Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Institutionalizing Trust in Healthcare Cybersecurity: A Qualitative Analysis of Cyber Assurance and Investment Readiness

Vaidyanathan R. Iyer[1*], Dr. Kishore Babu[2], Dr. Vignesh Ram Guruswamy[3]
[1*]Research Scholar, Department of Management, KL University, Guntur, Andhra Pradesh 522302, India
[2]Dean Management Humanities & Science, KL University, Guntur, Andhra Pradesh 522302, India
[3]Assistant Professor, Department of Geopolitics and International Relations, Manipal Academy of Higher Education (MAHE), Manipal, Karnataka 576104, India
***Corresponding Author:** Vaidyanathan R Iyer
*Email: vaidy20221@yahoo.com

ARTICLE INFO

Received: 10 Nov 2024

Revised: 25 Dec 2024

Accepted: 12 Jan 2025

ABSTRACT

In India's fast digitizing healthcare sector, these vulnerabilities are fast becoming evident, as the frequency and sophistication of cyberattacks are increasing. Although more people are becoming aware of the need for cybersecurity programs, most institutions have low cybersecurity maturity characterized with disjointed controls, disjointed architectures, and strongly enforced policies. The sector's dependence on sensitive patient data, IoT devices and digital health platforms makes these gaps especially concerning. This article fills an urgent need for strategic, governance led response to cybercrime by introducing a concept of cyber assurance which is a trustcentric mechanism that certifies over time the effectiveness, continuity and institutional accountability of a cybersecurity framework. Cyber assurance can mean more than compliance, as it signifies resilience, internal governance and confidence on the part of shareholders. Using a qualitative methodology, the study utilizes semi-structured interviews with 15 cybersecurity experts from hospitals, health-tech firms and regulatory consultancies. Systematic inequalities in cybersecurity preparation emerge, dependent on the awareness of leadership, progress of regulations, and shifting expectations of investors, based on the thematic analysis. This transition of cyber assurance practice from checkbox compliance to proactive assurance, and the notion that cyber assurance has become an important strategic enabler to attract the Foreign Direct Investments (FDI) and protect institutional credibility in global markets, is a notable trend for FDI attraction. The contribution of this paper is a sectoral Cyber Assurance Policy Framework proposed for India's healthcare ecosystem. It promotes alignment of governance, continual monitoring and national level certification mechanisms as well as third-party security audits. Practicality of these insights for actionable roadmaps for policymakers, investors and healthcare leaders seeking to create a digital trust, operational resilience and long term accountability contrast for India's healthcare infrastructure. In addition, the study plays a timely and policy relevant role in the broader discourse on policies for achieving cybersecurity preparedness in emerging digital health systems.

Keyword: Cybersecurity Maturity, Cyber Assurance, Healthcare Governance, Digital Health Infrastructure, Foreign Direct Investment (FDI), Data Protection, Cybersecurity Policy Framework, Zero Trust Architecture

1.INTRODUCTION:

The level of sophistication of cyber threat has become a critical challenge within the global industries and the health care industry has been found as the most vulnerable area being sensitive data in hand (Javaid et al., 2023). This vulnerability is more prominent in India, where the widespread adoption of

digital health technologies, reliance on interconnected medical systems, and poor cybersecurity maturity in the sector further enhance the risk (John et al. 2024). Although awareness of the need to mitigate potential cyber threats is growing among healthcare providers, cybersecurity is unevenly included within organizational priorities as healthcare institutions see an increase in cyberattacks on patient data, IoT devices, and continuous operations. Ransomware, data theft, and supply chain attacks are focusing on healthcare, causing catastrophe (Skorupka, & Boiney, 2021). In 2025, Lamche (2025) reported that Britain's NHS 111 services were the target of a 2023 ransomware attack, in Ireland, a ransomware breach hit the Health Service Executive (HSE) in 2021, and in 2021, Alder(2021) related the attack on Universal Health Services in the U.S. Globally, such incidents triggered widespread data disruption and care delays. India witnessed the AIIMS ransomware attack in 2022 which meant that 40 million patient data were compromised, and the ICMR, the Star Health, and the HealthifyMe all experienced data breaches (Gandhi & Pahwa, 2024). All these incidents point to how healthcare cyberattacks undermine not only privacy but also the delivery of public health and national security, and thus mandate security beyond just a technical defense.

Handling a huge volume of personally identifiable information (PII) and sensitive health data, it is one of the critical infrastructure sector from cybersecurity perspective (Vikash, 2022). While the National Digital Health Mission (NDHM), the increased adoption of telemedicine, electronic health records (EHRs), and AI driven diagnostics look encouraging, it results in a massive increase in the attacks surface (Bagga et al. 2024). Additionally, with medical IoT devices—almost all legacy firmware or unsecured network integration—together with the projection of the weaponization of AI/ML by cybercriminals make Indian healthcare providers highly vulnerable (Krishnan, & Singh, 2022).

However, weak healthcare specific implementation has been there (Mihir, 2023) through Digital Personal Data Protection (DPDP) Act and Information Technology Act in India. NIST CSF, ISO 27001, and zero trust architecture are already existing cybersecurity frameworks which are equally good (more so for ISO 27001, especially), and they mainly mange the technical control and compliance layers (Brown, 2025). Since most of the Indian institutions do not have the capacity or mandates to implement these models fully, the defenses are fragmented and with low cyber maturity (Bahuguna, Bisht, & Pande, 2019). This sector shows untrained staff, unsecured endpoints and disjointed systems which makes it difficult to achieve sector wide resilience.

Cyber Assurance is introduced and conceptualized as a governance oriented Cybersafety mechanism that certifies that not only Cybersafety (security) controls 'exist,' but are also 'in place' with minimal change going forward, are 'effective' to gain user confidence and certain (applicable) Cybersecurity controls are 'available' for independent Cybersecurity auditing and institutional accountability (Maleh et al 2021; Tomlinson et al 2024). Unlike reactive compliance models, cyber assurance primarily focuses on stakeholder trust, regulatory alignment, and investment readiness for highrisk and data-intensive sectors like healthcare (Lång, Nikundiwe, Hoogmoed, & Bonfadelli, 2016; Raizada & Srivastava, 2024). As a result of this, cyber assurance extends beyond frameworks and it asks are the right systems in place? (Desai & Desai, 2023). Are they working? Can stakeholders trust them consistently?

This is particularly important in the healthcare context. Sensitive data is entrusted in institutions, governments rely on hospitals to deliver public health, digital risk is evaluated before investing in health-tech ventures. Auditability, transparency, and policy certainty are the aspects that cyber assurance offers to these stakeholders (Adebukola et al., 2022). However, India has no ubiquitous cyber assurance model for the standardizing and formalizing of this trust. Current cybersecurity governance within the Indian healthcare sector is inadequate due to the pressing need to not only assess and elevate the cybersecurity of the sector through technical upgrades but by embedding policy driven assurance mechanisms. By understanding the risk perceptions, the current maturity levels and the implementation challenges, a more robust cyber trust infrastructure can be developed such as it is necessary to achieve digitization of healthcare and investment.

