Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 8 (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

The State of Healthcare Cybersecurity in the Kingdom of Saudi Arabia: A Comparative Analytical Study in Jeddah

Hasan Salih Alqudah[1], Noha Omer Alaggad[1], Roba Yousef Alhujaili[1], Hind hameed Aljehani[1], Hadeel Hassan Alaslani[2]

[1]Department of Health and Hospital Services Management, College of Business/Rabigh, King Abdul Aziz University, Jeddah, Saudi Arabia.

[2]Department of Public Health. College of Health Science, Saudi Electronic University, Jeddah, Saudi Arabia.

[*]**Corresponding author**

Email ID : hasancare@gmail.com

Cite this paper as Hasan Salih Alqudah, Noha Omer Alaggad, Roba Yousef Alhujaili, Hind hameed Aljehani, Hadeel Hassan Alaslani, (2025) The State of Healthcare Cybersecurity in the Kingdom of Saudi Arabia: A Comparative Analytical Study in Jeddah..*Journal of Neonatal Surgery*, 14, (8) 973-982

ABSTRACT

Background:This paper sought to research and examine the issue of privacy and cybersecurity of health data in healthcare centres in Jeddah Governorate with reference to the legislative context of countries, specifically the Saudi Personal Data Protection Law (PDPL).

Methods:The study was designed based on three principal axes, including the organisational axis (strength of organisational policy, procedures of compliance and notification systems), the technical axis (infrastructure preparedness, encryption, backup systems, and multi-factor authentication), and the human axis (awareness of the staff and cybersecurity culture). The analysis was qualitative and quantitative in nature by employing a descriptive-analytical approach the research gathered data in the field using structured questionnaires and semi-structured interviews. The stratified random sampling was employed and the final sample of the 380 respondents of six healthcare facilities was taken that provided the variety of professional representation, i.e., physicians, nurses, technicians, administrators, and IT professionals.

Results:The findings revealed out that the organisational dimension was the most rated (mean = 4.05) and there were significant differences in sector based with government hospitals leading. The technical dimension had a score of 3.72 with no significant differences in sectors. The human dimension scored the least (mean = 3.45) and yet there was a strong positive relationship with the technical dimension, indicating that the most effective solution to technical practices is to enhance the awareness and training.

Conclusion:The results revealed gaps between local laws and international standards, recommending improvements in notification systems, technical infrastructure, and mandatory training to ensure data security and build trust in healthcare organisations

Keywords: Health Cybersecurity, Data Privacy, Saudi Personal Data Protection Law (PDPL), HIPAA, GDPR, Jeddah, Organisational Axis, Technical Axis, Human Axis, Stratified Random Sampling, Quantitative and Qualitative Analysis

1. INTRODUCTION

One of the dominant pillars of Saudi Arabia in terms of the Vision 2030 is healthcare digital transformation, and the Ministry of Health adopts innovative technologies, such as Electronic Health Records (EHRs), mobile health applications, and Internet of Medical Things (IoMT) to enhance healthcare efficiencies. Nonetheless, these innovations pose serious problems to privacy and security of health information which is sensitive and susceptible to cyber-attacks. The implementation of the Personal Data Protection Law (PDPL) in March 2023 will streamline the data protection, yet several issues, including the inability of health information systems and security infrastructure to integrate, as well as the absence of cybersecurity awareness among medical staff, are impediments to its adoption[1]. The study examines organisational, technical, and human aspects that influence health data protection and assesses the correspondence between local regulations and international standards. The purpose of the study is to determine the key impediments to the health data privacy in Saudi Arabia and suggest a framework of enhanced cybersecurity that can ensure the safety of data as well as the promotion of digital innovation. The study is important because cyber-attacks against healthcare facilities are on the rise, and the PDPL was recently introduced that requires one to comprehend how the policy is applied[1]. The research is based on Jeddah Governorate and offers a case study of different healthcare facilities with diverse digital maturity. This research aims to

.

