worked in hospitals (43%), biomedical firms (30.5%), and regulatory agencies (26.5%), so the survey included several sectors involved with mobile biomedical technologies. Regarding professional experience, 46% of respondents reported 10 years, and 32% reported more than 10 years. This suggests that most participants were highly familiar with healthcare information systems and digital regulatory environments, which strengthens the reliability of the responses.

Table 2. Demographic profile of respondents

Demographic Variable	Category	Frequency	Percentage (%)
Gender	Male	118	59.0
	Female	82	41.0
Age	21–30 Years	54	27.0
	31–40 Years	79	39.5
	41–50 Years	47	23.5
	Above 50 Years	20	10
Position	IT Managers	63	31.5
	Compliance Officers	52	26
	Data Governance Specialists	48	24
	Healthcare Administrators	37	18.5
Organisation Type	Hospitals	86	43
	Biomedical Firms	61	30.5
	Regulatory Agencies	53	26.5
Experience	Less than 5 Years	44	22
	5–10 Years	92	46
	More than 10 Years	64	32

Table 3 shows the descriptive statistics for the study variables. All measured factors had mean values above 3.9, suggesting that participants viewed governance, COM, oversight, SP, and SS in the mobile biomedical system positively. SS had the highest mean score (M = 4.20), followed by SP (M = 4.16). This shows that respondents saw mobile biomedical systems as secure and effective. DG also scored high (M = 4.12), indicating positive views of organisational policies and data management. COM and DO had mean scores of 4.05 and 3.98, showing that participants viewed regulatory adherence and monitoring in a positive light. The low standard deviation across all constructs suggests a high level of consistency in respondents' perceptions. Figure 1 presents the mean scores for each study variable.

Table 3. Descriptive statistics

Variables	Items	Mean	Std. Deviation
Data Governance (DG)	5	4.12	0.61
Compliance (COM)	5	4.05	0.67
Digital Oversight (DO)	5	3.98	0.72
System Performance (SP)	3	4.16	0.59
System Security (SS)	3	4.20	0.57

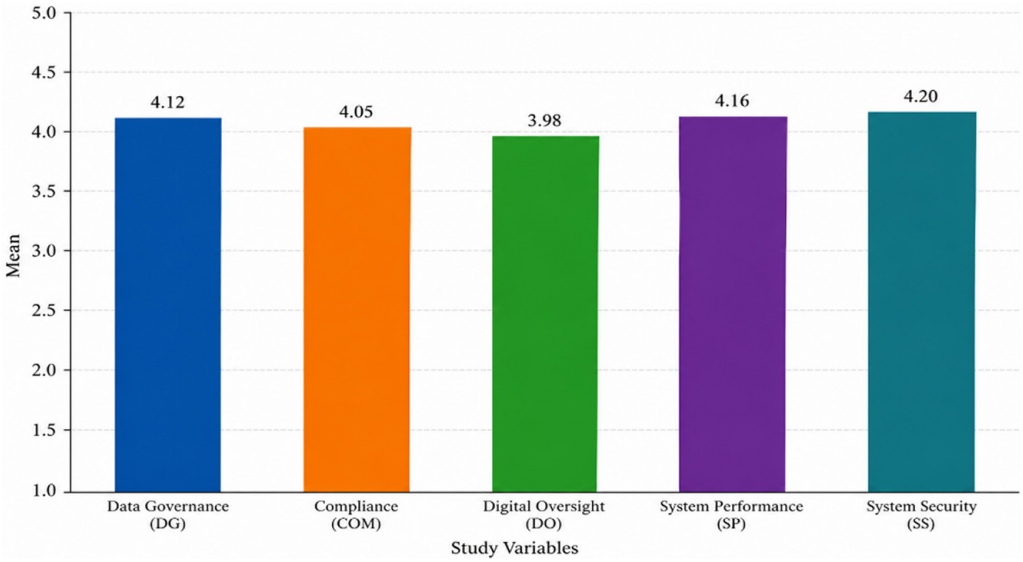

Fig. 1. Descriptive statistics of study variables

4.2 Correlation analysis

Table 4 shows positive and statistically significant correlations among all the variables. DG had the strongest correlation with SS (r = 0.718), followed by SP (r = 0.684). These results suggest that good governance practices are closely tied to better security and operational results in mobile biomedical systems. The correlation coefficients remained below the established multicollinearity threshold, demonstrating acceptable relationships among the independent variables.