This research aims to analyze the current state of cybersecurity maturity in India's healthcare sector, evaluate the effectiveness of existing policy frameworks, and explore the role of cyber assurance in enhancing trust and attracting Foreign Direct Investment (FDI). Specifically, the research contributes by:

- Analyzing cybersecurity vulnerabilities and challenges across Indian healthcare institutions
- Identifying institutional, regulatory, and behavioral factors shaping cybersecurity maturity
- Examining the influence of government policy and regulation on institutional practices and FDI sentiment
- Proposing a structured Cyber Assurance Policy Framework tailored to India's healthcare ecosystem

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Through these contributions, the research aims to support a more resilient, trusted, and investment-ready healthcare infrastructure for India's digital future.

2.LITERATURE REVIEW:

Casarosa (2024) considers potential cybersecurity threats of IoT medical device integration in terms of both data protection and system vulnerabilities. The study identifies categories of imperfections and overlaps in the EU legal framework, including between GDPR, MDR and new proposal CTIA. It requires more regulatory coherence to sufficiently and securely deploy medical IoT devices. Burrell (2023) discusses the increasing cybersecurity risk management complexity in healthcare that has been augmented by the quick pace of digitalization and the addition of technologies such as blockchain and virtual reality. The paper recognises human error as the most important threat vector, and urges improved public-private collaboration. This shows that despite more training and mitigations by the sector, the sector's cyber vulnerability is growing..

Abbasi and Smith (2023) provide an analysis of the cybersecurity threats to patient health information (PHI) and explore HIPAA's quest to establish as a basic compliance framework. Key challenges such as outdated infrastructures, lack of relevant resources, and vulnerabilities of humans that hinder the effective implementation are identified. The paper calls for the adoption of adaptive cybersecurity strategies and permanent training of staff with a view to protecting PHI as well as regulatory compliance.

In, their paper Tomlinson et al. (2024) investigate the shift of Perimeter Based Security Models to Zero Trust Architecture implemented in large healthcare facilities. ZTA is found to be robust and decreases the risks and security vulnerabilities, but is more costly to implement and complex. The given results show that access control frameworks for securing healthcare cybersecurity have strategic trade offs.

The work of Alozie and Chinwe (2025) suggests a modular framework for cybersecurity in protecting critical infrastructure requiring adaptability over various sectors such as healthcare and finance. The framework incorporates AI, blockchain, and zero trust principles to attack key vulnerabilities, including through five pillars: risk assessment, access control, incident response, resilience, and governance. The effectiveness of the process in minimizing cyberattack impact and improving organizational resilience are confirmed by case studies.

The research conducted by Joy et al. (2024) discusses advanced cybersecurity protocols for critical data management systems in industrial and healthcare environments such as ransomware and insider attack. In the end, the study highlights, based on real world situations, the usefulness of encryption, intrusion detection, and multi authentication factor. It highlights the necessity to educate staff continuously and to embrace technology to address emerging cyber risks.

According to Ahouanmenou (2024), a hospital cybersecurity maturity model has been proposed which specifies the various vulnerabilities of hospitals to the cybersecurity concerns related to the interconnected healthcare systems. The cyber risk assessment is improved along with enhancing data integrity and services continuity using Research Science Design Methodology. It gives a structured methodology to evaluate and enhance cybersecurity readiness in the hospital setting.

Raju and Kondle (2024) take a look at how the Cybersecurity Maturity Model Certification (CMMC) cyber controls can be integrated with HIPAA for improved healthcare IT cybersecurity. The argument is that CMMC is a step in the right direction to fill longstanding HIPAA security gaps, and that practices introduced are more robust and modernized. This hybrid model study advocates this hybrid model as one means to strengthening resilience and supporting digital transformation in healthcare systems.

In the light of the sudden digitalization, Gupta, Mishra and Makkar (2024) come forward with the global cybersecurity standardization framework for healthcare informatics, fearing lapses in existing privacy regulations. They prioritize critical activities into five domains, thereby prioritizing data protection and policy compliance, using Delphi, DBSCAN, and TOPSIS methods. It provides a structured roadmap for secure management of PHI from the perspective of healthcare stakeholders.

According to Sharma, Habibi Lashkari and Parizadeh (2024), cybersecurity in healthcare is evolving, and involves the protection of patient data, system integrity and patient safety. In this chapter, it is important to design the resilient cybersecurity systems and regulation compliance remains one of the important pillars. The guideline provides practical guidance to healthcare professionals and policymakers in an environment that becomes ever more threat prone. In Ali and Mijwil (2024), they review cybersecurity in smart healthcare systems in a comprehensive way by pointing out that Sybil attacks and medjacking are two debilitating attacks. A taxonomy of attack types and defense

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

mechanisms (mainly cryptography and digital watermarking) with respect to ensure data integrity and system availability is presented. Risk assessment is emphasized as continuous in order to keep the smart healthcare ecosystems resilient and sustainable.
In their research, Qurashi et al. (2024) propose how generative AI can be leveraged to revolutionize cybersecurity defenses in healthcare and allows real time threat detection and mitigation. Five AI driven mechanisms, from anomaly detection to zero-day exploit counter measures, are proposed to strengthen digital health infrastructure. This demonstrates how AI plays a crucial role in changing threat response strategies and making security more proactive and adaptive. Statistical modeling is used by Dobrovolska et al. (2024) to identify global health security and cybersecurity interdependencies among 190 countries. Additionally, their findings show that robust health security systems, in fact, have a robust, positive influence on national cybersecurity performance. It shows the causality between health security factors which contributes to form cybersecurity outcomes with the proviso that policies should be developed in an integrated fashion.
In order to facilitate cybersecurity self evaluation, Burke et al (2024) argue for the development of specific self evaluation tools for the relevant Australian Healthcare sector directed towards the proactive identification of risk, rather than the reactive response. The study uses focus group insights to substantiate key challenges related to financial constraints, regulatory ambiguity and concerns of privacy. The paper promotes sector specific strategies to build up preparedness and resilience to new cyber threats.
While prior studies have explored cybersecurity risks, technical frameworks, and regulatory compliance in healthcare, they largely emphasize reactive and fragmented approaches. There is limited focus on governance-level mechanisms that ensure continuous, verifiable trust in cybersecurity systems. The strategic role of cyber assurance in enhancing institutional credibility and attracting FDI remains underexamined. This study addresses these gaps by proposing a policy-driven assurance framework tailored to India's healthcare sector.