Identify the organisational, technical, and human challenges that hinder protection of health data privacy in Saudi Arabia.

Assess the level of compliance between the PDPL and international standards such as HIPAA and GDPR.

Establish the level of cybersecurity awareness and practice among staff in the healthcare sector.

Propose an integrated framework for enhanced cybersecurity and health data protection without suppressing digital innovation.

2. LITERATURE REVIEW

Healthcare cybersecurity does not just against attacks but also takes into consideration risk management, business continuity, and recovery of disasters. According to a survey conducted by a study[2], healthcare data breaches cost the most, with an average of 10.93 million, the highest out of all industries. Hackers have a good opportunity of exploiting Electronic Health Records (EHRs) and IoMT devices because of the sensitive data that is stored in them and can be used to commit fraud or ransom[3, 4]. Medical equipment (infusion pumps) that is networked can also be attacked and this can pose a risk to patient safety[4]. In March 2023, the Saudi Personal Data Protection Law (PDPL) came into effect and is designed to control the process of personal data management in Saudi Arabia, including medical care. PDPL requires informed consent, which is secure, and limits the transfer of data beyond the Kingdom and timely notification of breaches[5]. HIPAA, enacted in 1996, provides the requirements that secure the Protected Health Information (PHI) in the U.S. in Privacy and Security Rules which comprise the encryption and access control provisions to allow the privacy, integrity, and availability of data[6]. The GDPR, which came into force in the year 2018, monitors the privacy of data throughout the Union of Europe (EU), and any organisation processing data of EU nationals is subject to the implementation of the law. It requires express approval, clear data treatment and obligates breach notification within 72 hours[7]. Failure to comply will attract a fine of up to 4% of global annual turnover.

The study[8] concluded that the process of reducing the threat of cybersecurity in healthcare can be achieved by enhancing organisational alignment and streamlining systems. Another study[9] stressed, effective data protection depends on the effective internal security culture that can only be reinforced by in-service training. An important research that is also one of the local Saudi Arabian studies[10] which were aimed at ensuring electronic health information security with structures compatible with HIPAA. Other papers noted gaps in cybersecurity awareness[11] identifying the dangers of phishing attacks, and another study[12] identifying the gaps in the utilisation of multi-factor authentication. The 2024 data breach in the Oxyhealth Clinics case[13] highlighted the need to have encryption and access controls. According to national reports, Saudi Arabia had the highest count of ransomware attacks in the Gulf region between 2021 and 2022, which affected the security of patient data[14]. According to a report[15], the region had fewer than 28% of hospitals fitted with advanced email defence mechanisms, which subjected them to cybersecurity threats. A lot of past research was either individual (organisational, technical, or human) or done in international comparisons without discussing the practical capabilities of Saudi healthcare[16, 17]. This study will fill the gap by combining law, organisation, and cybersecurity awareness and establishing a framework that would allow aligning PDPL with the standards of international trade, such as HIPAA and GDPR, within Saudi healthcare environments. Hence, the study has tested the following hypotheses:

First Hypothesis: Despite the robustness of regulations such as the PDPL, there is clear implementation gap with respect to international standards such as HIPAA and GDPR, particularly in aspects such as notification processes and technical infrastructure integration.

Second Hypothesis: Lack of awareness of cybersecurity among healthcare personnel is the most important factor that heightens the risk to health information even when there is a strong regulatory framework and an acceptable technical infrastructure.

Theoretical Framework

The Information Protection Theory is based on the CIA Triad (Confidentiality, Integrity, and Availability) that lies at the heart of healthcare cybersecurity. Confidentiality is a guarantee that patient data is accessible to authorised personnel, which is consistent with the consent principles of PDPL and GDPR[18]. Integrity guarantees data integrity and eliminates unauthorised changes with the help of the controls such as digital signature in HIPAA[19]. The Availability ensures that data and systems are available at the time of emergencies, backed up and recovered by the backup and recovery processes as it happened with Saudi Arabia in 20212022 with ransomware attacks[20]. This theory assesses the health care of Saudi in following PDPL, HIPAA and GDPR, and it is possible to determine where the balance of the CIA elements can be improved. Organisational, Technical, and Human (OTH) Model underlines that cybersecurity would need to be coordinated at the organisational, technical and human levels. Legal frameworks and compliance are handled by the organisational element and encryption, scanning, and emerging technologies such as blockchain are covered by the technical element[21]. The human factor is concerned with training and awareness. The breakdown in any of the dimensions affects the security of any cyber world therefore there is need to have a well-balanced governance, technology and human factors to ensure long-term safety of the data.