Table 4. Correlation matrix

Variables	DG	COM	DO	SP	SS
Data Governance (DG)	1				
Compliance (COM)	0.612**	1			
Digital Oversight (DO)	0.548**	0.587**	1		
System Performance (SP)	0.684**	0.641**	0.603**	1	
System Security (SS)	0.718**	0.672**	0.645**	0.701**	1

Note: (**$p < 0.01$).

4.3 Regression analysis for system performance

A multiple linear regression analysis was performed to assess the effects of DG, COM, and DO on SP and SS. All Variance Inflation Factor (VIF) values were below 5, indicating no multicollinearity concerns. Table 5 shows that the regression model explained 58.4% of the variance in SP ($R^2 = 0.584$). This means that DG, COM, and DO together played a key role in improving the operation of mobile biomedical systems.

Table 5. Model summary for the system performance

Model	R	R^2	Adjusted R^2	Std. Error of Estimate
1	0.764	0.584	0.578	0.421

Table 6 shows that the ANOVA results were statistically significant ($F = 91.338$, $p < 0.001$). This means the independent variables were strong predictors of System Performance.

Table 6. ANOVA results for system performance

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	49.21	3	16.405	99.338	0
Residual	35.84	196	0.179		
Total	84.3	199			

Table 7 indicates that each independent variable exerted a significant positive effect on SP. DG emerged as the strongest predictor ($\beta = 0.398$), followed by COM ($\beta = 0.321$) and DO ($\beta = 0.267$). These findings indicate that governance policies, regulatory COM, and monitoring mechanisms are critical for enhancing operational efficiency and reliability in mobile biomedical systems.

Table 7. Regression coefficients for system performance

Hypotheses	Variables	β	t-Value	p-Value	VIF	Decision
H1a	Data Governance → SPS	0.398	7.892	$p < 0.001$	1.634	Supported
H2a	Compliance → SPS	0.321	6.118	$p < 0.001$	1.52	Supported
H3a	Digital Oversight → SPS	0.267	5.284	$p < 0.001$	1.427	Supported

4.4 Regression model for system security

The regression model shown in Table 8 explained 62.3% of the variance in SS ($R^2 = 0.623$). This result shows that the regulatory variables have strong explanatory power for cybersecurity and data protection outcomes.

Table 8. Regression model for system security

Model	R	R^2	Adjusted R^2	Std. Error
1	0.789	0.623	0.617	0.403

The ANOVA results presented in Table 9 indicate that the regression model for SS is statistically significant ($F = 108.742$, $p < 0.001$).

Table 9. ANOVA results for system security

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	54.113	3	18.038	108.742	$p < 0.001$
Residual	32.517	196	0.166		
Total	86.630	199			

Table 10 shows that DG had the strongest effect ($\beta = 0.437$), suggesting that clear governance frameworks are key to protecting biomedical information and improving cybersecurity. COM and DO also had significant positive effects, demonstrating that adhering to regulations and ongoing monitoring are important for maintaining the security of mobile biomedical systems.

Table 10. Regression coefficients for system security

Hypotheses	Variables	β	t-Value	p-Value	VIF	Decision
H1b	Data Governance → SS	0.437	8.014	$p < 0.001$	1.634	Supported
H2b	Compliance → SS	0.349	6.572	$p < 0.001$	1.520	Supported
H3b	Digital Oversight → SS	0.291	5.903	$p < 0.001$	1.427	Supported

4.5 Discussion

The results indicate that DG, COM, and DO each have a significant impact on SP and SS in mobile biomedical systems. Structured governance frameworks are essential for enhancing operational reliability and safeguarding sensitive biomedical information. The strong impact of DG on SS and performance matches the findings of Anioke and Atima [20], who showed that governance models using performance metrics and regulatory oversight help improve healthcare system accountability and effectiveness. These results also support the work of Anklam [29], who found that new biomedical technologies require stronger governance to ensure digital healthcare remains safe and reliable. This study adds to these discussions by offering evidence that governance mechanisms lead to clear improvements in both operational and cybersecurity outcomes in mobile biomedical systems.

