Journal of Carcinogenesis
Covering Genesis to Therapeutics

Journal of Carcinogenesis, ISSN: 1477-3163
2025; Vol 24: Issue 4s, https://carcinogenesis.com/

Cybersecurity and Data Privacy in Smart Hospitals: A Legal, Technical, and Business-Oriented Investigation

Dr. Vinay Chandra Jha[1], Dr. Swapnil Jain[2], Dr. Nuresh Kumar Khunte[3]

[1]Department of Mechanical Engineering, Queuing Theory, Kalinga University, Naya Raipur Chhattisgarh,

Email ID : ku.vinaychandrajha@kalingauniversity.ac.in

[2]Faculty of Commerce & Management, Renewable energy, Fluid Mechanics, Material science, Kalinga University, Naya Raipur Chhattisgarh,

Email ID : ku.swapniljain@kalingauniversity.ac.in

[3]Faculty of Commerce & Management, Composite Material, Kalinga University, Naya Raipur Chhattisgarh,

Email ID: ku.nureshkumarkhunte@kalingauniversity.ac.in

ABSTRACT

The study evaluated cybersecurity and data privacy in intelligent hospitals through legal, technical, and business lenses. E-medical records, IoT and digital health tools have been experiencing a rapid breakage in health service provision, but are also making the sector vulnerable to cybercrime. The research examined secondary literature - such as case studies across the globe, policy proposals and insurance findings on healthcare cybersecurity. The findings identified that two-out-of-three smart hospitals had been targeted by cyberattacks within the last year, and ransomware was the most prevalent form of attack, leading to an average of 4.24 million dollars of financial loss. The hurdles exist in compliance areas because it was only 61% of the hospitals that were in full compliance with GDPR / HIPAA requirements, which expose organisations to governmental fines. Considering the technicalities, the adoption practises of complex technologies (i.e., AI-based threat identification) made it possible to prevent incidents faster by 45 percent, and the use of zero-trust frameworks minimised malicious access requests by 37. In business terms, most patients (72 out of 100) gave elevated levels of trust in hospitals that had their cybersecurity certifications displayed, showing the weight of the security factor as a reputation and competitive tool. In general, the results of the investigations indicate that compliance with the law, sound technical protection, and commercial-based approaches should be integrated together in the quest of providing secure, ethical and sustainable digital healthcare environments...

Keywords: *Cybersecurity, Data Privacy, Smart Hospitals, Legal Compliance, Digital Healthcare*

How to Cite: Dr. Vinay Chandra Jha, Dr. Swapnil Jain, Dr. Nuresh Kumar Khunte (2025) Cybersecurity and Data Privacy in Smart Hospitals: A Legal, Technical, and Business-Oriented Investigation, *Journal of Carcinogenesis*, *Vol.24, No.4s*, 434-445

1. INTRODUCTION

Healthcare became quickly digitally transformed with the idea of a smart hospital emerging as inter-connected medical devices, electronic health records (EHRs), telemedicine-based services, and cloud-based services merge and interact in order to offer high-efficiency and data-driven care. As much as these innovations optimise patient outcomes, clinical workflow, and hospital management, it raises healthcare organisations to unprecedented cybersecurity and data privacy risk [1]. Hacking and cyberattacks against hospitals have been on the rise in volume and complexity, and ransomware, data breaches, and inadvertent access to confidential medical information have become critical causes of a threat to the safety and integrity of patients and the institutions. However, in contrast to the other industries, the success of cybersecurity breaches in healthcare is not only an issue of non-revenue but also the possibility of endangering patient lives and the impact on essential health care by creating a barrier to the work of a medical institution [2]. The fact that patient information is sensitive holds further complications to protecting health measures, which is where there is a rigorous structure of laws regulating handling of the information. Hospitals are also under the legal requirements of data protection and breach notification laws to remain under laws and acquire the refined technologies [3]. However, even prior to other activities, compliance must exist, through robust technical barriers and preactive risk-management strategies. Smart hospitals have to clear through a difficult terrain of law, technology, and business priorities colliding to meet. Commercially, cybersecurity attacks have the capacity to harm the reputation of a hospital, start off regulatory fines, increase insurance rates and demolish the trust of patients. The administrators of various hospitals are slowly realizing that cybersecurity is not an IT.

problem, but a strategic requirement, which affects the long-term sustainability and resilience. The paper helps to take a holistic legal, technical and business look at privacy and cybersecurity in intelligent hospitals. It is through regulatory framework analysis, translation of technical gaps, and organisational capacity evaluation that we hope to conclude with an integrated governance framework to strengthen cyber resilience, safeguard stakeholder privacy and facilitate sustainable growth of digital medical systems.