Table 1: Core Study Variables and Their Operational Definitions

Concept	Operational Definition
Health Cybersecurity	Technical and organisational procedures to protect health data from cyber threats[22].
Health Data Privacy	Patient control over how health data is collected, used, and stored, per PDPL and global standards[23].
Regulatory Compliance	Adherence to PDPL, HIPAA, and GDPR requirements in Saudi healthcare[24]
Security Awareness	Knowledge of cyber threats and best practices among healthcare staff[25].

The theoretical model ties directly to the research objectives by defining three independent variables: regulatory compliance, technical infrastructure quality, and cybersecurity training. These variables collectively influence the dependent variable—health data privacy protection.

3. METHODOLOGY

An analytical approach that was used is descriptive, which offered a detailed description of organisational, technical and human factors that influence health data privacy and cybersecurity in Saudi healthcare systems. The approach provides both the qualitative and the quantitative analysis, as it is possible to compare the work in various sectors of hospitals (government, private, and specialised) and identify gaps and inconsistency. The study applied both secondary (literature reviews, governmental reports) and the primary data (structured questionnaires and semi-structured interviews) to increase the validity of results. The paper targeted healthcare organisations in Jeddah that adopted Electronic Health Records (EHRs) and Internet of Medical Things (IoMT) technologies, and classified them as government and private, as well as special centres. In order to achieve a wide spectrum of data practices and maturity in cybersecurity, these institutions were chosen.

Table 2: Research Population

Sector	Institution Name	Affiliation	Operational Capacity	Distinguishing Features
Government	King Fahad General Hospital – Jeddah	Ministry of Health	Not specified	Largest public healthcare facility in western Saudi Arabia
	King Abdulasis Medical City – Jeddah	National Guard Health Affairs	751 beds	Advanced referral medical centre in Makkah region
Private	International Medical Centre (IMC)	Private	300 beds	Multidisciplinary, prominent private hospital in Jeddah
	Dr. Soliman Fakeeh Hospital	Private	Not specified	Ranked among the world's best hospitals
Specialised	King Faisal Specialist Hospital & Research Centre	Specialised Medical Institution	Not specified	Leading referral centre for oncology and organ transplantation

The sampled population was used to have a representative sample covering all types of healthcare institutions in Jeddah, such as government, private, and specialised healthcare centres, and it was possible to have a comprehensive overview of cybersecurity and data privacy practices in various healthcare segments. The sample sise was composed of 380 participants who were spread among six institutions as shown below:

Table 3: Sample Distribution by Institution Type and Number of Participants

Institution Type	Institution Name	Number of Participants
Government	King Fahad General Hospital – Jeddah	80
	King Abdulasis Medical City – Jeddah	70
Private	International Medical Centre (IMC)	50
	Dr. Soliman Fakeeh Hospital	45
	Saudi German Hospital – Jeddah	45
Specialised	King Faisal Specialist Hospital & Research Centre	90
Total	**6 Healthcare Institutions**	**380**

The sample was sized to ensure diversity across job categories (administrative, physicians, nurses, technicians, IT specialists) and to meet the 95% confidence level with a ±5% margin of error. A 5% increase accounted for incomplete data.