Compliance was also shown to have a positive and significant effect on SP and security. This means that following healthcare regulations, legal standards, and

ethical guidelines helps build organisational trust, lowers regulatory risks, and makes systems more stable. The study [24–26] demonstrates that regulatory frameworks such as HIPAA and GDPR are essential for maintaining secure and standardised digital healthcare environments. Similarly, Kamnoore et al. [23] highlight the growing importance of regulatory requirements for mobile medical applications in healthcare systems. Salameh et al. [28] emphasised the increasing significance of digital medical technologies and mHealth platforms within contemporary healthcare systems.

The observed positive effect of DO on both dependent variables suggests that continuous monitoring, auditing, and supervisory mechanisms are critical for ensuring the security and efficiency of mobile biomedical systems. Tettey et al. [22] identified cybersecurity oversight as a critical requirement for modern biomedical devices and digital healthcare systems. The findings support Socio-Technical Systems Theory by demonstrating that technological effectiveness in biomedical systems is significantly influenced by organisational governance structures, regulatory processes, and supervisory practices. These results are aligned with [27], which confirms that operational performance and cybersecurity resilience depend not only on technological infrastructure but also on institutional controls and regulatory accountability mechanisms. The findings suggest that healthcare organisations, biomedical technology providers, and policymakers in Indonesia should strengthen their governance, regulatory COM, and DO to help make mobile biomedical technologies safer and more effective.

5 CONCLUSION AND RECOMMENDATIONS

This study examines how DG, COM, and DO affect SP and security in mobile biomedical systems in Indonesia. The results showed that all three factors improved operational effectiveness and cybersecurity, with DG having the greatest impact. These findings suggest that clear governance policies, adherence to regulations, and ongoing DO are important for maintaining the reliability and security of mobile healthcare systems. The study also supports Socio-Technical Systems Theory by showing that how organisations are governed directly affects technological results in biomedical systems. This study concludes that healthcare organisations should strengthen governance frameworks, regulatory COM practices, and digital monitoring systems to enhance cybersecurity and operational reliability. Additionally, policymakers in Indonesia are encouraged to improve digital health regulations and promote standardised governance practices to support the secure and sustainable implementation of mobile biomedical technologies.

6 REFERENCES

[1] F. Tsvetanov and M. Pandurski, "Delay of transmitted data in the remote patient monitoring system through AMQP and CoAP," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 20, no. 7, pp. 130–144, 2024. https://doi.org/10.3991/ijoe.v20i07.47661

[2] P. Sharma, "Healthcare data governance ecosystems: Balancing privacy, innovation, and compliance in real-world evidence platforms," *IPHO-Journal of Advance Research in Science and Engineering*, vol. 3, no. 12, pp. 8–16, 2025. https://doi.org/10.5281/zenodo.17853218

[3] I. Perez-Pozuelo, D. Spathis, J. Gifford-Moore, J. Morley, and J. Cowls, "Digital phenotyping and sensitive health data: Implications for data governance," *Journal of the American Medical Informatics Association*, vol. 28, no. 9, pp. 2002–2008, 2021. https://doi.org/10.1093/jamia/ocab012

[4] B. A. Bene *et al.*, "Regulatory standards and guidance for the use of health apps for self-management in Sub-Saharan Africa: Scoping review," *Journal of Medical Internet Research*, vol. 26, p. e49163, 2024. https://doi.org/10.2196/preprints.49163

[5] M. M. Baig, H. GholamHosseini, and M. J. Connolly, "Mobile healthcare applications: System design review, critical issues and challenges," *Australasian Physical & Engineering Sciences in Medicine*, vol. 38, no. 1, pp. 23–38, 2015. https://doi.org/10.1007/s13246-014-0315-4

[6] L. Fitria, R. Eliza, and S. Sari, "Impact of social media advertising on business performance: Evidence from micro, small, and medium enterprises in Dumai City, Indonesia," *International Journal of Management Thinking*, vol. 3, no. 2, pp. 16–31, 2026. https://doi.org/10.56868/ijmt.v3i2.101

[7] J. Sarabdeen and M. M. Mohamed Ishak, "A comparative analysis: Health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)," *International Journal of Law and Management*, vol. 67, no. 1, pp. 99–119, 2025. https://doi.org/10.1108/ijlma-01-2024-0025