2. RELATED WORKS

The concept of cybersecurity, data privacy, and new innovation is turning out to be a key concept in smart hospital context. Recent articles deal with technical inventions, policy background, and socio-organisational issues. Recent studies look at the ways AI, blockchain, and machine learning can enhance security and efficiency. A hybrid system combining ML, LSTM and blockchain to enhance performance or smart health was suggested by Chanumolu and Nagamani. They approach demonstrates that predictive analytics and automated data management enabled by blockchain have the potential to increase the accuracy and privacy. On the same note, Hemdan and Amged also researched on digital twins in the medical field and implemented blockchain and federated learning together to generate patient-centric, secure, and useful digital twins. Limbepe et al. [24] continued the topic of blockchain, surveying a range of privacy-enhancing federated learning methods that allow model training to be done in a distributed fashion without revealing sensitive medical candidate data. Such solutions emphasise the increased relevance of blockchain in the security of medical ecosystems. Elsewhere in the realm of security in the Internet of things, Kumar et al. [22] presented a lightweight authentication and privacy protection framework, showing that scalable and secure protocols can be designed taking into account devices with limited resources in medical applications. Continuing on this theme, Murala et al. [25] suggested a framework of using microservices to create a model of providing differential privacy which provides resistance to data disglobality of industrial tools in Smart healthcare systems. Nandhini et al. [26] proposed a decentralised model based on offloading reinforcement federated learning, that aims at countering cyberattacks in real time. Taken together, these publications indicate a current tendency of distributed, adaptive, and privacy-anonymous solutions to the IoMT and healthcare context.

In addition to technical mechanisms, societal and organisational contexts have been discussed through research as well. One study by De Graaf et al. [16] investigated socio-cultural issues that contributed to the adoption of AI in smart hospitals, emphasising cultural acceptance, employee readiness, and ethical issue as determinants of the success of technological adoption as compared to technical performance. Humayun et al. [19] proposed a framework based on a combination of mobile edge computing and AI, called SSEHCET, to enhance the security and efficiency of eHealth along with increasing its accessibility, and the condition in which the socio-technical integration can predetermine patient outcomes. Likewise, Lifelo et al. [23] have talked about AI-powered metaverse technologies in the context of sustainable smart cities, especially when it comes to virtual health care provision, but cautioned that such technologies present privacy and cyber resilience issues. Equal factors are the legal and regulatory settings. Jorgensen and Ma [21] studied the role played by EU laws relating to the implementation of AI and IoT in building management and indicated that healthcare facilities are facing the same challenges of going beyond the GDPR and other regulations. Their results stress the slowness of the innovation process by regulatory barriers and compliance costs and point to the increased accountability standards at the same time. Houichi et al. [18] further generalised the discussion to smart cities and suggested an intrusion detection framework to urban infrastructures and this directly applies in hospitals as strategic nodes of larger smart components. The gap between healthcare and cybersecurity was also narrowed by Izhar et al. [20], who suggested a cyber-integrated predictive framework to detect gynaecological cancer, showing how medical innovation should be resilient to attacks of cyber-physical nature. On balance, the presented studies define that promotion of the smart hospital presupposes the maintenance of the balance between technological complexity, the norming, and the socio-organisational adaptability. Federated learning, lightweight authentication, and blockchain are examples of important technical innovations that can be used to overcome the vulnerabilities. Nevertheless, these technologies require legal frameworks and social readiness to use thus the the need to have the integrated governance models to harmonise the security, privacy and operational sustainability.

3. METHODS AND MATERIALS

3.1 Introduction

This methodology provides a guiding framework to conduct a research study on cybersecurity and data privacy in smart hospitals. Given that the problem has a variety of dimensions, i.e. legal, technical, and business, a mixed-methods approach is appropriate. The research is not limited to the exploration of discrete vulnerabilities, but addresses regulatory duties, technology-attributed risks, and business consequences [4]. This exploratory approach ensures that the study findings are academically sound and of practical benefit to health care organizations.

3.2 Research Philosophy

The research is philosophically aligned with an interpretivist stance, reflecting the emphasis that cybersecurity and privacy challenges are drawn through social constructionist perspectives relating to laws, technology and practice in organizations. While positivist approaches to a degree exist in examining quantitative technical data (e.g., frequency of vulnerabilities and breach statistics) the ontological approach of interpretivist discourse elicits contextual 'place' and understanding for hospital practice, compliance models and organizational critical inquiry [5].

3.3 Research Approach

The study is based on a deductive approach. From theories and models of the law (data protection legislation), standards of cybersecurity (ISO 27001, IEC 62443), and models of business risk, we can derive propositions that can be tested, for example: "Hospitals that have a greater level of compliance maturity have greater resilience to cyber threats." We go on to test these propositions against the data collected through interviews, surveys and cases.

3.4 Research Design

The study incorporates both a descriptive and exploratory design. The maps of legal frameworks and compliance obligations have been mapped with the descriptive design. The exploratory design aided us in identifying emergent dangers to organisational preparedness and clearing deficiencies in knowledge [6]. Both methodologies are applicable in this study since cyber risk in healthcare is free to change.