3.RESEARCH METHODOLOGY:

This research used a qualitative research design to analyze cybersecurity maturity, cyber assurance practice, and policy gap in India's healthcare industry. 15 cybersecurity experts working in hospitals, health-tech companies, pharmaceutical companies, and cybersecurity consultancies in India were interviewed using in-depth, semi-structured interviews. Purposive sampling was employed in order to select participants to obtain strategic and managerial representation across the healthcare ecosystem. The interviews were designed to construct deep insights from institutional practices, policy perceptions and investor considerations. Braun and Clarke's six-phase method of identifying, refining and mapping emergent themes was adopted to entitle and map single emergent themes from interviews using NVivo 14, a qualitative research program. An AI assisted analysis tool, NotebookLM, was used to help cluster between the responses and validity the coding structure.

4.DATA ANALYSIS:

Thematic Analysis:

Theme 1:

There is a growing but uneven recognition of cybersecurity within India's healthcare industry. Many experts agree that while awareness is increasing, cybersecurity remains under-prioritized compared to other sectors. One respondent stated:

"The healthcare industry in India has understood the importance of cybersecurity but has still not invested enough in implementation."
Several professionals highlighted that larger organizations are beginning to adopt advanced practices, such as the Zero Trust model, while others are still grappling with the basics of threat monitoring and data protection. A senior advisor shared:

"Raksha being an IT organization has a robust cybersecurity infrastructure... but when it comes to healthcare organizations, the coverage is diligent yet incomplete."
This is quite like a fragmented ecosystem where cybersecurity maturity differs immensely from one institution to the other. As mentioned by Poongodi etal. (2024), these gaps have been recently exploited by recent ransomware attacks particularly small healthcare providers and public hospitals. Indian

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

institutions have been trailing the global counterparts when it comes to adoption of structured frameworks like NIST CSF or ISO 27001 in the country, it continues to be vulnerable to data leaks. The need for this is reinforced by the 2021 AIIMS ransomware incident, and 2023 that has witnessed more than 348,000 cyber attacks (Raizada & Srivastava, 2024). Maturity growth is not binary, it's stages flow. With limited resources, personnel and leadership attention, many institutions are stuck in reactive postures. Such lack of strategic integration is caused not only by phenomenon of internal inertia, but also by the fact that there is no strong external regulatory compulsion. Part 1 concludes that internal capability building and external regulatory mandates have become equally important forces to address this maturity gap as is discussed in the theme below.

Theme 2: Key Factors Contributing to Cybersecurity Maturity
However, maturity levels across India's healthcare sector are inconsistent, and there are a number of interconnected drivers pushing it up. Further, the forces identified by the experts from the field while assessing the growth of organizational commitment for cybersecurity as government regulations, rising cyber awareness, and technological advances. It is one of the external catalysts e.g. Evolving regulatory ecosystem in India. The regulatory momentum for data protection has been building up with frameworks such as the Digital Personal Data Protection (DPDP) Act, the National Digital Health Mission (NDHM) and the proposed G20 Digital Health framework. As one respondent emphasized:

"DPDP Act, NDHM, and the proposed G20 Digital Health framework are crucial for building trust and driving cybersecurity practices."
These initiatives set compliance requirements that usher in the need for healthcare institutions to revisit how they manage, protect, and report breaches on their data. This trend is supported by literature — Kumar (2024) mentions that "the present legal framework is being transformed from passive data handling into proactive healthcare data governance in India, mainly due to new legislations." Secondly, cyber risks are getting more noticeable consciousness due to global and domestic incidents. Both IT leaders and hospital boards have been sensitized about high profile ransomware attacks on Indian hospitals and insurance companies. As one industry expert put it:

"The awareness created or experienced by cyber incidents globally has compelled healthcare leaders to start asking the right questions."
This growing awareness is also fuelling internal investments in data monitoring, encryption, and risk assessment. According to Desai and Desai (2023), Indian healthcare institutions have started incorporating NIST CSF and Zero Trust frameworks, especially in urban and corporate hospital networks. Another contributing factor is the digitization of healthcare delivery — including virtual doctor consultations, telemedicine, and electronic health record (EHR) systems — which inherently carry higher exposure to cyber threats. This digital expansion necessitates robust security architecture. One participant reflected this:

"Data protection, virtual doctor services, and patient records in the cloud are now understood as security-sensitive areas."
Awareness of such a challenge has driven organizations into a slow paradigm shift from a reactive to a proactive security posture, wherein their internal controls tend to be aligned to industry standards such as ISO 27001, ISO 22301, and HITRUST. They added that investments in threat detection, endpoint protection and data classification are becoming mainstream, and especially prevalent among larger players with larger stakes. However, these developments are not even across the board. Smaller clinics and public health units still face budget, talent, and infrastructure constraints. In maturity, therefore, is not yet free of regulatory triggers from the outside and does not yet have commitment at top leadership level.
Summarizing all, critical factors are involved that are molding the cybersecurity maturity of India's healthcare system. The rapid shifts in data regulation due to the enactment of the Digital Personal Data Protection (DPDP) Act has increased the demand for compliance and data governance. Also, growing awareness of the market, a result of potent cybersecurity incidents of various high scale magnitude, has further increased focus on security practices. Increasing technological complexity from rapid digitization only compounds the landscape requiring more robust and adaptive security strategies. Given this, healthcare institutions are increasingly adopting advanced frameworks such as Zero Trust

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

architectures and standards based on NIST and ISO. These developments together comprise a foundation for institutional transformation. However, the extent to which these efforts succeed or fail is largely dependent on the internal organizational capability of having a robust governance practice combined with cybersecurity strategy that is well aligned to the wider institutional goals.

Theme 3: Approaches to Cybersecurity within Healthcare Organizations
As cybersecurity threats evolve in complexity, healthcare organizations in India are developing diverse approaches to data protection, threat mitigation, and resilience. These approaches, however, are deeply shaped by the institution's size, digital maturity, data sensitivity, and sectoral specialization—such as hospitals, pharma, or MedTech. Respondents described a spectrum of internal strategies, ranging from basic endpoint protection to advanced in-house threat intelligence teams. For instance, one participant from a cybersecurity consultancy highlighted a multi-layered approach:

"Raksha Technologies being a Cyber Security Services firm follows industry standards. We have endpoint, database, and network security integrated with asset classification and threat detection."
Others emphasized a contextual approach where the focus depends on the specific type of data handled. For example, pharma companies prioritize intellectual property (IP) protection, whereas hospitals focus on electronic medical records (EMRs) and clinical workflow integrity. A director working with fraud prevention noted:

"We have in-house threat hunting teams. Our data masking and endpoint monitoring systems are built around the risk models we've developed internally."
This indicates a shift towards risk-based, asset-centric protection frameworks, aligning with globally recommended standards like NIST CSF, ISO/IEC 27001, and HITRUST.
Importantly, organizations are increasingly adopting Zero Trust architecture—a paradigm shift that assumes breaches are inevitable and emphasizes least-privilege access, micro-segmentation, and continuous authentication. One respondent stated:

"Implementing Zero Trust principles helped us tighten our access control and minimize lateral movement in case of a breach."
For organizations delivering telehealth services, the architectural focus extends to cloud-native controls, encryption of patient health information (PHI), and regulatory compliance checks. The integration of data protection, detection, and response is a common emerging practice.
From an operational perspective, the implementation of several core components is routinely conducted in order to improve cybersecurity maturity within healthcare organizations. Asset discovery and classification are included in these, and, they provide the base for detecting and managing essential digital assets. Vulnerability risk assessments and control audits are performed to validate compliance with regulatory standards. Network endpoints (the end points of a network) are monitored and mitigated in real time by deploying Endpoint Detection and Response (EDR) tools. Safeguarding of sensitive health information is based upon data encryption and backup restoration mechanisms to prevent breaches from sensitive health information and to restore continuity of business in case of data breaches or system failures. In addition, behavioral analytics are used to detect insider threats in discovering anomalous user behavior, which may help in being preemptive in risk mitigation. These operational measures, when viewed as a whole, contribute greatly to a resilient and responsive cybersecurity framework.
Yet, the interviews also reveal that these structured frameworks are not the norm across the board. Many small and medium healthcare providers lack the budgets, technical know-how, and leadership commitment to adopt such models. For example, one respondent noted:

"Many organizations still don't have a baseline cybersecurity policy. They treat it as a compliance checkbox rather than a core business enabler."
This points to an urgent need for sector-wide capacity building, especially in Tier 2 and public institutions, where digital transformation is outpacing cyber preparedness. Furthermore, the intersection of operational technology (OT)—such as connected medical devices—and traditional IT systems introduces unique challenges in securing device firmware, patient telemetry, and hospital automation. Organizations that manage Internet of Medical Things (IoMT) are beginning to explore network segmentation, anomaly detection, and secure-by-design hardware. In summary, the approach

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

to cybersecurity in India's healthcare organizations is evolving from basic IT protection toward strategic, architecture-driven, and compliance-aligned systems.

Theme 4: Primary Challenges and Vulnerabilities
Despite regulatory pushes and the increasing adoption of cybersecurity frameworks, healthcare organizations in India continue to face systemic and operational challenges that undermine their cybersecurity resilience. These vulnerabilities are not merely technical—they are organizational, cultural, and infrastructural. A dominant thread across expert interviews is the sector's underestimation of cybersecurity as a strategic priority. Unlike banking or finance, healthcare is often perceived to lag in cyber investments. One respondent aptly captured this sentiment:

"There's a lack of adequate knowledge of the risks, hence limited management focus. Cybersecurity is still treated as a support function, not a business enabler."
This perception gap results in cybersecurity being reactive—driven by compliance rather than strategic foresight. Even in relatively advanced organizations, coverage remains "diligent yet incomplete," as noted in earlier themes. Another recurring concern is the fragmentation and disparity in system architectures across the Indian healthcare ecosystem. Hospitals, diagnostics labs, and pharma companies often use disparate legacy systems, lacking standardized protocols or centralized governance. This fragmentation makes it difficult to enforce consistent cybersecurity policies, leaving systems vulnerable to lateral attacks and unauthorized access.

"Disparate systems and lack of standards in medical software complicate maintaining consistent cyber hygiene," said one IT consultant with decades of experience.
A critical technical vulnerability discussed by respondents is the configuration and management of existing security controls—firewalls, EDR, encryption, and patching—especially in institutions where IT staff are minimal or overburdened. Moreover, medical devices and IoT (Internet of Medical Things) are now integral to patient care but often lack robust firmware-level security. Devices are frequently connected to hospital networks without segmentation, increasing the attack surface significantly.

"Managing medical devices, IoT security, and endpoint vulnerabilities is becoming more difficult every year," a cybersecurity director shared.
In addition to external threats, several interviewees emphasized insider risks. The lack of cybersecurity training among medical professionals, staff using weak credentials, or sharing devices and login information, opens new avenues for data compromise. This is particularly concerning when handling sensitive patient data, clinical trial results, or genomic records.

"Getting doctors and medical staff to follow cyber hygiene is one of the hardest parts. They don't see it as their responsibility," another respondent emphasized.
This is corroborated by literature as well. Wazid et al. (2022) highlight that most healthcare institutions globally—and especially in India—struggle with legacy infrastructure, budget constraints, and lack of qualified cybersecurity personnel, all of which contribute to a high risk of breaches. Similarly, Desai and Desai (2023) points to a chronic underinvestment in staff training and process-level controls in Indian healthcare organizations. In many cases, institutions implement isolated tools without holistic integration, resulting in coverage gaps that can be exploited. The overreliance on antivirus and basic firewalls, without a layered defense-in-depth strategy, further exposes critical systems.

Table 1: Key challenges identified across interviews:

S.No	Key Challenge
1	Lack of cyber maturity and knowledge at leadership level
2	Misconfigured or underutilized cybersecurity tools
3	Inadequate security for medical IoT and telemedicine infrastructure
4	Weak data-sharing protocols across departments or with third parties
5	Poor enforcement of user access controls and behavioral monitoring
6	Insider threats and low awareness among non-technical staff
7	Absence of standard operating procedures and unified policy enforcement

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Theme 5: Best Practices and Successful Approaches

Amidst growing threats and systemic challenges, several Indian healthcare organizations are beginning to demonstrate cybersecurity leadership by implementing proactive, risk-based, and layered defense strategies. These organizations are not merely reacting to regulations or breaches — they are creating internal cultures of cyber resilience, led by structured practices and guided frameworks.
Interview data reveals that organizations making the greatest strides in cybersecurity consistently implement a combination of technical controls, organizational training, and operational discipline. One of the most emphasized strategies is awareness and incident response training:

"Cyber awareness training and incident response training have been crucial in strengthening our internal posture," stated a respondent from a leading security consulting firm.
Another key success factor is the practice of conducting periodic cyber health checks—internal audits that test the effectiveness of current defenses and simulate breach scenarios. These checks not only help uncover vulnerabilities but also improve organizational response readiness, ensuring departments act swiftly and in coordination during a real incident. In terms of technical strategies, experts highlighted the implementation of Zero Trust architecture as a major turning point:

"Implementing Zero Trust principles has helped us control access more precisely, particularly for remote and third-party users," noted one cybersecurity facilitator.
Zero Trust, in this context, involves network segmentation, strict access controls, real-time authentication, and micro-level monitoring — essential components in preventing lateral movement during attacks, especially in hospital IT systems or cloud-hosted patient data environments.
Several respondents also cited the use of risk-based frameworks aligned with global standards such as:

- ISO/IEC 27001 (Information Security Management)
- ISO 22301 (Business Continuity)
- NIST CSF (Cybersecurity Framework)

These frameworks help organizations define, monitor, and continually improve their security posture in a structured and measurable way.
A particularly recurring theme was data resilience — especially strategies for data backups, encryption, and restoration testing. One expert emphasized:

"We not only back up sensitive data regularly but also perform restoration drills to ensure that recovery procedures actually work."
This kind of practice, often overlooked in smaller institutions, plays a vital role in ransomware preparedness and post-breach recovery, especially for electronic health records (EHRs), insurance data, and diagnostic imaging files.