[8] H. Alnasser, "Negligence and data breaches under Saudi Arabian Personal Data Protection Law (PDPL): A doctrinal analysis approach," *Journal of Advances in Humanities Research*, vol. 4, no. 3, pp. 23–38, 2025. https://doi.org/10.56868/jadhur.v4i3.321

[9] D. B. Kharisma and A. Diakanza, "Patient personal data protection: Comparing the healthcare regulations in Indonesia, Singapore and the European Union," *International Journal of Human Rights in Healthcare*, vol. 17, no. 2, pp. 157–169, 2024. https://doi.org/10.1108/ijhrh-04-2022-0035

[10] R. Vadisetty and A. Polamarasetti, "Regulatory framework for digital health, data privacy, and cybersecurity," in *Sustainable Healthcare Systems in Africa*, CRC Press, 2025, pp. 132–153. https://doi.org/10.1201/9781003530879-10

[11] R. Jeya, H. A. Karim, and S. B. Mansor, "Artificial Intelligence and mobile apps support intelligent healthcare systems for mental health services," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 20, pp. 157–168, 2024. https://doi.org/10.3991/ijim.v18i20.50743

[12] I. V. Nastasa, A.-R. Artamonov, Ș. S. Busnatu, D. G. Mincă, and O. Andronic, "From innovation to regulation: Insights from a bibliometric analysis of research patterns in medical data governance," *Informatics*, vol. 12, no. 3, p. 66, 2025. https://doi.org/10.3390/informatics12030066

[13] A. Saporito and B. Mrad Georgis, "Healthcare compliance and data governance," in *Healthcare Services Management*, Cham: Springer, 2025, pp. 391–406. https://doi.org/10.1007/978-3-032-12602-3_36

[14] J. S. Winter and E. Davidson, "Harmonizing regulatory regimes for the governance of patient-generated health data," *Telecommunications Policy*, vol. 46, no. 5, p. 102285, 2022. https://doi.org/10.1016/j.telpol.2021.102285

[15] A. Ashish and R. R. Pal, "Digital health and regulatory affairs: A comparative analysis of regulations in the USA, Europe, Canada, and Australia," *Applied Drug Research, Clinical Trials and Regulatory Affairs*, vol. 11, no. 1, p. e26673371404752, 2025. https://doi.org/10.2174/0126673371404752250827231906

[16] N. Tiffin, A. George, and A. E. LeFevre, "How to use relevant data for maximal benefit with minimal risk: Digital health data governance to protect vulnerable populations in low-income and middle-income countries," *BMJ Global Health*, vol. 4, no. 2, 2019. https://doi.org/10.1136/bmjgh-2019-001395

[17] J. Scheibner *et al.*, "Data protection and ethics requirements for multisite research with health data: A comparative examination of legislative governance frameworks and the role of data protection technologies," *Journal of Law and the Biosciences*, vol. 7, no. 1, p. 010, 2020. https://doi.org/10.1093/jlb/lsaa010

[18] A. Bernier, F. Molnár-Gábor, and B. M. Knoppers, "The international data governance landscape," *Journal of Law and the Biosciences*, vol. 9, no. 1, p. lsac005, 2022. https://doi.org/10.1093/jlb/lsac005

[19] H. M. Zangana, M. Omar, and J. N. Al-Karaki, "Regulatory frameworks in science, technology, and medical innovation," in *Navigating Law and Policy in STM Enterprises: Ethical Governance, Regulation, and Innovation Strategy*, IGI Global Scientific Publishing, 2025, pp. 1–34. https://doi.org/10.4018/979-8-3373-4862-9.ch001

[20] S. C. Anioke and M. E. Atima, "Public health governance models using process optimization and performance metrics for regulatory oversight," *International Journal of Advanced Multidisciplinary Research and Studies*, vol. 3, no. 6, pp. 2534–2548, 2023. https://doi.org/10.62225/2583049x.2023.3.6.5491

[21] F. A. Fernandes and G. V. Chaltikyan, "Analysis of legal and regulatory frameworks in digital health: A comparison of guidelines and approaches in the European Union and United States," *Journal of the International Society for Telemedicine and eHealth*, vol. 8, p. e11, 2020. https://doi.org/10.29086/jisfteh.8.e11

[22] F. Tettey, S. K. Parupelli, and S. Desai, "A review of biomedical devices: Classification, regulatory guidelines, human factors, software as a medical device, and cybersecurity," *Biomedical Materials & Devices*, vol. 2, no. 1, pp. 316–341, 2024. https://doi.org/10.1007/s44174-023-00113-9