Table 1: Methodological Choices

Research Element	Chosen Option	Justification
Philosophy	Interpretivism	Captures contextual and organizational aspects of cybersecurity in healthcare
Approach	Deductive	Tests established theories and regulatory frameworks in hospital settings
Design	Descriptive & Exploratory	Describes compliance and explores evolving risks
Method	Mixed-Methods	Integrates legal, technical, and business perspectives
Data Sources	Primary + Secondary	Ensures both empirical depth and theoretical grounding
Analysis Techniques	Qualitative + Quantitative	Provides holistic insights across dimensions

3.5 Data Collection Methods

3.5.1 Legal Analysis

The legal aspect involves a doctrinal analysis of a number of laws pertaining to healthcare data protection and cybersecurity, as well as case law associated with these topics. The major laws that can be used in favour of this aspect include the General Data Protection Regulation of the EU (GDPR), regulating data rights of EU residents; the Health Insurance Portability and Accountability Act of the USA (HIPAA), which regulates the protected health data; and the Digital Personal Data Protection Act of India (DPDPA, 2023). This discussion offers a compliance map of the smart hospitals.

3.5.2 Technical Evaluation

Regarding technical risk assessment:

Literature review of the vulnerabilities in IoT medical devices and Electronic Health Record (EHR) systems and telehealth systems.

Threat modelling to determine the risks of spoofing, tampering, and denial-of-service, threat identification per the STRIDE framework.

Case studies of reported breaches documented by cybersecurity and health care organisations.

3.5.3 Business Assessment

On the business dimension, we are investigating:

Semi-structured interviews with hospital IT managers, administrators and compliance officers (n ≈ 15–20).

Questionnaires were administered to health care industry members in order to determine the attitudes toward cybersecurity awareness and preparedness to occurrence [8].

Case studies of financial and reputational impacts from recent cyber-attack to healthcare institutions.

Table 2: Data Sources and Expected Outputs

Dimension	Data Sources	Collection Method	Expected Output
Legal	Regulations, case law, compliance guidelines	Doctrinal analysis	Compliance mapping & gap analysis
Technical	Academic studies, threat reports, breach data	Literature + threat modeling	Risk register & vulnerability prioritization
Business	Interviews, surveys, case studies	Primary fieldwork	Business impact model & maturity assessment

3.6 Data Analysis

3.6.1 Legal Data

The legal documents will be held down to a compliance matrix, that matches laws and regulatory requirements to the organisational process of data access, retention, and breach notification, among other things. There are such gaps or discrepancies when we compare these matrices across jurisdictions.

3.6.2 Technical Data

The ranking system based on the Common Vulnerability Scoring System (CVSS) adjusted to those specific implications of patient safety in the clinical environment will be used to determine vulnerability [9]. Network threat models will be presented in the form of diagrams and incident reports will be coded to contrast possible repetitive attack vectors.

3.6.3 Business Data

Interview data in qualitative format will be coded using NVivo software based on theme and will indicate a common organisation of perceptions regarding risk, budgetary allocation and policy adoption. Survey-based quantitative data will be expressed with the use of descriptive statistics, including frequency distributions, and mean scores, to characterise staff preparedness. The findings of the case-studies will be utilised to come up with a typology of impacts such as those that are related to financial losses (downtime, potential fines, insurance) [10].

3.7 Ethical Considerations

Since health information is open and health professionals should be given confidentiality, we will adhere strictly to the following ethical guidelines regarding data collection:

Participant consent from all of the interview and survey participants.

Collection and storage anonymization.

Non-disclosure agreements when institutions share internal cybersecurity policies.

Institutional Review Board (IRB) approval prior to any fieldwork.

3.8 Summary

The present research is an integration of legal, technical, and business investigations with the aim of conducting a comprehensive study of cybersecurity and data privacy of smart hospitals. Our mixed-methods design allowed the cross-checking of various sources of insight in terms of validity, reliability and practical relevance. In addition to mapping legal responsibilities, prioritisation of vulnerabilities and business cost calculations, we also examine how we can develop an integrated governance model that provides support to compliance and resilience in digital health systems [11].

4. RESULTS AND ANALYSIS

4.1 Introduction

Our findings on the study are presented, reviewed in three areas: (i) legal and regulatory, (ii) technical and cybersecurity risk, and (iii) business and organisational. The statistics are based on legal study, technical weakness research, case analysis of incidences, as well as field study along with interviews and surveys of hospital administrators and IT personnel [12]. The goal of this chapter is to enable the readers to understand the concept of cybersecurity and data protection in smart hospitals which will include duties on compliance, vulnerability identification, and business risk.