Table 2: Best practices observed across organizations:

S.No	Best Practice
1	Asset discovery and classification
2	Privileged Access Management (PAM)
3	Behavioral analytics for insider threat detection
4	Deployment of Managed XDR (Extended Detection and Response)
5	In-house or outsourced threat intelligence monitoring

High performers are fundamentally different: Whereas cybersecurity has been understood as a one time setup or compliance task, it has now turned into a continuous, strategic function and is linked to business risk. Academic literature reinforces these findings. As per Mishra et al. (2024), the higher resilience of healthcare networks is achieved by using layered security along with staff training and early threat detection systems. Desai and Desai (2023) also state that disaster recovery plans need to be tested regularly, and encrypted backups are necessary to gain stakeholders' trust.

Theme 6: Investor Perspectives on Cybersecurity
As India's healthcare industry becomes increasingly digitalized and globally integrated, cybersecurity has emerged as a key determinant of investor confidence. Particularly for foreign direct investment (FDI), cybersecurity is no longer viewed as a back-office IT issue but as a strategic parameter that

signals organizational maturity, data governance, and operational risk management. Multiple respondents emphasized that today's investors, especially those in the health-tech and pharmaceutical sectors, explicitly assess cybersecurity readiness during pre-investment evaluations. This includes reviewing internal policies, regulatory alignment (e.g., DPDP compliance), and breach history. As one security lead explained:

"Cybersecurity is increasingly becoming a key parameter for investors. It reflects whether the organization can manage digital risk in a regulated environment."
In healthcare, where the sensitivity of patient data is paramount, cyber readiness is directly linked to brand reputation, regulatory compliance, and litigation risk. Several experts noted that investors are now looking for quantifiable indicators such as:

- Cyber hygiene scores or internal audit reports
- Compliance with international frameworks (e.g., ISO 27001, HITRUST)
- Evidence of incident response plans and data breach drills
- Metrics on data encryption, access control, and monitoring systems

"A robust cybersecurity policy makes investors feel more confident. They want to see readiness, not just intentions," remarked a presales leader working with multinational clients.
Traditional financial due diligence is complemented by more routine evaluation of technology and cybersecurity as a part of the investment due diligence process. This is most important particularly when you are dealing with cross border data flow, joint venture or a third party cloud provider. Scholarly research echoes these insights. Raizada & Srivastava (2024) states that India's DPDP Act compliance and GDPR style controls are now the key consideration for the foreign investor's prospective for Indian healthcare assets. Prominent internal controls, incident preparedness as well as third party risk management frameworks are governance indicators that serve as risk mitigators for investment portfolios. The recent wave of cyber incidents in India's healthcare sector adds to the alignment between cybersecurity and investor sentiment. As an example, in 2022, the AIIMS ransomware attack and the Star Health exposure in 2024 have eroded any trust that investors might have had in their ransomware models, especially for new or small businesses who are not familiar with India's own data protection mechanisms. In other words, in addition to compliance investors also consider whether cybersecurity is integrated into the strategic governance of the company. Does the board oversee cybersecurity risk? Is there a CISO or designated officer accountable for data protection? Are security incidents logged and reviewed at the leadership level?

"Foreign investors today ask about more than revenue—they ask about your breach history, DPDP audit status, and how data is segregated," said one respondent who advises multinational buyers.
In addition, pharmaceutical and clinical research organization (CRO) sectors, where IP is dealt with and clinical trial data is handled, are subject to even more restricted control, because the leak or covert gathering of data has international implications. It was by this theme that this revelation was revealed that the Indian healthcare sector is experiencing a transition from old times where the economic attractiveness and the potential of receiving capital flow into the country is so closely intertwined with the issue of cybersecurity. In the past, cyber resilience meant protecting systems; now it means establishing trustworthiness with partners all over the globe. The bridging of the focus on institutional assurance into the next theme, on how healthcare organizations can use structured cyber assurance policy to signal trust, governance, and data integrity, is also accomplished.

Theme 7: Impact of Regulations and Policies
Regulatory frameworks in India are playing an increasingly pivotal role in shaping cybersecurity priorities within the healthcare sector. As the sector undergoes rapid digitization, both domestic legislation and international policy frameworks are emerging as essential catalysts for governance reform, investor trust, and institutional transformation. Respondents unanimously acknowledged the regulatory environment as a core driver of cybersecurity evolution. The enactment of the Digital Personal Data Protection (DPDP) Act, the rollout of the National Digital Health Mission (NDHM), and the deliberations around the G20 Digital Health Framework are regarded as game changers that are pushing healthcare organizations toward more rigorous cybersecurity postures.

"The DPDP Act, NDHM, and the proposed G20 Digital Health framework are crucial for building trust and driving cybersecurity practices," stated one cybersecurity advisor.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

These policies introduce mandatory data protection principles, patient consent protocols, breach reporting obligations, and accountability structures—all of which force healthcare providers to re-evaluate legacy systems and institutionalize data security.
Widening ranges of regulatory and operational standards now require organizational demonstration of a set of robust data protection and cybersecurity measures. To achieve these, users must be granted access only to the information that they need to perform their specific roles, while role based access control and least privilege mechanisms are implemented to make such that users do not have access to information that they are not required to have. Moreover, timely mechanisms to breach notification, adhering to regulatory timeframes, are crucial for transparency and for holding parties accountable. In addition, data minimisation and purpose limitation are required by organisations so that they limit collection and processing of data to a minimum, thereby reducing possible risks. It is equally important to establish broader consent management frameworks that respect individual autonomy and guarantee that personal data are lawfully processed. Together these measures represent an increasingly mature way in which organizations are viewing cybersecurity and data governance today.
The introduction of the DPDP Act in particular has led to increased executive-level awareness, prompting many organizations to either formally appoint Data Protection Officers (DPOs) or embed data governance functions within their IT and legal teams. According to Joshi (2021), the DPDP Act marks a paradigm shift in India's approach to health data regulation, aligning it more closely with global standards like GDPR. Beyond compliance, the regulatory push is improving investor confidence. One respondent noted:

"Foreign investors want clarity. When they see clear policy and strong enforcement mechanisms, they're more likely to engage with Indian healthcare companies."
This link between regulatory certainty and investment attractiveness is supported by Raizada & Srivastava (2024), who argue that mandatory cybersecurity audits and maturity disclosures can become differentiators in international deal-making. However, experts also cautioned against policy-overload without capacity-building. Regulations may exist on paper, but without trained enforcement bodies, standardized protocols, or institutional readiness, compliance risks becoming performative rather than transformative.