Table 4: Participants Distribution According to Job Status

Job Category	Number of Participants	Percentage
Physicians	110	28.9%
Nurses	130	34.2%
Technicians & Technologists	60	15.8%
Administrative Staff	50	13.2%
IT Specialists	30	7.9%
Total	**380**	**100%**

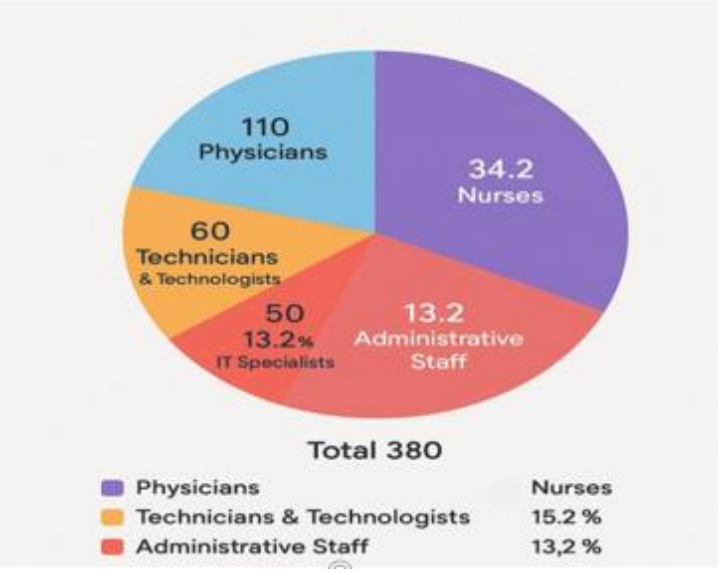

Figure 1: Distribution of the Study Sample by Professional Role

Two principal tools were used: a 45-point structured questionnaire and semi-structured interviews. The questionnaire was

divided into three dimensions—organisational, technical, and human—addressing compliance with PDPL, security measures (encryption, multi-factor authentication), and staff awareness.

Table 5: Questionnaire Distribution and Data Retrieval

Institution	Distributed	Completed	Incomplete	Valid Response Rate
King Fahad General Hospital – Jeddah	100	80	20	80%
King Abdulasis Medical City – Jeddah	90	70	20	77.8%
International Medical Centre (IMC)	65	50	15	76.9%
Dr. Soliman Fakeeh Hospital	60	45	15	75%
Saudi German Hospital – Jeddah	60	45	15	75%
King Faisal Specialist Hospital – Jeddah	100	90	10	90%
Total	**475**	**380**	**95**	**80%**

Twelve semi-structured interviews were conducted with key experts, including CISOs, IT managers, and members of the Saudi Data and Artificial Intelligence Authority (SDAIA), covering topics like PDPL enforcement, technical readiness, and cybersecurity culture. Data collection was coordinated with healthcare institutions, with a clear schedule and ethical standards. Questionnaires were distributed via both paper copies and electronic systems, with a two-week window for completion. Interviews were conducted with consent and recorded for transcription accuracy. The data collected from both questionnaires and interviews were analysed quantitatively and qualitatively. Cronbach's Alpha was used to test reliability, with results indicating high internal consistency (Cronbach's Alpha > 0.80) across all domains:

Domain	Number of Items	Cronbach's Alpha	Reliability Level
Organisational	15	0.89	Very High
Technical	15	0.86	High
Human	15	0.91	Very High
Total	**45**	**0.90**	**Very High**

Descriptive statistics of Likert scale responses revealed high organisational compliance, medium technical readiness, and low human awareness:

Domain	Mean	Standard Deviation	Level of Agreement
Organisational	4.05	0.78	High
Technical	3.72	0.85	Medium-High
Human	3.45	0.91	Medium
Overall	3.74	0.85	Medium-High

4. RESULTS

The section shows the quantitative and qualitative findings of the surveys and interviews done with the healthcare institutions of Jeddah Governorate. There were 475 questionnaires that were given out and 380 questionnaires returned. Also, there were 12 semi-structured interviews with the key experts (information security officers, IT managers, etc.). The findings are classified on the basis of the three key dimensions of the study which include organisational, technical and human dimensions.