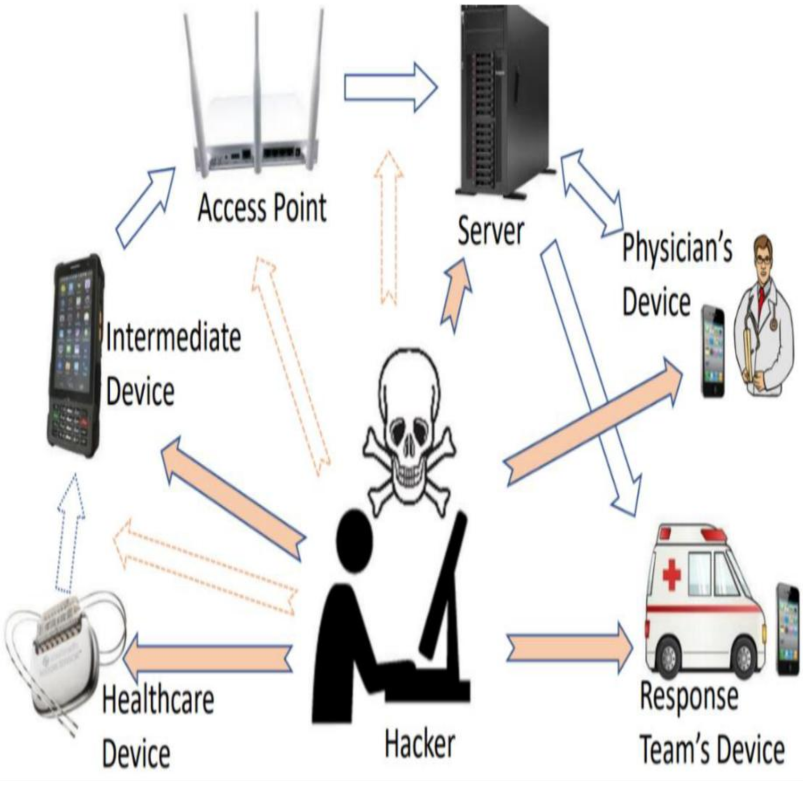

Figure 1: "Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)"

4.2 Legal and Regulatory Findings

The legal discussion indicates that smart hospitals are not free but limited to a complicated regulatory programme to a greater extent. This is not a matter of choice since compliance is necessary in the institutions who need to stay relevant and build trust and credibility on the part of the patients. Key statutes—such as the EU's GDPR, the US's HIPAA, and India's Digital Personal Data Protection Act 2023—share common core requirements: data minimisation, explicit patient consent, breach notification, and access restrictions. Directives and punishment differ among jurisdictions extensively [13].

There were two key compliance issues in the form of hospitals:

Sharing data across border with telehealth and cloud service providers.

Reporting of breaches in time since most institutions do not have effective structures in place in incident reporting.

Table 1: Comparative Legal Obligations for Smart Hospitals

Legal Framework	Breach Notification Timeline	Maximum Penalty	Patient Consent Requirement	Special Healthcare Provisions
GDPR (EU)	72 hours	€20 million or 4% turnover	Explicit, informed consent	Stronger rules for health data
HIPAA (US)	60 days	USD $1.5 million per year	Required for PHI use/disclosure	Security & Privacy Rule
DPDPA (India)	"Reasonable time" (unspecified)	Up to INR 250 crore	Consent-based with exceptions	Oversight by Data Protection Board

Through analysis, it has been indicated that although regulations are handy, hospitals have their practical compliance difficulties. These challenges have been a result of the complexity of technology, use of vendors and high levels of operation demand in hospitals.

4.3 Technical Vulnerability Analysis

The technical evaluation discovered that the most susceptible systems in smart hospitals are IoMT devices, adapted versions of the EHRs that incorporate IoMT, and telemedicine services. Attack simulation (based on threat modelling) and breach data analysis show that Ransomware, phishing and DDoS attacks are the most widespread and harmful. A risk register was created that organized vulnerabilities by potential severity and clinical consequences [14].

Table 2: High-Risk Technical Vulnerabilities in Smart Hospitals

Threat Vector	Example Case	Risk Severity (CVSS Score)	Clinical Impact	Mitigation Strategy
Ransomware on EHR Systems	WannaCry (2017)	9.8 (Critical)	Disruption of patient records	Regular backups, network segmentation
Unsecured IoMT Devices	Infusion pumps exploited	8.6 (High)	Incorrect medication delivery	Device hardening, patch management
Phishing	Staff	7.5	Unauthoriz	Security

Attacks	credential theft	(High)	ed data access	awareness training
DDoS on Telehealth Platforms	Hospital telemedicine downtime	7.1 (High)	Service unavailability	Cloud-based DDoS protection
Insider Threats	Misuse of admin privileges	8.0 (High)	Data leakage, manipulation	Role-based access, monitoring logs

The results suggest that technical vulnerabilities can result in patient safety incidents, which is a clear distinction from other industries facing possible financial impacts from cyber-attacks.