"Policies are great, but implementation is where we fail. There's a need for periodic audits and a central authority to certify maturity," one respondent emphasized.
Respondents also state that a sector specific regulatory body for healthcare cybersecurity should be created independent of general regulator for IT. This would be a certified body that would certify cybersecurity maturity, do audits, set standards, and which would enforce breach accountability. Similar can be found in Desai and Desai (2023) as they suggest that India must set up mandatory cybersecurity scorecards in their healthcare sector to hold individuals accountable enough. Healthcare cybersecurity is global so there is integration of international norms, like HIPPA and ISO/IEC standards. Last but not the least, support for policy like DPDP Act and NDHM should be backed by monitoring bodies and agencies to drive trust, and investor confidence and innovation in terms of delivery of public services.

Theme 8: Importance of Cyber Assurance
As healthcare institutions in India grapple with increasing cyber threats, digital transformation, and evolving regulatory demands, a critical concept has begun to gain prominence—cyber assurance. Beyond compliance and technology adoption, cyber assurance is about offering verifiable, ongoing confidence to all stakeholders—patients, regulators, partners, and most importantly, investors—that data security is not only implemented but consistently governed, monitored, and improved. The interviews revealed a growing recognition among experts that cyber assurance acts as a strategic trust enabler in healthcare, especially in the context of foreign direct investment (FDI), global partnerships, and patient data sensitivity. One respondent stated:

"Developing and implementing a Cyber Assurance Policy is vital to enhance trust and attract FDI."
This highlights how cyber assurance is distinct from general cybersecurity. While cybersecurity focuses on defense mechanisms and technical controls, cyber assurance involves validating the effectiveness, governance, and continuity of those controls over time. It addresses not just "Are we secure?" but "Can we prove we are secure and compliant—and will we stay that way?"

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Several experts highlighted that cyber assurance is becoming essential in areas such as clinical trials and pharmaceutical collaborations, telemedicine platforms serving international patients, healthtech startups managing large-scale sensitive health data, and the insurance and diagnostics sectors with cross-system integrations.

"Cyber assurance provides confidence to stakeholders that systems will continue to perform securely, even under stress," noted one IT governance professional.
Practically, cyber assurance translates into policies and actions such as independent audits and maturity assessments aligned with standards like DPDP, ISO 27001, and HITRUST. It also includes cyber resilience planning, including disaster recovery testing, third-party risk management, particularly for cloud and IoT integrations, periodic re-certification of security controls, and transparent reporting of cybersecurity KPIs to boards or investors.
Cyber assurance is increasingly understood as distinct from simple compliance. According to Tomlinson et al. (2024), cyber assurance is the 'next evolution' for digital governance when the risks involved in an organization's privacy are complex, such as in healthcare. Institutionalizing cyber assurance presents healthcare organizations with a strategic strength in defending against cyberattacks—and influencing public perception, as well as improvement in help for legal defense and investment appeal. In India's healthcare ecosystem, cybersecurity maturity is still inconsistent, many institutions are still relying on a fragmented and or a checklist driven approach. Indian healthcare respondents suggest that a centralized cyber assurance framework, possibly endorsed by a national certifying authority, could standardize cybersecurity benchmarks across Indian healthcare, enable clarification and continuity for international partners and investors following cybersecurity breaches; this would also support a broader, positive cultural shift towards stronger security governance.
One expert emphasized:

"Cyber assurance is not optional anymore. It's the currency of trust in digital healthcare."
The assurance model bolsters resilience to emerging risks, including AI enabled attacks and IoT vulnerability based attacks, by helping healthcare organisations shift from 'compliance based security' to 'trust based resilience,' among others. Finally, cyber assurance becomes a unifying principle that knits together the technical controls, regulatory compliance, investor expectations and reputational trust. It gives measurable, auditable cybersecurity confidence, a strategic competitive edge in the acquisition of foreign direct investment (FDI) and partnerships, and serves as a foundation for long-term digital health expansion.

Theme 9: Emerging Threats and Concerns
As India's healthcare sector embraces rapid digitization, a new generation of cybersecurity threats is emerging—threats that are dynamic, AI-powered, and often deeply embedded in the expanding Internet of Medical Things (IoMT) ecosystem. This theme explores the expert consensus that the threat landscape is no longer limited to conventional malware or phishing; it is evolving into a highly sophisticated, deeply integrated, and potentially AI-enhanced domain of cyber risk. Several respondents expressed concern over the rise of AI/ML-enabled cyberattacks, which are expected to outpace traditional security measures in both scale and complexity. These attacks could leverage machine learning to bypass traditional defense mechanisms, automate credential harvesting, or adapt attack vectors in real time.

"Cybercriminals will soon begin exploiting AI/ML models to design even more complex attacks. We're not ready for that yet," said a cybersecurity advisor involved with national telehealth systems.
Scholars echo this warning. Desai and Desai (2023) caution that healthcare organizations must now account for adversarial AI—where attackers manipulate data inputs or use deepfakes to breach biometric systems or trick clinical AI algorithms. In parallel, the widespread integration of Medical IoT devices introduces massive vulnerability. Devices such as insulin pumps, cardiac monitors, and imaging scanners often lack firmware-level security and are rarely updated. These devices operate in low-resource environments, often remain connected to hospital networks, and typically lack encryption or authentication protocols.

"Attacks are increasingly targeting Medical IoT devices. They're easy to access and hard to secure," noted one security manager.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

This is particularly problematic in the Indian context, where budget constraints and low cybersecurity maturity among many providers mean that these devices are seldom monitored with intrusion detection systems. Moreover, IoMT networks are often integrated with operational hospital systems, allowing attackers to move laterally from a compromised device to patient records or hospital databases.
Beyond technical vectors, respondents highlighted a growing concern about data breaches, particularly involving third-party vendors and cloud service providers. As healthcare organizations increasingly rely on SaaS-based EMRs and diagnostics platforms, data control becomes diluted, increasing the risks of unauthorized access, cross-border data exposure, and accidental leaks.