Organisational Dimension Results

Table 6: Mean Scores and Standard Deviations – Organisational Dimension

Item	Mean	Std. Dev.	Agreement Rate
Written privacy policy	4.20	0.70	88%
Data breach notification mechanism	3.95	0.82	78%
Periodic review of data protection policies	4.00	0.79	80%

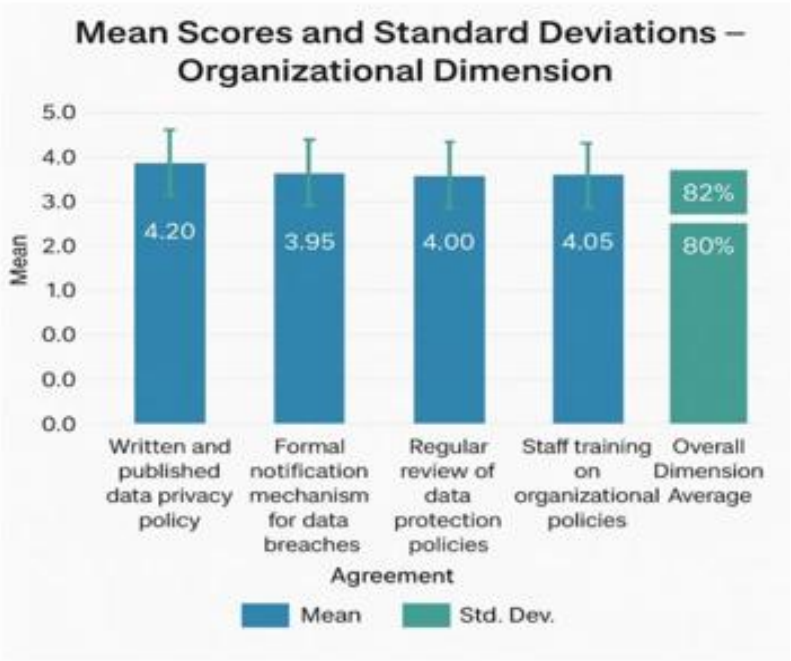

Figure 2: Mean Scores and Standard Deviations – Organisational Dimension

The scores show that the organisational policies are mostly well implemented with all the items scoring above 3.95. The written privacy policy had the highest score of 4.20, whereas the lowest score was 3.95 on the breach notification mechanism, which means that it can be improved by adding communication timeliness.

Technical Dimension Results

Table 7: Mean Scores and Standard Deviations – Technical Dimension

Item	Mean	Std. Dev.	Agreement Rate
Encryption systems	4.12	0.82	84%
External data backups	3.50	1.05	65%
Multi-factor authentication (MFA)	3.82	0.91	73%
Continuous threat monitoring	3.45	0.88	62%