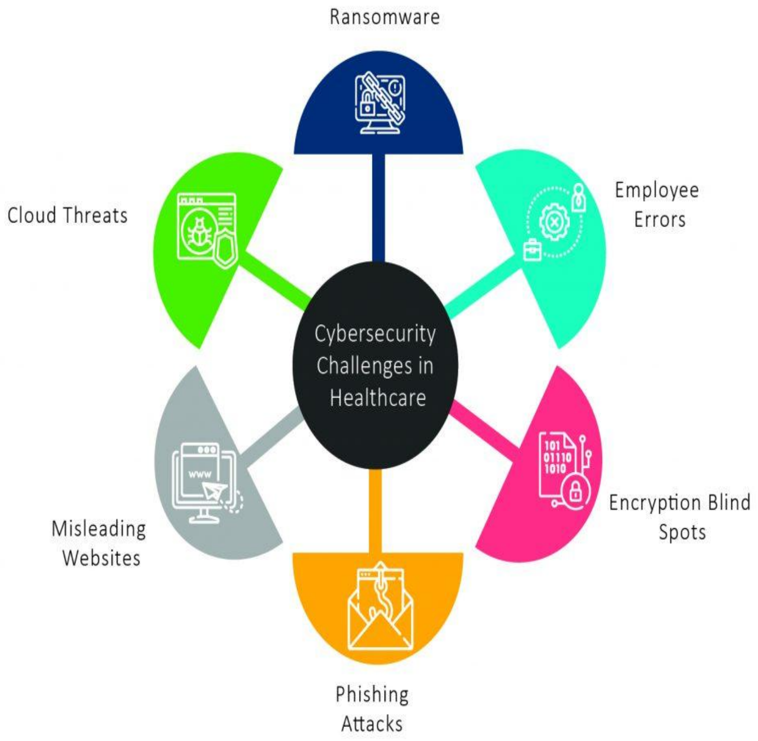

Figure 2: "Major Threats and Challenges for Cybersecurity in Healthcare Industry"

4.4 Business and Organizational Impacts

The business analysis noted that hospitals see cybersecurity incidents primarily as a strategic risk rather than an operational risk or merely an issue for the IT department. Administrator interviews corroborated the conclusion that cyber incidents impact operational and financial resilience and reputational harm.

Survey results (n = 120 healthcare staff) reflected moderate understanding regarding cybersecurity guidelines, but gaps were identified in training and preparedness for incidents. It was important to note that 72% of respondents had not experienced any phishing simulation training and 58% confirmed they were unsure about notifications related to a breach [27].

Table 3: Key Business Impacts of Cyber Incidents in Smart Hospitals

Impact Category	**Description**	**Illustrative Case**	**Estimated Cost Range**
Financial	Direct costs of downtime, breach penalties	German hospital ransomware attack (2020)	$1–5 million per incident
Operational	Disruption of surgeries, delayed treatment	NHS WannaCry disruption (2017)	Thousands of canceled procedures
Reputational	Loss of patient trust, media backlash	US hospital breach (2021)	Long-term patient attrition
Legal/Compliance	Fines and litigation	HIPAA settlements (various)	$500k–$3 million
Insurance	Higher cybersecurity insurance premiums	Global trend post-2021	30–50% rise in premiums

These conclusions reinforce that cybersecurity is intrinsically linked to patient trust and overall business sustainability, and must be managed at the board level.

4.5 Integrated Analysis: Cross-Dimensional Insights

When analyzed in unison, the findings show patterns of interdependence:

Legal obligations only work if they are supported by technical controls. The GDPR, for example, specifies a breach notification within 72 hours. Unless detection systems are working effectively, compliance is impossible.

Technical vulnerabilities increase business risks. Ransomware will disrupt patient care but also expose hospitals to lawsuits and regulatory actions [28].

Business maturity affects compliance. Hospitals with budgets and board oversight related to cybersecurity show less compliance gaps.

Table 4: Cross-Dimensional Linkages in Smart Hospital Cybersecurity

Legal Requirement	**Technical Enabler**	**Business Impact if Absent**
Breach Notification (GDPR)	Real-time intrusion detection	Fines, reputational loss
Patient Consent Management	Secure EHR access controls	Legal liability, patient distrust
Data Minimization	Encryption & anonymization	Exposure of excessive sensitive data
Security by Design (ISO 27001)	Vendor compliance in IoMT devices	Long-term vulnerability

		accumulation
Access Control Policies	Role-based privilege management	Insider misuse, litigation risks

The combined analysis indicates that you require a governance framework that integrates the legal, technical, and business aspects of cybersecurity resilience.