"We're worried about third-party data processors. We may be compliant, but what about the services we use?" asked a digital health entrepreneur.
Further, the progress of digital transformation itself—from telemedicine to genomic data integration—has significantly raised the stakes. Patient data is now more voluminous, more sensitive, and more mobile, which makes real-time protection and governance extremely difficult without adaptive security models. In addition to external threats, insider risks continue to be underestimated. Several respondents expressed concern over the human element—untrained staff, shared logins, social engineering, and credential misuse remain common vulnerabilities in public and private health facilities alike.
Experts believe that in order to manage these risks, it is suggested to implement proactive AI monitoring tools such as behavior anomaly detection, device level security baselining for the Internet of Medical Things (IoMT), regular cyber simulations for insider threat scenarios, AI resistant authentication systems and vendor cybersecurity audits and certifications. To wind up, the Indian health care sector deals with a consistently advancing danger scene comprising AI empowered assaults, IoT weaknesses, supply chain dangers and insider dangers. This requires a move away from traditional, reactive, defensive cybersecurity measures to anticipatory, intelligence driven security architectures. In this context, the building of cyber resilience will involve not only advanced tools but also a greater requirement for institutional governance, reassurance in the field of continuous assurance and cross sector collaboration, concepts that cover the core themes of this analysis.

5.DISCUSSION:

India's healthcare cybersecurity landscape is an active one, but a journey still in the making. These findings align the scholarly consensus that the cybersecurity maturity in the healthcare tends to solely rise due to regulatory pressure and reputation risks and not due to proactively implementing institutional governance (Kumar, 2024; Mishra et al., 2024). But the qualitative data that you insert provides nuance, revealing internal variation: that some organizations exhibit sophisticated variations of zero trust but others basically have perimeter basic defenses. Stratification of maturity is prompted by a broader takeaway from global research that cybersecurity capability generally mirrors where an organization's leadership puts its priority, not just its technical capabilities (Desai & Desai, 2023).
Indian recent policy developments like DPDP Act and NDHM provide a much needed regulatory scaffold in absence of which whatever little progress was made in building collaborations largely relied on the social good structure being diffused voluntarily within the private sector players, despite the prevalence of adequate leadership in that regard. However, as Joshi (2021) and Raizada and Srivastava (2024) also note about these laws in literature, expert responses indicate uneven implementation and adherence of these laws driven by compliance, rather than culture. The gap is not unique to India. In sectors in Europe where digital governance maturity was low, it wasn't that GDPR had not changed anything, and in those sectors Tomlinson et al. (2024) found similar inertia during the GDPR rollout. To bridge this gap in implementation in India, laws will not be enough, there will be a need for localized enforcement, sector specific adaptation, and building capacity, particularly of mid size hospitals and regional providers.
It is interesting that academic models typically emphasize structural enablers, such as audit frameworks, cybersecurity maturity models (e.g., NIST CSF), and legislative compliance, yet the insights from the healthcare sector in this study indicate that there is an equally powerful set of motivators at work: trust, investor expectations, and executive level awareness. However, cyber assurance has become a strategic differentiator for healthcare institutions, specifically those with patients' data or clinical research, or running telemedicine platforms, experts stressed. This is a growing convergence between market driven security signaling and governance level assurance at a place that

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

the Indian healthcare policy literature has not yet explored in depth. Therefore, policy frameworks do exist but they have not been translated into trustbased ecosystems in healthcare. This gap is addressed in the present research, which demonstrates that institutional behavior in healthcare is as much driven by investment readiness and stakeholder trust as it is by statutory compliance protocols.

6.CONCLUSION AND POLICY RECOMMENDATIONS

This research qualitatively inquired into the cybersecurity maturity landscape in India's healthcare sector and considered expert insights as well as relevant literature. The findings further reveal that although the awareness of cybersecurity in health institutions is rising overall, maturity in this area continues to be uneven and mostly driven by compliance. One key spin was that the legal frameworks such as the DPDP Act and NDHM are only one part of the story here and increasing pressures are coming from investor expectations, reputational risk and stakeholder trust.
Although there exists global frameworks (NIST CSF, ISO 27001, HITRUST), we do not have a standardized national mechanism to assure the cybersecurity maturity of Indian healthcare sector. The absence of regulation chokes investor confidence, renders governance opaque, and renders India unready to welcome foreign capital in the areas of health-tech, clinical research and digital health ventures. Of more importance is the fact that because there is no sector specific Cyber Assurance Policy, institutions are not able to develop and operationalize long term trust, particularly in settings that deal with sensitive patient information and cross border collaborations.
It contributes a novel perspective to this study by framing cyber assurance as a lever of policy, not simply a technical function. This demonstrates how when assured framework elicited from national level governance ecosystems these gaps between security and compliance and investment readiness can be bridged. In order, therefore, a proactive, structured and sector aligned policy intervention is essential.

Table 3: Policy Recommendations: Toward a Cyber Assurance Framework for Indian Healthcare

S.No	Policy Recommendation	Details
1	Establish a Sector-Specific Cyber Assurance Authority	Create an agency under NDHM or CERT-In focused on healthcare cybersecurity oversight, including issuing guidelines, auditing maturity levels, and certifying compliance.
2	Implement a National Cybersecurity Maturity Index for Healthcare	Develop a maturity model aligned with NIST CSF or ISO 27001 for Indian healthcare. Benchmark healthcare providers annually and encourage voluntary disclosure of scores.
3	Institutionalize Cyber Assurance Certification	Introduce a voluntary Cyber Assurance Certification Program based on core pillars like governance, data protection, real-time monitoring, incident response, and supply chain security.
4	Integrate Assurance Requirements into FDI and Public-Private Partnership (PPP) Policies	Make cyber assurance a prerequisite in health PPPs and cross-border data collaborations. Include it as a metric in FDI proposals for digital health and cloud platforms.
5	Launch Capacity-Building and Awareness Programs	Mandate cyber hygiene training for healthcare staff, especially in public institutions. Incentivize IT upskilling in rural areas through NDHM and CSR programs.
6	Mandate Cybersecurity Audits and Disclosures	Require annual cybersecurity audits for mid-to-large healthcare providers, with summaries provided to regulators and investors, and link results to regulatory incentives.

It no longer remains optional to develop a Cyber Assurance Policy Framework for the healthcare sector in India, as it is a strategic imperative. In the era of digital, decentralized and cross border health care delivery, the integration of cyber security governance and foreign investment policy is going to be a tight fit. Drawing such conclusions, this research offers a foundation for policy makers to reimagine

assurance as a tool not only to control digital systems but also to enable digital trust, global partnerships, and create long term resilience in healthcare.

References:

[1] Abbasi, N., & Smith, D. A. (2024). Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. *Journal of Knowledge Learning and Science Technology*, *3*(3), 278-287.

[2] Abrams, L. (2021, May 20). *Conti ransomware gives HSE Ireland free decryptor, still selling data*. BleepingComputer. https://www.bleepingcomputer.com/news/security/conti-ransomware-giveshse-ireland-free-decryptor-still-selling-data/

[3] Adebukola, A., Navya, A., Jordan, F., Jenifer, N., & Begley, R. D. (2022). Cyber security as a threat to health care. *Journal of Technology and Systems*, *4*(1), 32-64.