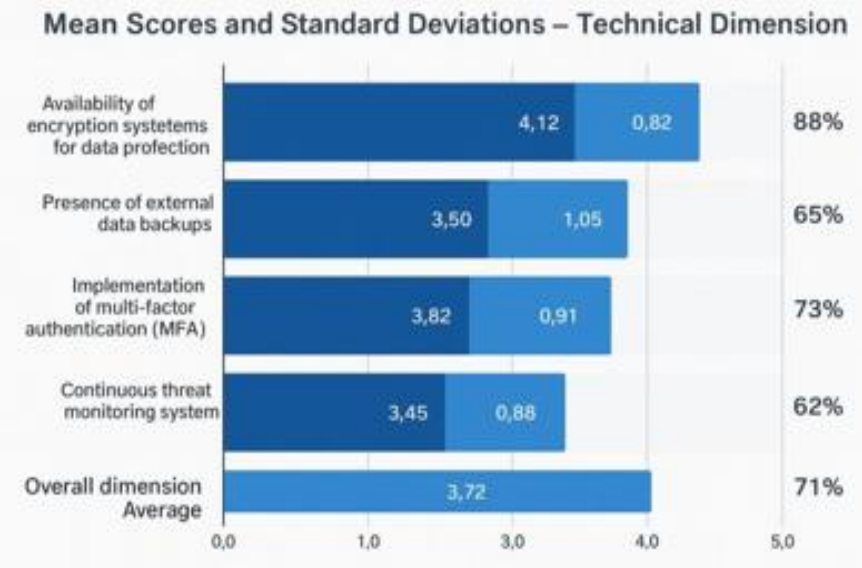

Figure 3: Mean Scores and Standard Deviations – Technical Dimension

The technical infrastructure is fairly robust, especially in the area of encryption systems (4.12), with the gap observed in the area of external backups (3.50) and continuous threat monitoring (3.45), which means that more extensive technical interventions are required.

Human Dimension Results

Table 8: Mean Scores and Standard Deviations – Human Dimension

Item	Mean	Std. Dev.	Agreement Rate
Regular security training	3.20	1.02	58%
Awareness of phishing procedures	3.55	0.95	68%
Compliance with password policies	3.60	0.88	70%
Reporting suspicious activity	3.45	0.90	66%

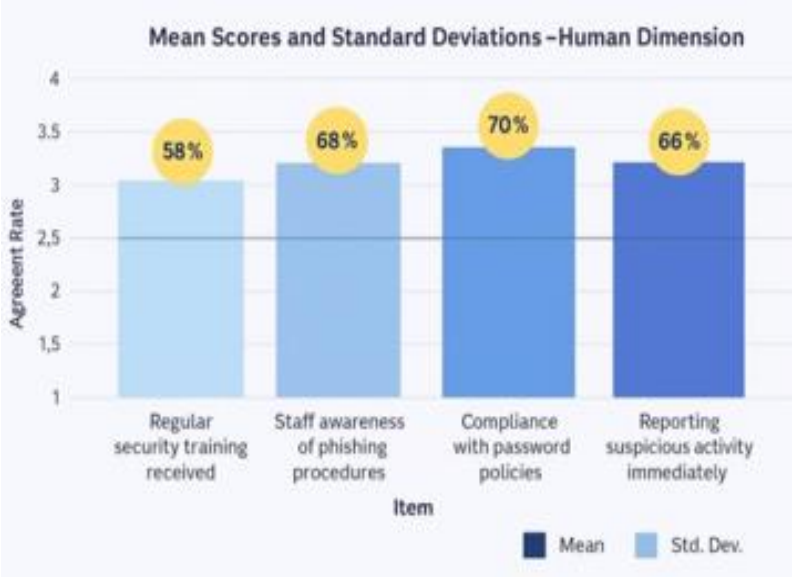

Figure 4: Mean Scores and Standard Deviations – Human Dimension

The human dimension was the least scored and the highest score was on compliance with password policies (3.60). It is also important to note that there should be better security awareness and training programs since none of the items scored higher than 3.60.

Comparison of the Three Dimensions

Table 9: Overall Means of the Three Dimensions

Dimension	Mean	Standard Deviation	Agreement Rate
Organisational	4.05	0.78	82%
Technical	3.72	0.85	71%
Human	3.45	0.91	65.5%

The highest score was received on the organisational dimension (4.05) whereas the lowest was recorded on the human dimension (3.45). This gap means that more funds should be invested in human resource development and training.

Figure 5: Comparison of the Three Dimensions

These results indicate that although organisational policies are fairly robust, technical infrastructure and human awareness gap considerably require filling in. There are necessary improvements in the area of training, technical controls like backups and the improvement of the practice of breach notification to promote cybersecurity in healthcare institutions in Jeddah Governorate.