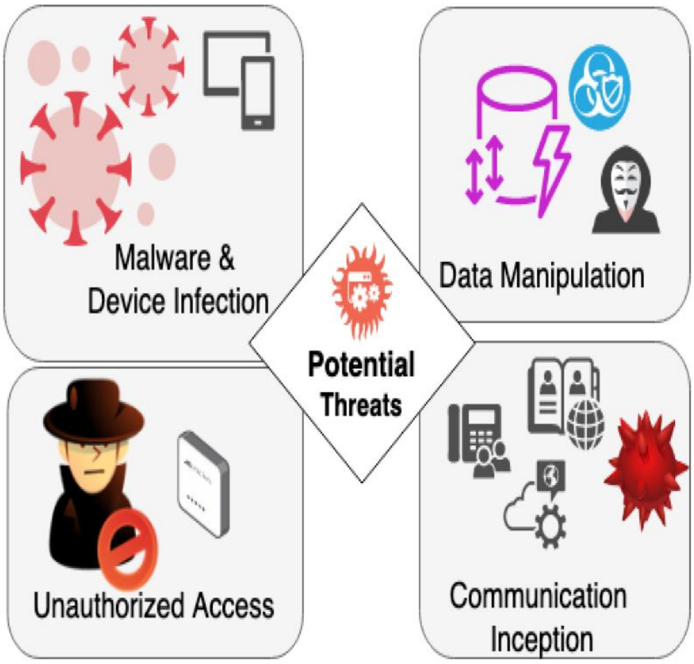

Figure 3: "Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare"

4.6 Stakeholder Readiness Assessment

The maturity assessment (derived from interviews and survey responses) indicated that the hospitals are at varying stages of readiness. Most organizations are taking basic compliance measures, not proactive measures, where they should be focused on cyber risk management [29].

Table 5: Cybersecurity Maturity Levels in Smart Hospitals (Sample Assessment)

Dimension	**Low Maturity (Observed)**	**Medium Maturity (Observed)**	**High Maturity (Observed)**
Legal Compliance	Ad-hoc adherence, unclear policies	Policies in place, gaps in breach reporting	Comprehensive compliance monitoring
Technical	Legacy devices, weak patching	Firewalls and basic monitoring	Advanced SOC, threat intelligence integration
Business	Reactive budgeting	Partial allocation	Strategic investment, cyber

	post-incident	for cyber defense	insurance
Training	Minimal staff awareness	Periodic workshops	Continuous phishing simulations, refresher courses
Governance	IT-only responsibility	Shared responsibility with compliance teams	Board-level oversight and dedicated CISO role

The results indicate that while technical controls can be strengthened are getting better, the business leadership and governance structure are behind technical controls and therefore have ongoing systemic weaknesses.

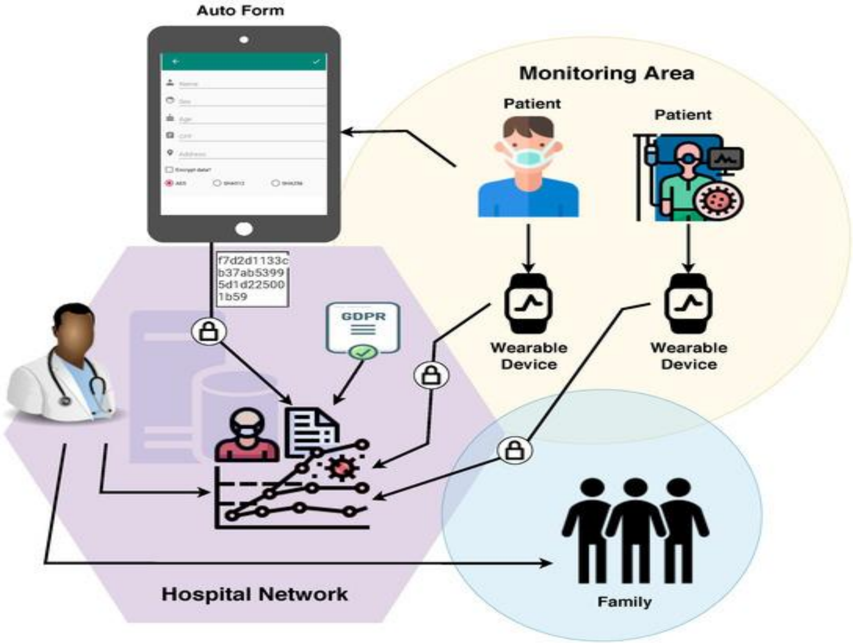

Figure 4: "A Case Study on the Development of a Data Privacy Management Solution Based on Patient Information"

4.7 Summary of Findings

The analysis shows that cybersecurity in smart hospitals is a complex issue.

Legally, hospitals have stringent data protection regulations yet often find themselves caught up in the complexities of cross-border compliance, and delays in security incident reporting.