[23] K. Kamnoore, M. P. Venkatesh, V. Balamuralidhara, and T. P. Kumar, "Regulatory requirements for mobile medical applications for USA, EU and other countries," *Journal of Pharmaceutical Sciences and Research*, vol. 11, no. 8, pp. 2910–2914, 2019. https://doi.org/10.5958/0974-360x.2020.00276.0

[24] M. R. Moshi, J. Parsons, R. Tooher, and T. Merlin, "Evaluation of mobile health applications: Is regulatory policy up to the challenge?" *International Journal of Technology Assessment in Health Care*, vol. 35, no. 4, pp. 351–360, 2019. https://doi.org/10.1017/s0266462319000461

[25] C. J. Vincent, G. Niezen, A. A. O'Kane, and K. Stawarz, "Can standards and regulations keep up with health technology?" *JMIR mHealth and uHealth*, vol. 3, no. 2, p. e3918, 2015. https://doi.org/10.2196/mhealth.3918

[26] G. Karageorgos *et al.*, "The promise of mobile technologies for the health care system in the developing world: A systematic review," *IEEE Reviews in Biomedical Engineering*, vol. 12, pp. 100–122, 2018. https://doi.org/10.1109/rbme.2018.2868896

[27] G. Tiwari, S. Kumar, and S. Sharma, "Biomedical applications based on mobile phone cell network systems," in *Smart Electronic Devices and Systems for Biomedical and Healthcare Applications*, New York, NY, USA: Apple Academic Press, 2025, pp. 155–187. https://doi.org/10.1201/9781003560852-7

[28] A. A. Salameh, I. A. Abu-AlSondos, N. H. Abu, and A. N. Harun, "Current knowledge and future possibilities of medical digital technologies based on mobile health," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 17, pp. 134–147, 2023. https://doi.org/10.3991/ijim.v17i17.42801

[29] E. Anklam *et al.*, "Emerging technologies and their impact on regulatory science," *Experimental Biology and Medicine*, vol. 247, no. 1, pp. 1–75, 2022. https://doi.org/10.1177/15353702211052280

7 AUTHORS

Ade Ikhlas Amal Alam is affiliated with the Faculty of Economics and Business, Hasanuddin University, Indonesia. His contribution to this research is particularly relevant to legal and regulatory perspectives on digital transformation, including public law and governance issues surrounding interactive mobile technologies. This background supports the present study by strengthening its analysis of regulation, accountability, and constitutional governance in the digital era (E-mail: adeikhlas@unhas.ac.id).

Khairunnisa Azrin is affiliated with the Faculty of Business Management and Professional Studies at Management and Science University, Malaysia. Her contribution to this study is relevant to governance, digital regulation, and institutional responses to the rapid expansion of interactive mobile technologies. This perspective supports the present research by enriching its discussion of legal oversight, media-related issues, and regulatory frameworks in contemporary digital environments (E-mail: khairunnisa_azrin@msu.edu.my).

Fakhrul Indra Hermansyah is an academic at the Faculty of Economics and Business, Hasanuddin University. His research and publications reflect a strong focus on Islamic economics and business, governance, Islamic finance, and digital transformation within organizations. As a key member of this research team, he contributed to strengthening the conceptual foundation, developing the research framework, and formulating academic arguments that bridge digital financial systems with the principles of Sharia governance (E-mail: rulindrasyah@unhas.ac.id).

Dr. Syamsu Alam is affiliated with the Faculty of Economics and Business, Hasanuddin University, Indonesia. His role in this collaborative research contributes to the discussion of governance, public policy, and the broader legal implications of interactive mobile technologies in society. This background is relevant to the study's focus on constitutional governance, digital rights, and public law in the digital era (E-mail: syamsu.alam@unhas.ac.id).

Andi Raina Ananda Herdiyana is affiliated with the Faculty of Economics and Business, Hasanuddin University, Indonesia. Her public academic profile indicates an interest in management-related studies, with particular relevance to organizational and business issues in contemporary settings. Her academic background and institutional affiliation support her contribution to research on interactive mobile technologies, organizational behaviour, and innovation in business environments (E-mail: rainaherdiyana@unhas.ac.id).