5. DISCUSSION

The results of the study show that the organisational dimension was the most used (4.05) meaning that healthcare institutions in Jeddah have mostly adopted policies and procedures to protect data, as required by the Saudi Personal Data Protection Law (PDPL). Nevertheless, the breach notification process has some discrepancies, which align with a study[1] who concluded that healthcare organisations still face the difficulty of informing about data breaches on time, suggesting a lack of regulatory standards and practice compliance. A mean of 3.72 shows the technical dimension that is developed, particularly in the fields of encryption and multi-factor authentication. However, it was found that offline backups are vulnerable to intrusion and a continuous threat monitoring system, which is in line with the results of a study cited above[2] that show that even complex security systems can lack some traditional security features, such as regular backups. Although some standardisation exists between the public and the private hospitals, the latter are more likely to adopt and renew technology, according to a study[3]

The human dimension with the lowest mean (3.45) points out the urgency to have regular security training, the least score has been made on the frequency of training (3.20). This observation agrees with the literature[4], who have highlighted the human factor as the greatest risk to data security in Saudi Arabia. Also, the fact that the staff awareness is closely related to the technical efficacy ($r = 0.71$) confirms the results of the past study[5], who observed that training is closely tied to the efficiency of technological practices. Overall, the healthcare organisations in Jeddah demonstrate excellent organisational and technical structures, and staff lack of awareness of cybersecurity is still the most significant obstacle to the achievement of the optimal data protection. The theoretical framework correlates with the study, as it is necessary to focus on the

organisational, technical, and human factors and balance them to achieve effective data security. Ongoing education and culture of security are necessary to enhance the general state of cybersecurity within the healthcare facilities.

6. CONCLUSION AND RECOMMENDATIONS

The purpose of the study was to evaluate health information privacy and cybersecurity of Jeddah health facilities with a focus on organisational, technical, and human aspects. The results showed that the organisational domain was the most powerful, and most of the institutions comply with the Saudi PDPL, but there is a need to enhance the breach notification. Encryption and multi-factor authentication were strengths of the technical infrastructure, whereas the weaknesses were based on offline backup and constant monitoring. The human factor, however, was the most lacking and poor training and awareness has influenced the performance of security measures. Health information security requires a harmonious combination of effective laws, technology, and human resources to achieve this. The suggested training, technical development, and transparency improvements will help to make the healthcare environment more secure and encourage the growth of trust between healthcare institutions and patients. The study suggests the need to conduct further studies in the area of healthcare cybersecurity in the Kingdom to keep up with the developments. To enhance the level of privacy of health data and cybersecurity, healthcare organisations in Jeddah should implement improved breach notification, revise the policies biannually, and develop an implementation guide of Saudi PDPL, tailored to smaller organisations. Technically they are expected to pay attention to offline backups, regular system restoration checks and real time monitoring systems 24/7. Cybersecurity training is to be conducted on a regular basis (simulated phishing attacks and performance reviews) to increase the degree of compliance and awareness of the security practices among the staff. Besides, an integrated strategy will be pursued by forming data security committees together with legal, technical, and HR to fit the national strategy like the Saudi Data and AI Authority (SDAIA) and annual security audits to maintain the practices and security gap close to each other.

Conflict of Interest Disclosure: The authors declare no conflict of interest.

Consent to Publiction: Author(s) declared taking informed written consent for the publication of clinical photographs/material (if any used), from the legal guardian of the patient with an understanding that every effort will be made to conceal the identity of the patient, however it cannot be guaranteed.

Author Contribution: Authors declare full authorship as advised by ICMJE and have approved the final version for publishing

REFERENCES

[1] Al-Kahtani N, Al-Sahrani A, Al-Shammari M, et al. Saudi Arabia's readiness for digital health transformation: Comparing public and private healthcare sectors in the Eastern Region. Securing Health Data in the Digital Age: Challenges, Regulatory Frameworks, and Strategic Solutions in Saudi Arabia.

[2] Ponemon Institute. Cost of a data breach report 2023. IBM Security.

[3] Kluge E, Howard W, Werner B, et al. Cybersecurity and data privacy in healthcare: Ethical and legal considerations. BMC Med Ethics. 2022;23(1):1–10. doi:10.1186/s12910-022-00783-3

[4] Aljedaani W, Alomar N, Bamasoud A. Security challenges of the Internet of Medical Things (IoMT) in smart healthcare: A review. Int J Adv Comput Sci Appl. 2020;11(10):1–9. doi:10.14569/IJACSA.2020.0111001

[5] Saudi Data & Artificial Intelligence Authority. Personal Data Protection Law (PDPL) and implementing regulations. Saudi Data & Artificial Intelligence Authority (SDAIA); March 2023.