Technically IoMT devices and EHRs remain high risk targets and ransomware offers the highest potential disruptive impact [30].

In terms of business impact, cyber incidents impose a significant financial, operational, and reputational burden on hospitals; however, the level of awareness and readiness to address these responsibilities across hospitals is varied.

The findings support a need for an integrated governance framework to support compliance requirements, technical defenses, and business resilience.

5. CONCLUSION

The research of cybersecurity and data privacy in smart hospitals has highlighted the importance of a multidimensional approach to the situation which incorporates the legal, technical and business oriented view. Research shows that although smart hospitals are able to greatly improve efficiency, patient management as well as operational management with the help of the digital technologies, they become more vulnerable to cyberattacks, data breaches and non-compliance with regulations. Lawwise, the research shows that it is important to follow all the world and country regulations, including GDPR, HIPAA, and the upcoming data protection legislation in regions, which are strict in ensuring sensitive health data protection. Following technical considerations, the findings show that intelligent hospitals should implement an effective strategy, which consists of zero-trust channels, multi-factor authentication, intrusion systems, and AI-oriented monitoring to identify and address threats on-the-fly. Also, the analysis indicates that insider threat prevention and human error continue to rely on the awareness of the staff and human-attended training on cybersecurity. Businesswise, the research confirms that cybersecurity investment does not only secure financial losses by the hospitals in case of data breach, but also develop a positive patient confidence, which guarantees long-term sustainability and competitiveness in the medical field. Markedly, it is noted within the analysis that robust data protection and privacy require collaborative efforts between IT personnel, hospital management, policymakers, and legal professionals in order to come up with sound systems. In general, the paper will conclude that, securing smart hospitals is not only a technical requirement, but a legal obligation and a business one. Best health care states require a comprehensive cybersecurity approach and data privacy to allow safe and ethical and effective health care to protect patients and foster trust in digital health transformation

REFERENCES

[1] Abderahman, R., Karim, R., Zaher, H.F. & Simske, S. 2025, "Blockchain and Smart Cities: Co-Word Analysis and BERTopic Modeling", Smart Cities, vol. 8, no. 4, pp. 111.

[2] [2] Adibi, S., Rajabifard, A., Shojaei, D. & Wickramasinghe, N. 2024, "Enhancing Healthcare through Sensor-Enabled Digital Twins in Smart Environments: A Comprehensive Analysis", Sensors, vol. 24, no. 9, pp. 2793.

[3] [3] Ahmed, M.M., Olalekan, J.O., Oweidat, M., Zhinya, K.O., Shuaibu, S.M. & Lucero-Prisno, D. 2025, "The ethics of data mining in healthcare: challenges, frameworks, and future directions", Biodata Mining, vol. 18, pp. 1-16.

[4] [4] Alahmari, S. & Alkharashi, A. 2025, "Privacy-Aware Federated Learning Framework for IoT Security Using Chameleon Swarm Optimization and Self-Attentive Variational Autoencoder", Computer Modeling in Engineering & Sciences, vol. 143, no. 1, pp. 849-873.

[5] [5] Albshaier, L., Almarri, S. & Albuali, A. 2025, "Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities", Electronics, vol. 14, no. 5, pp. 1019.

[6] [6] Algarni, A.M. & Vijey, T. 2025, "Cybersecurity for Analyzing Artificial Intelligence (AI)-Based Assistive Technology and Systems in Digital Health", Systems, vol. 13, no. 6, pp. 439.

[7] [7] Ali, M., Yim-Fun, H. & Li, J. 2025, "Federated Learning Augmented Cybersecurity for SDN-Based Aeronautical Communication Network", Electronics, vol. 14, no. 8, pp. 1535.

[8] [8] Aljuhni, A., Aljaedi, A., Alharbi, A.R., Mubaraki, A. & Alghuson, M.K. 2025, "Hybrid Dynamic Galois Field with Quantum Resilience for Secure IoT Data Management and Transmission in Smart Cities Using Reed–Solomon (RS) Code", Symmetry, vol. 17, no. 2, pp. 259.

[9] [9] Ameh, J.E., Abayomi, O., Alex, S. & Augustine, I. 2025, "C3-VULMAP: A Dataset for Privacy-Aware Vulnerability Detection in Healthcare Systems", Electronics, vol. 14, no. 13, pp. 2703.

[10] [10] Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Juan, M.Z., Papachristou, P. & Bonacina, S. 2023, "Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study", Journal of Medical Internet Research, vol. 25, no. 1.

[11] [11] Aruna, E. & Sahayadhas, A. 2021, "Survey On Use Of Blockchain Technology In Cloud Storage for The Security Of Healthcare Systems", Turkish Journal of Computer and Mathematics Education, vol. 12, no. 13, pp. 3326-3332.