[4] Agrawal, H. K., Agrawal, N. K., & Agrawal, S. (2024). Privacy and Security Issues for IoT and Deep Learning in Next-Generation Healthcare: An Indian Perspective. In *Deep Learning in Internet of Things for Next Generation Healthcare* (pp. 194-207). Chapman and Hall/CRC.

[5] Ahouanmenou, S. (2024, May). Towards a Cybersecurity Maturity Model Specific for the Healthcare Sector: Focus on Hospitals. In *International Conference on Research Challenges in Information Science* (pp. 141-148). Cham: Springer Nature Switzerland.

[6] Alder, S. (2021, March 24). *Universal Health Services ransomware attack cost $67 million in 2020*. HIPAA Journal. https://www.hipaajournal.com/universal-health-services-ransomware-attack-cost/

[7] Ali, G., & Mijwil, M. M. (2024). Cybersecurity for sustainable smart healthcare: state of the art, taxonomy, mechanisms, and essential roles.

[8] ALOZIE, C. E., & CHINWE, E. E. (2025). Developing a Cybersecurity Framework for Protecting Critical Infrastructure in Organizations.

[9] Bagga, G., Singh, H., & Hood, M. M. (2024). Revolutionizing Indian healthcare: The impact of digital health, AI, telemedicine, and data security. *IOSR Journal of Business and Management (IOSR-JBM)*, *26*(9, Ser. 1), 30–34.

[10] Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context. *Information Security Journal: A Global Perspective*, *28*(6), 164-177.

[11] Brown, E. (2025, April 1). *A comparison of leading security frameworks: NIST, ISO 27001, and Zero Trust*. Quick and Dirty Tips. https://www.quickanddirtytips.com/articles/a-comparison-of-leading-security-frameworks-nist-iso-27001-and-zero-trust/

[12] Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making*, *24*(1), 133.

[13] Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review*, *29*(1), 38-49.

[14] Casarosa, F. (2024). Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework. *Computer law & security review*, *53*, 105982.

[15] Desai, A., & Desai, M. (2023). A review of the state of cybersecurity in the healthcare industry and propose security controls. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2023*, 82-84.

[16] Dobrovolska, O., Ortmanns, W., Dotsenko, T., Lustenko, V., & Savchenko, D. (2024). Health security and cybersecurity: analysis of interdependencies. *Health Economics and Management Review*, *5*(2), 84-103.

[17] Gandhi, P., & Pahwa, S. (2024). All India Institute of Medical Sciences (AIIMS), Delhi: Cyberattack Puts Digitalisation Under Scanner. *Management*, *1*, 8.

[18] Gupta, K., Mishra, V., & Makkar, A. (2024). A global cybersecurity standardization framework for healthcare informatics. *IEEE Journal of Biomedical and Health Informatics*.

[19] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016.

[20] John, D., Majumdar, A. D., Pillai, R. N., Khatoon, S., Bhattacharya, P., Mukherjee, N., ... & Jakovljevic, M. (2024). Health technology assessment for digital health Technologies in India: a framework for action. *International journal of technology assessment in health care*, *40*(1), e70.

[21] Joshi, V. (2021). The Use of Artificial Intelligence in the Healthcare Sector: A Critical Analysis of the Existing Legal Framework in India with Respect to Privacy and Data Protection. *Indian JL & Legal Rsch.*, *2*, 1.

[22] Joy, Z. H., Islam, S., Rahaman, M. A., & Haque, M. N. (2024). Advanced Cybersecurity Protocols For Securing Data Management Systems in Industrial and Healthcare Environments. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(4), 25-38.

[23] Krishnan, D., & Singh, S. (2022). Medical IoT: Opportunities, Issues in Security and Privacy-A Comprehensive Review. *Smart and Secure Internet of Healthcare Things*, 91-112.

[24] Kumar, R. (2024). *Privacy and protection of patient sensitive data in the healthcare sector: a critical analysis* (Doctoral dissertation, School of Law, UPES, Dehradun).

[25] Lamche, A. (2025, March 27). *NHS software provider fined £3m over data breach after ransomware attack*. BBC News. https://www.bbc.com/news/articles/cp3yv1zxn940

[26] Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *EDPACS*, *63*(6), 1-22.

[27] Mihir, R. (2023, August 23). *Digital Personal Data Protection Act, 2023: A missed opportunity for horizontal equality*. Supreme Court Observer. https://www.scobserver.in/journal/digital-personal-data-protection-act-2023-a-missed-opportunity-for-horizontal-equality/

[28] Mishra, V., Gupta, K., Saxena, D., & Singh, A. K. (2024). A global medical data security and privacy preserving standards identification framework for electronic healthcare consumers. *IEEE Transactions on Consumer Electronics*.

[29] Poongodi, R. K., Samuel, R., Rohith, P., Parthasarathy, S., & Ramana, B. (2024). Strengthening Cybersecurity in Indian Healthcare–Lessons from the Recent Ransomware Attacks on Hospitals.

[30] Qurashi, S. N., Sobia, F., Hetany, W. A., & Sultan, H. (2025). Enhancing Cybersecurity Defenses in Healthcare Using AI: A Pivotal Role in Fortifying Digital Health Infrastructure. *Medinformatics*.

[31] Raizada, N., & Srivastava, P. (2024). Cyber-Threat Landscape in Healthcare Industry and Legal Framework Governing Personal Health Information in India. *Kutafin Law Review*, *11*(3), 452-490.

[32] Raju, N., & Kondle, P. (2024). Enhancing Healthcare IT Cybersecurity Resilience: Integrating CMMC Controls with HIPAA Compliance. *Available at SSRN 5031149*.

[33] Sharma, D. P., Habibi Lashkari, A., & Parizadeh, M. (2024). Defining Cybersecurity in Healthcare. In *Understanding Cybersecurity Management in Healthcare: Challenges, Strategies and Trends* (pp. 35-54). Cham: Springer Nature Switzerland.

[34] Skorupka, C., & Boiney, L. (2021). *Threat-informed cybersecurity operations for healthcare delivery organizations: A guide to maturing cyber defense capabilities for HDOs* (MITRE Report No. 21-2768). The MITRE Corporation. https://www.mitre.org/publications/technical-papers/threat-informed-cybersecurity-operations-for-healthcare-delivery

[35] Tomlinson, E. W., Abrha, W. D., Kim, S. D., & Ortega, S. A. (2024). Cybersecurity Access Control: Framework Analysis in a Healthcare Institution. *Journal of Cybersecurity and Privacy*, *4*(3), 762-776.

[36] Vikash, B. S. (2022). *Exploring Challenges Faced by Information Technology Security Managers in Implementing Risk Management Framework to Protect Protected Health Information and Personally Identifiable Information* (Doctoral dissertation, Northcentral University).

[37] Wazid, M., Das, A. K., Mohd, N., & Park, Y. (2022). Healthcare 5.0 security framework: applications, issues and future research directions. *IEEE Access*, *10*, 129429-129442.