[6] United States Department of Health & Human Services. Summary of the HIPAA privacy rule. U.S. Department of Health & Human Services; 2013.

[7] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J Eur Union. 2016;L 119:1–88.

[8] Jalali MS, Kaiser JP. Cybersecurity in hospitals: A systematic, organisational perspective. J Med Internet Res. 2018;20(5):e10059. doi:10.2196/10059

[9] Appari A, Johnson ME. Information security and privacy in healthcare: Current state of research. Int J Internet Enterp Manag. 2010;6(4):279–314. doi:10.1504/IJIEM.2010.035624

[10] Hakami N, Alshareef H, Helal M. A security framework to protect ePHI in Saudi Arabia's healthcare infrastructure. Int J Adv Appl Sci. 2024;11(4):167–181. doi:10.21833/ijaas.2024.04.019

[11] Shadadi E, Ibrahim R, Ghadafi E. Exploring cybersecurity and phishing attacks within healthcare institutions in Saudi Arabia: A narrative review. World Acad Sci Eng Technol Int J Comput Inf Eng. 2025;19(4).

[12] Aljedaani W, Alshammari R, Alfarraj O. Security awareness of end users of mobile health applications: An

empirical analysis. IEEE Access. 2020;8:123599–123613. doi:10.1109/ACCESS.2020.3007530

[13] Cyber Press. Kill hacking group claims breach of Saudi Arabia Oxyhealth Clinics. Cyber Press; November 11, 2024.

[14] Group-IB. Hi-Tech Crime Trends 2022/2023 report [Cyber-security research]. Arab News; January 17, 2023.

[15] Proofpoint. UAE and KSA hospitals exposed to email scam, Proofpoint warns. TECHx Media; July 13, 2023.

[16] Yawson RM. Systems thinking and the future of health informatics: A systems approach to health data privacy and cybersecurity. J Am Med Inform Assoc. 2021;28(6):1222–1229. doi:10.1093/jamia/ocab013

[17] Alhussain T, Drew S, AlGhamdi R, Turki. A governance framework for cybersecurity in Saudi Arabian healthcare organisations: Bridging national and international regulations. Health Policy Technol. 2022;11(3):100635. doi:10.1016/j.hlpt.2022.100635

[18] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J Eur Union. 2016;L 119:1–88.

[19] United States Department of Health & Human Services. Summary of the HIPAA security rule. U.S. Department of Health & Human Services; 2013.

[20] Group-IB. Hi-Tech Crime Trends 2022/2023 report. Group-IB; January 17, 2023.

[21] Alhussain T, Drew S, AlGhamdi R, Alhussain T. A governance framework for cybersecurity in healthcare organisations in Saudi Arabia: Bridging national and international regulations. Health Policy Technol. 2022;11(3):100635. doi:10.1016/j.hlpt.2022.100635

[22] Alhussain T, Drew S, AlGhamdi R, Alhussain T. A governance framework for cybersecurity in healthcare organisations in Saudi Arabia: Bridging national and international regulations. Health Policy Technol. 2022;11(3):100635. doi:10.1016/j.hlpt.2022.100635

[23] Saudi Data & Artificial Intelligence Authority. Personal Data Protection Law (PDPL) and implementing regulations. Saudi Data & Artificial Intelligence Authority (SDAIA); March 2023.

[24] United States Department of Health & Human Services. Summary of the HIPAA security rule. U.S. Department of Health & Human Services; 2013.

[25] Shadadi E, Ibrahim R, Ghadafi E. Exploring cybersecurity and phishing attacks within healthcare institutions in Saudi Arabia: A narrative review. World Acad Sci Eng Technol Int J Comput Inf Eng. 2025;19(4)..