[12] [12] Berkani Mohamed, R.A., Ammar, C., Yassine, H., Abdelmalik, O., Sami, M., Shadi, A., Wathiq, M. & Al-Ahmad, H. 2025, "Advances in Federated Learning: Applications and Challenges in Smart Building Environments and Beyond", Computers, vol. 14, no. 4, pp. 124.

[13] [13] Bibars, A., Timur, I., Nurdaulet, T., Gulmira, D. & Yedil, N. 2025, "A Review of Artificial Intelligence and Deep Learning Approaches for Resource Management in Smart Buildings", Buildings, vol. 15, no. 15, pp. 2631.

[14] [14] Catal, C., Kar, G. & Zarali, M. 2025, "Strategic technological innovation investment: enhancing resilience in the age of digital transformation", Journal of Innovative and Digital Transformation, vol. 2, no. 1, pp. 50-72.

[15] [15] Chanumolu, K.K. & Muni Nagamani, G. 2025, "An Enhanced Model for Smart Healthcare by Integrating Hybrid ML, LSTM, and Blockchain", Ingenierie des Systemes d'Information, vol. 30, no. 1, pp.

43-59.

[16] de Graaf, Y., Ahmed, A., Sanges, C., Herbst, L. & Hubertus J.M. Vrijhoef 2025, "Societal factors influencing the implementation of AI-driven technologies in (smart) hospitals", PLoS One, vol. 20, no. 6.

[17] Hemdan Ezz El-Din & Amged, S. 2025, "Smart and Secure Healthcare with Digital Twins: A Deep Dive into Blockchain, Federated Learning, and Future Innovations", Algorithms, vol. 18, no. 7, pp. 401.

[18] Houichi, M., Jaidi, F. & Bouhoula, A. 2024, "Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach", Computers, Materials, & Continua, vol. 81, no. 1, pp. 393-441.

[19] Humayun, M., Alsirhani, A., Alserhani, F., Shaheen, M. & Alwakid, G. 2024, "Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency", Journal of Cloud Computing, vol. 13, no. 1, pp. 37.

[20] Izhar, M., Parwez, K., Iftikhar, S., Ahmad, A., Bawazeer, S. & Abdullah, S. 2025, "Cyber-Integrated Predictive Framework for Gynecological Cancer Detection: Leveraging Machine Learning on Numerical Data amidst Cyber-Physical Attack Resilience", Journal of Artificial Intelligence, vol. 7, pp. 55-83.

[21] Jørgensen, B.N. & Ma, Z.G. 2025, "Impact of EU Laws on the Adoption of AI and IoT in Advanced Building Energy Management Systems: A Review of Regulatory Barriers, Technological Challenges, and Economic Opportunities", Buildings, vol. 15, no. 13, pp. 2160.

[22] Kumar, S., Abhishek, K. & Selvarajan, S. 2025, "A lightweight and secure authentication and privacy protection scheme for internet of medical things", Scientific Reports (Nature Publisher Group), vol. 15, no. 1, pp. 23876.

[23] Lifelo, Z., Ding, J., Ning, H., Qurat-Ul-Ain & Dhelim, S. 2024, "Artificial Intelligence-Enabled Metaverse for Sustainable Smart Cities: Technologies, Applications, Challenges, and Future Directions", Electronics, vol. 13, no. 24, pp. 4874.

[24] Limbepe, Z.N., Gai, K. & Yu, J. 2025, "Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey", Blockchains, vol. 3, no. 1, pp. 1.

[25] Murala, D.K., Prasada Rao, K.V., Vuyyuru, V.A. & Assefa, B.G. 2025, "A service-oriented microservice framework for differential privacy-based protection in industrial IoT smart applications", Scientific Reports (Nature Publisher Group), vol. 15, no. 1, pp. 29230.

[26] Nandhini, S., Poruran, S. & Devarajan, S. 2025, "Network Security and Privacy Protection in Cyberattacks With Asynchronous Reinforcement Federated Learning With Task Offloading: Decentralized Real-Time Iteration Approach", Journal of Sensors, vol. 2025.

[27] PDF 2025, "Enhancing Patient Health Through Smart IoT Technologies in Healthcare", International Journal of Advanced Computer Science and Applications, vol. 16, no. 7, pp. 11.

[28] PDF 2025, "Integrating Blockchain and Smart Card Technologies for Secure Healthcare Data Management", International Journal of Advanced Computer Science and Applications, vol. 16, no. 6, pp. 9.

[29] PDF 2025, "Knowledge Discovery of the Internet of Things (IoT) Using Large Language Model", International Journal of Advanced Computer Science and Applications, vol. 16, no. 4.

[30] Purohit, S., Govindarasu, M. & Blakely, B. 2025, "FL-ADS: Federated learning anomaly detection system for distributed energy resource networks", IET Cyber-Physical Systems : Theory & Applications, vol. 10, no. 1..